WAGENINGEN
UNIVERSITY & RESEARCH

Postbus 9101 | 6700 HB Wageningen

UITSLUITEND PER E-MAIL

[redacted]
E-mail: [redacted]

Wageningen
University

DATUM
14 juni 2024

ONDERWERP
Besluit op uw verzoek om informatie

ONS KENMERK
2414978

POSTADRES
Postbus 9101
6700 HB

BEZOEKADRES
Wageningen Campus
Gebouw 104
Droevendaalsesteeg 4
6708 PB Wageningen

INTERNET
www.wur.nl

CONTACTPERSOON
[redacted]

E-MAIL
woo@wur.nl

Geachte [redacted]

Op 30 maart jl. hebben wij uw verzoek om informatie ontvangen betreffende bij of onder het college van bestuur van Wageningen University vallende datalekken.

Uw verzoek om informatie
Uw verzoek heeft specifiek betrekking op:

1) Alle in documenten vastgelegde communicatie over concrete gevallen van (vermeende) datalekken die zich in de periode van 01 januari 2020 t/m 31 december 2021 bij Wageningen University hebben voorgedaan. U noemt hierbij de volgende voorbeelden: een e-mail van een medewerker waarbij melding wordt gemaakt van een (vermeend) datalek, notulen van overleggen waarin (vermeende) datalekken worden besproken, meldingen aan de Autoriteit Persoonsgegevens, terugkoppeling van de Autoriteit Persoonsgegevens, melding naar persoon waarop het datalek ziet, een extern advies over een concreet (vermeend) datalek en het datalekregister;
2) Documenten ten aanzien van procedures en beleid ten aanzien van datalekken;
3) Audits ter voorkoming van datalekken.

Behandeling van uw verzoek
Per e-mail van 02 april jl. hebben wij de ontvangst van uw verzoek bevestigd. Op 08 april jl. hebben wij u onze interpretatie van de reikwijdte van uw verzoek voorgelegd en gevraagd of u de juistheid daarvan kon bevestigen. U heeft naar aanleiding daarvan verduidelijkt op welke informatie uw verzoek ziet. Op 08 april jl. hebben wij de ontvangst van uw reactie bevestigd.

Op 24 april jl. hebben wij per e-mail aangegeven naar alle waarschijnlijkheid twee weken extra nodig te hebben voor de behandeling van uw verzoek overeenkomstig met artikel 4.4. lid 2 Woo.

Naar aanleiding van uw verzoek hebben wij de informatie zoals hierboven beschreven opgevraagd binnen de organisatie van Wageningen University en vervolgens inhoudelijk getoetst op de aanwezigheid van wettelijke uitzonderingsgronden. Wij hebben informatie opgevraagd bij onze (corporate) privacy officers, de functionaris

gegevensbescherming en de chief information security officer. De reactie op de uitvraag hebben wij meegenomen in onze uiteindelijke besluitvorming.

Besluit
Het college van bestuur van Wageningen University besluit om uw verzoek om informatie gedeeltelijk te honoreren, waarbij wij de kaders van de Woo in acht nemen. Dit betekent dat wij de door u verzochte documenten verstrekken indien en voor zover Wageningen University die informatie onder zich heeft en indien en voor zover de uitzonderingsgronden van de Wet open overheid zich niet tegen openbaarmaking van deze informatie verzetten. Wij hebben in ieder document aangegeven op welke grond wij eventueel informatie hebben afgeschermd.

Toepassing van de uitzonderingsgronden
Niet alle informatie die aan uw verzoek voldoet kan openbaar worden gemaakt. Waar de bescherming van persoonlijke levenssfeer zwaarder weegt dan het algemeen belang van openbaarheid, is de uitzonderingsgrond van artikel 5.1 lid 2, aanhef en onder e van de Wet open overheid toegepast.

Concreet betekent dit dat in de documenten de namen van personen en hun contactgegevens, zoals e-mailadressen, telefoonnummers en specifieke kamernummers, zijn weggelakt. Het belang van openbaarmaking van die gegevens weegt naar het oordeel van het college van bestuur niet op tegen het belang bij bescherming en eerbiediging van de persoonlijke levenssfeer van de betrokken personen. De persoonsgegevens van personen die een openbare functie bij Wageningen University bekleden, voor zover deze gegevens relevant zijn binnen het bestek van dit informatieverzoek, zijn niet weggelakt.

Tevens is artikel 5.1. lid 2, aanhef en onder h op informatie waarbij het algemeen belang van de openbaarheid van informatie niet opweegt tegen het belang van de beveiliging van Wageningen University en het voorkomen van sabotage. Het openbaar maken van deze informatie kan de beveiliging van Wageningen University schaden.

Daarnaast is artikel 5.1 lid 5 van de Wet open overheid in een enkel geval toegepast op informatie waarbij het belang van openbaarmaking niet opweegt tegen het voorkomen van onevenredige benadeling van bij de aangelegenheid betrokken natuurlijke personen of rechtspersonen dan wel derden.

Informatie en termijn voor bezwaar
Wij vertrouwen erop u hiermee voldoende te hebben geïnformeerd. Indien u vragen heeft over dit besluit kunt u contact opnemen met onze woordvoerder Vincent Koperdraat, via vincent.koperdraat@wur.nl.

U kunt binnen zes weken na de dag waarop dit bekend is gemaakt een bezwaarschrift indienen. U dient in dat geval schriftelijk uw bezwaren te richten aan het college van bestuur van Wageningen University, Postbus 9101, 6700 HB Wageningen dan wel per e-mail gericht aan woo@wur.nl.

Hoogachtend,

[redacted]

Dr. ir. S. Heimovaara
Voorzitter college van bestuur
Wageningen University

PRIVACY/SECURITY INCIDENT – PROCES

Indien sprake is van een beveiligingsincident waar persoonsgegevens in het geding kunnen zijn wordt onderstaand proces gevolgd. Dit speelt onder andere bij dreigingen van buiten de organisatie (zoals ransomwaregevallen, phishing en hacks) en bij situaties waar door middel van een lek persoonsgegevens per ongeluk zijn gepubliceerd of anderszins (mogelijk) onrechtmatig verwerkt (denk aan: SQL-injectie gevoeligheden of open shares).

Toelichting

De melder dient het meldfomulier in te vullen dat hier beschikbaar is op intranet. De melder stuurt het ingevulde formulier naar servicedesk.it@wur.nl. De Servicedesk IT zendt het formulier door naar de corporate privacy officer (CPO) via privacy@wur.nl en de information security officer (ISO). Zodra vastgesteld is dat persoonsgegevens in het geding zin, schakelt de CPO de local privacy officer (LPO) in om samen met de melder, en eventuele andere betrokkenen onderzoek te doen naar het incident. De LPO houdt nauw contact met de CPO en informeert de CPO over de bevindingen. De CPO informeert de functionaris voor de gegevensbescherming (FG) en de ISO. De FG en CPO stellen vervolgens aan de hand van artikel 33 en 34 AVG en de richtsnoeren van de Autoriteit Persoonsgegevens (AP) vast of hier sprake is van een meldplichtig incident. Indien het incident gemeld moet worden bij de AP verzorgt de CPO die melding in afstemming met de FG. Indien het incident ook gemeld moet worden aan betrokkenen zal de FG dit escaleren naar het Privacy-Security Incident Response Team (PSIRT). Dit team bestaat uit de ISO, FG, de woordvoerder en situational eigenaar. Het PSIRT beslist vervolgens hoe en door wie het incident aan betrokkenen zal worden gemeld, waarbij qua inhoud in ieder geval voldaan moet zijn aan de eisen van artikel 34 lid 2 AVG. Bij een incident met een potentieel grote impact voor de organisatie, kan het PSIRT de behandeling van het incident escaleren naar het Crisis Management Team (CMT) en de raad van bestuur (RvB).

FORMULIER MELDING DATALEKKEN

In geval van een beveiligings~~security~~ incident waarbij ~~mogelijk~~ persoonsgegevens ~~verloren~~ betrokken zijn ~~gegaan~~ (ook als je dat niet zeker weet) gebruik je het datalekformulier om een melding te doen. ~~Dat dient binnen 48 uur na constatering van het incident te gebeuren.~~

Het is van belang dit formulier zo volledig en nauwkeurig mogelijk in te vullen. Op basis van dit formulier maakt de functionaris voor de gegevensbescherming (F-G) een afweging of het incident gemeld moet worden aan de Autoriteit Persoonsgegevens en/of betrokken personen.

Alle communicatie over dit incident met betrokkenen of toezichthouders dient vooraf afgestemd te worden met de F-G via 0317 of privacy@wur.nl.

FORMULIER

Contactgegevens melder	
Naam	5.1.2.e [redacted]
Functie	5.1.2.e [redacted]
E-mailadres	5.1.2.e [redacted] @wur.nl
Telefoonnummer	5.1.2.e [redacted]
Gegevens over het incident (omschrijving van het incident)	Ik werd er gisteren door een student attent op gemaakt dat ik mijn gehele OneDrive had gedeeld in een MS Teams groep met 30 studenten en 5 docenten. Ik heb geen idee hoe het gebeurd is, wanneer het gebeurd is, wie het gezien heeft, en of iemand er iets mee gedaan heeft. Ik heb na de melding (zondagmiddag) de melding zo snel als ik kon (zondagavond) verwijderd. Op de OneDrive staat gevoelige informatie: beoordelingsformulieren, reflectieverslagen, foto's enzovoort. Ook veel privégegevens (foto's e.d.)
Samenvatting van het incident	Per ongeluk minstens 24 uur lang maar mogelijk langer mijn OneDrive gedeeld in een MS Teams groep. Op de OneDrive staat privacygevoelige informatie.
Toelichting	*[wat is er gebeurd (diefstal of verlies van gegevens, malware/hack/DDoS, gegevens per ongeluk gepubliceerd, etc.), op welke manier (bijv. via internet, e-mail, aanval van buitenaf, etc.) en hoe is het incident ontdekt]*
Aard van het incident	Niet bekend
Toelichting	*[bijv. inzage door onbevoegden, gegevens gekopieerd/gedownload, wijzigingen aangebracht, gegevens verwijderd of vernietigd, diefstal van gegevens of nog niet bekend]*
Datum en tijdstip van het incident	Ontdekt 20.09.2020 19.21 na melding van student, ca. 2 uur later door mij verwijderd. Begintijdstip onbekend.
Toelichting	*[op welk moment of gedurende welke periode vond het incident plaats]*
Datum en tijdstip van ontdekking	Zie boven
Toelichting	*[wanneer is het incident ontdekt]*
Betrokkenen	Heel veel personen potentieel, onder meer beoordelingen bachelor theses van laatste 3 jaar en reflectieverslagen ACT en EUW. Thesis contracten, internship contracten.
Toelichting	*[van welke personen (medewerkers, studenten, proefpersonen etc) zijn gegevens betrokken bij het incident]*
Aantal betrokkenen	Mogelijk heeft niemand de gegevens ingezien.
Toelichting	*[eventueel een schatting van minimaal/maximaal aantal personen]*

Welke soorten persoonsgegevens (aankruisen)		Ja	Nee
	naam, adres, woonplaats (zakelijk en/of privé):	x	
	contactgegevens (telefoonnummer, e-mailadres, etc.):	x	
	geboortedatum en -plaats	x	
	nationaliteit	x	
	geslacht	x	
	identificatiegegevens (login, wachtwoord):		x
	financiële- of HRM-gegevens		x
	persoonsgebonden nummers (BSN, onderwijsnummer, etc.)		x
	strafrechtelijke gegevens (veroordelingen, berispingen, etc.)		x
	kopie paspoort		x
	kopie rijbewijs		x
	foto	x	
	medische gegevens		x
	godsdienst, politieke voorkeur, vakbondslidmaatschap		x
	anders, namelijk:		
Mogelijke gevolgen (aankruisen)		Ja	Nee
	stigmatisering of uitsluiting		x
	schade aan de gezondheid		x
	blootstelling aan (identiteits)fraude		x
	blootstelling aan spam of phishing		x
	anders, namelijk:		
Welke acties zijn genomen	Direct alles verwijderd		
Toelichting	*[beschrijving welke acties zijn getroffen om het incident te adresseren en om verdere incidenten te voorkomen]*		
Welke maatregelen zijn getroffen	Geen – maar mijn administratie is een ongeregeld zooitje dus het is lastig om dingen te vinden		
Toelichting	*[beschrijving en toelichting welke beveiligingsmaatregelen van toepassing zijn op de betrokken persoonsgegevens; zijn die bijv. versleuteld, gehasht, gepseudonimiseerd of anderszins ontoegankelijk gemaakt]*		
Internationale aspecten	Ja		
Toelichting	*[heeft het incident betrekking op personen in andere EER-landen [Europese Unie, Liechtenstein, Noorwegen of IJsland]:*		

Stuur dit formulier zo snel mogelijk~~, doch uiterlijk binnen 48 uur~~ na het constateren van een datalek naar **servicedesk.it@wur.nl**. ~~Dan wordt uw melding afgehandeld volgens het datalekkenprotocol.~~

Privacy

Van: Privacy
Verzonden: maandag 21 september 2020 15:28
Aan: Privacy ESG
CC: 5.1.2.e
Onderwerp: FW: Formulier datalekken.docx
Bijlagen: Formulier datalekken.docx

Categorieën: 5.1.2.e

Dag 5.1.2.e en 5.1.2.e,

Hierbij een melding van een datalek van ESG. Zouden jullie het volgende kunnen uitvragen om te bepalen of wij dit moeten melden bij de AP en misschien bij betrokkenen?

- Welke persoonsgegevens zijn precies gelekt? Met name welke gevoelige gegevens (ik zie bijv. beoordelingen, maar zijn die ook gedeeld met de studenten, kopietjes paspoort? Financiële gegevens?)?
- Kunnen we iets meer achterhalen over de periode waarbinnen de drive heeft opengestaan (in afstemming met IT)? Wanneer is de Teams-page aangemaakt?
- Kunnen wij vaststellen of onbevoegden de bestanden hebben geopend?
o Zo ja, hoe? Met logging (in afstemming met IT vast te stellen)?
- Kunnen wij uitsluiten dat sprake is van misbruik (bijv. door degenen die de files hebben geopend te laten verklaren deze te hebben vernietigd)?
- Hoe heeft deze actie kunnen gebeuren en hoe kunnen wij dergelijke situaties voorkomen.

Fijn als jullie hier morgen op terug te komen bij privacy@wur.nl. We kunnen natuurlijk ook even bellen.

Alvast dank en groeten,
5.1.2.e

Van: 5.1.2.e @wur.nl>
Verzonden: Monday, September 21, 2020 2:22 PM
Aan: Privacy <privacy@wur.nl>; Servicedesk IT <servicedesk.it@wur.nl>
Onderwerp: Formulier datalekken.docx

5.1.2.e
5.1.2.e
Environmental Systems Analysis group (ESA)
Wageningen University & Research
PO Box 47, 6700 AA, Wageningen
Wageningen Campus, Lumen building, 5.1.2.e
Visiting address: Droevendaalsesteeg 3, 6708 PB, Wageningen
Tel. 5.1.2.e

WAGENINGEN
UNIVERSITY & RESEARCH

www.esa.wur.nl

5.1.2.e

Van: 5.1.2.e
Verzonden: maandag 21 september 2020 15:19
Aan: Privacy
CC: 5.1.2.e
Onderwerp: RE: Formulier datalekken.docx

Ha 5.1.2.e

Allereerst voor jouw eigen achtergrond een korte schets van het afwegingskader. Daarna zal ik ingaan op de acties.

AFWEGINGSKADER
De vragen die wij moeten doorlopen zijn:

1. Betreft het hier een datalek in de zin van de AVG?
2. Zo ja, moeten wij dit datalek ook melden bij de AP?
3. Zo ja, moeten wij dit datalek ook melden bij betrokkenen?

Ad 1). Betreft het hier een datalek?

> Juridisch kader: artikel 4 sub 12 AVG: "inbreuk in verband met persoonsgegevens": een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens".

De AVG definieert een incident al snel als datalek. Met name daar waar sprake is van een vernietiging/verlies, wijziging (inbreuk op integriteit) of ongeoorloofde verstrekking/toegang van/tot persoonsgegevens.

Zoals gezegd, voor de meldingen over verloren telefoons/laptops doen wij meestal niets. Die zijn gelocked en verlies/diefstal kwalificeert niet als datalek, maar alleen als beveiligingsincident omdat wij kunnen uitsluiten dat sprake is van ongeoorloofde toegang.

In dit geval gaat het om een docent die kennelijk haar privédrive (met gevoelige data waaronder persoonsgegevens) inzichtelijk heeft gemaakt voor 30 studenten en 5 medewerkers. Dat kwalificeert als datalek in de zin van de AVG omdat onbevoegden kennis hebben kunnen nemen van de persoonsgegevens.

Ad 2). Moeten wij dit datalek melden aan de AP?

> Juridisch kader: artikel 33 lid 1 AVG: "Indien een inbreuk in verband met persoonsgegevens heeft plaatsgevonden, meldt de verwerkingsverantwoordelijke deze zonder onredelijke vertraging en, indien mogelijk, uiterlijk 72 uur nadat hij er kennis van heeft genomen, aan de overeenkomstig artikel 55 bevoegde toezichthoudende autoriteit, tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen (...)."

Voor de vraag of het waarschijnlijk is dat het datalek een risico inhoudt voor de rechten en vrijheden van natuurlijke personen moet met name gekeken worden: (i) welke (soorten) persoonsgegevens zijn precies gelekt; en (ii) leiden de aard en omvang van het incident tot (een kans op) nadelige gevolgen voor de betrokkenen (de personen wiens data is gelekt). Als wij een dergelijk risico niet waarschijnlijk achten (bijv. door een tweede beveiligingslaag, dichte logging of bevestiging van verwijdering) hoeven we het niet te melden.

Ad 3). Moeten wij dit datalek melden aan de betrokkenen?

> Juridisch kader: artikel 34 lid 1 AVG: Wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen,

deelt de verwerkingsverantwoordelijke de betrokkene de inbreuk in verband met persoonsgegevens onverwijld mee.

Voor de vraag of het datalek waarschijnlijk een hoog risico meebrengt voor de betrokkenen moet worden gekeken naar de aard van de gelekte gegevens en naar de aard en omvang van de inbreuk. Met name of misbruik van de gegevens waarschijnlijk kan leiden tot fysieke, materiële of immateriële schade voor de betrokkenen, zoals discriminatie, (identiteits-)fraude, financiële schade en reputatieschade.

IN DIT GEVAL
Het normale proces bij incidenten is dat de PO van de betreffende groep op de hoogte wordt gesteld van het incident om het uitzoekwerk te starten.

In dit geval is het sowieso een datalek in de zin van de AVG. Voor de vraag of wij dit moeten melden bij de AP (stap 2) en misschien bij betrokkenen (stap 3) zou ik met name willen weten:

- Welke persoonsgegevens zijn precies gelekt? Met name welke gevoelige gegevens (ik zie bijv. beoordelingen, maar zijn die ook gedeeld met de studenten, kopietjes paspoort? Financiële gegevens?)?
- Kunnen we iets meer achterhalen over de periode waarbinnen de drive heeft opengestaan (in afstemming met IT)? Wanneer is de Teams-page aangemaakt?
- Kunnen wij vaststellen of onbevoegden de bestanden hebben geopend?
    - Zo ja, hoe? Met logging (in afstemming met IT vast te stellen)?
- Kunnen wij uitsluiten dat sprake is van misbruik (bijv. door degenen die de files hebben geopend te laten verklaren deze te hebben vernietigd)?
- Hoe heeft deze actie kunnen gebeuren en hoe kunnen wij dergelijke situaties voorkomen.

Ik zou deze vragen aan 5.1.2.e en 5.1.2.e sturen (privacy.esg@wur.nl) en 5.1.2.e in de cc. met het verzoek daar morgen op terug te komen bij privacy@wur.nl. Ze kunnen ook even bellen.

Groet, 5.1.2.e

5.1.2.e
Corporate Governance & Legal Services

Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 5.1.2.e
www.wur.nl/disclaimer

Van: Privacy <privacy@wur.nl>
Verzonden: maandag 21 september 2020 14:33
Aan: 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
Onderwerp: FW: Formulier datalekken.docx

Dag 5.1.2.e en 5.1.2.e,

Ik stuur dit bericht naar jullie beiden door. Wat is de eerst te nemen stap en heb ik daar een rol in? Ik zit van 15.00 tot 17.00 uur in overleg. Als ik zie dat één van jullie belt, kan ik uit het overleg gaan.

Groeten, 5.1.2.e

Van: 5.1.2.e @wur.nl>
Verzonden: Monday, September 21, 2020 2:22 PM
Aan: Privacy <privacy@wur.nl>; Servicedesk IT <servicedesk.it@wur.nl>
Onderwerp: Formulier datalekken.docx

5.1.2.e
5.1.2.e

Environmental Systems Analysis group (ESA)
Wageningen University & Research
PO Box 47, 6700 AA, Wageningen
Wageningen Campus, Lumen building, 5.1.2.e
Visiting address: Droevendaalsesteeg 3, 6708 PB, Wageningen
Tel. 5.1.2.e

www.esa.wur.nl

Ontvangstbevestiging

Uw verzoek tot het indienen van een melding wordt in behandeling genomen.
U kunt de melding niet online raadplegen. Maak daarom een print voor uw eigen administratie. Doe dit voordat u deze pagina afsluit. Na het afsluiten van deze pagina zijn de gegevens die u heeft opgegeven niet meer beschikbaar. Onder het onderstaande meldingsnummer is de melding bekend bij de Autoriteit Persoonsgegevens. U heeft het meldingsnummer nodig om de melding aan te kunnen passen of in te kunnen trekken. Vermeld het meldingsnummer bij eventuele correspondentie met de Autoriteit Persoonsgegevens over de melding.

Tijdstip ontvangst	23-09-2020 16:53:28
Uniek nummer	5.1.2.e

0. Over deze melding

Gaat het om een nieuwe of bestaande melding?	Een nieuwe melding indienen
Op grond van welke wettelijke bepaling doet u deze melding?	Algemene verordening gegevensbescherming (AVG)

1. Contactgegevens en overige algemene informatie

1.1 Contactgegevens

Over welke organisatie of welk bedrijf gaat het?

Registratienummer bij de Kamer van Koophandel	09215846
Naam van het bedrijf of de organisatie	Wageningen University
Adres	Droevendaalsesteeg 4
Postcode	6708PB
Plaats	Wageningen
In welke sector is de organisatie of het bedrijf actief?	Onderwijs - Tertiair onderwijs

Wie meldt het datalek?

Naam	5.1.2.e
Functie	corporate privacy officer
E-mailadres	5.1.2.e @wur.nl
Telefoonnummer	5.1.2.e

Met wie kan de Autoriteit Persoonsgegevens contact opnemen voor nadere informatie over de melding?

De melder is contactpersoon	Nee
Naam contactpersoon	5.1.2.e
Functie contactpersoon	functionaris gegevensbescherming
E-mailadres contactpersoon	dpo@wur.nl
Telefoonnummer contactpersoon	5.1.2.e

1.2 Betrokkenheid andere organisatie

Was er een andere organisatie betrokken bij de inbreuk?	Nee

2. Tijdlijn

Exacte datum waarop de inbreuk was, indien bekend	20-09-2020
Startdatum van de periode waarbinnen de inbreuk was	16-09-2020
Einddatum van de periode waarbinnen de inbreuk was	20-09-2020
Duurt de inbreuk op dit moment nog voort?	Nee
Wanneer werd de inbreuk ontdekt?	20-09-2020

3. Gegevens over het datalek

3.1 Aard van de inbreuk

Inbreuk op de vertrouwelijkheid van de gegevens	Ja
Inbreuk op de integriteit van de gegevens	Nee

Inbreuk op de beschikbaarheid van de gegevens	Nee

3.2 Aard van het incident

Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest?	Persoonsgegevens per ongeluk gepubliceerd

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest

Op 20 september jl. om 19.21 is een van onze docenten er door een student op geattendeerd dat de docent haar cloudopslagomgeving (OneDrive) onbedoeld had gedeeld in een Microsoft Teams-groep, waar 30 studenten en 5 docenten van uitmaken. Op de OneDrive-omgeving stond werkgerelateerde informatie, waaronder enkele (onderwijsgerelateerde) beoordelingsformulieren en reflectieverslagen, en privéinformatie. Dit was ingedeeld in een rootfolder en submappen. In de rootfolder stond een beperkt aantal bestanden met persoonsgegevens. In de submappen stond (in omvang) een aanzienlijk groter aantal bestanden. Voor zover nu bekend is alleen de rootfolder gedeeld met de studenten en docenten. Direct na de melding door de student is het delen beëindigd. Het is op dit moment nog niet vast te stellen of daadwerkelijk toegang is verkregen tot de privébestanden, zodat de precieze omvang en impact van het incident nog niet volledig kan worden beoordeeld.

4. Persoonsgegevens die betrokken zijn bij het datalek

4.1 Persoonsgegevens in het algemeen

Naam	Ja
Geslacht, geboortedatum en/of leeftijd	Ja
Burgerservicenummer (BSN)	Nee
Contactgegevens	Ja
Toegangs- of identificatiegegevens	Nee
Financiële gegevens	Nee
(Kopieën van) paspoorten of andere legitimatiebewijzen	Nee
Locatiegegevens	Nee

Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen	Nee
Onbekend / anders, namelijk:	foto's

4.2 Bijzondere categorieën van persoonsgegevens

Persoonsgegevens waaruit iemands ras of etnische afkomst blijkt	Nee
Persoonsgegevens waaruit iemands politieke opvattingen blijken	Nee
Persoonsgegevens waaruit iemands religieuze of levensbeschouwelijke overtuigingen blijken	Nee
Persoonsgegevens waaruit iemands lidmaatschap van een vakbond blijkt	Nee
Gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid	Nee
Gegevens over iemands gezondheid	Nee
Genetische gegevens	Nee
Biometrische gegevens	Nee

4.3 Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords ("gegevensregisters") zijn getroffen door de inbreuk	1

5. De groep mensen van wie persoonsgegevens betrokken zijn bij het datalek

Werknemers	Ja
Klanten (huidig en potentieel)	Nee
Leerlingen of studenten	Ja
Patiënten	Nee
Minderjarigen	Nee

Personen uit kwetsbare groepen	Nee

Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk.
Met name de docent zelf (waar het haar privégegevens betreft) en studenten. Het precieze aantal studenten is nog niet bekend omdat de omvang nog niet kan worden bepaald.

Van minimaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?	3
Van maximaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?	3

6. Maatregelen die zijn getroffen voordat het datalek plaatsvond

Waren de persoonsgegevens op het moment dat de inbreuk zich voordeed versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk voor onbevoegden?	Deels, namelijk:
Als de persoonsgegevens deels onbegrijpelijk of ontoegankelijk waren, om welk deel gaat dat dan?	Informatie in sub-mappen

Als de persoonsgegevens geheel of deels onbegrijpelijk of ontoegankelijk waren gemaakt, op welke manier is dit dan gebeurd?
Naar de huidige stand van de informatie is alleen de 'root folder' gedeeld en de submappen op de OneDrive-omgeving niet. De deelnemers in de MS Team-omgeving hadden geen autorisatie/toegang tot de onderliggende mappen.

7. Gevolgen van het datalek

7.1 Gevolgen van de inbreuk op de vertrouwelijkheid, de integriteit en/of de beschikbaarheid van de gegevens.

Onbevoegden hebben kennis kunnen nemen van de gegevens	Ja

De gegevens kunnen op een onbehoorlijke of onrechtmatige manier worden misbruikt	Nee
Er worden binnen uw eigen organisatie mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens gebruikt	Nee
Er worden mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens hergebruikt voor andere doeleinden of doorgegeven aan andere organisaties	Nee
Een essentiële dienst kan tijdelijk niet meer worden verleend aan de betrokkenen	Nee
Een essentiële dienst kan permanent niet meer worden verleend aan de betrokkenen	Nee

7.2 Lichamelijke, materiële en immateriële schade voor de betrokkenen

Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkenen?

Discriminatie	Nee
Identiteitsdiefstal of -fraude	Nee
Financiële verliezen	Nee
Reputatieschade	Ja
Verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens	Nee
Ongeoorloofde ongedaanmaking van pseudonimisering	Nee
Betrokkenen kunnen hun rechten en vrijheden niet uitoefenen	Nee
Betrokkenen worden verhinderd controle over hun persoonsgegevens uit te oefenen	Nee

Andere gevolgen, namelijk:
Mogelijk zijn enkele beoordelingsverslagen en -formulieren inzichtelijk geweest. Dit betreft een persoonlijke beoordeling en niet de uiteindelijke cijferregistratie (manipulatie van de administratie is niet aan de orde).

Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkenen	1. Verwaarloosbaar

8. Vervolgacties naar aanleiding van het datalek

8.1 Informeren van de betrokkenen

Heeft u het datalek gemeld aan de betrokkenen of bent u van plan dat te gaan doen?	Nog niet bekend
Hoeveel betrokkenen heeft u geïnformeerd of gaat u informeren?	3
Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken om de betrokkenen te informeren?	n.n.b.

8.2 Maatregelen om de inbreuk aan te pakken

Welke technische en organisatorische maatregelen heeft uw organisatie getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?
Het delen is direct gestaakt. Momenteel wordt onderzocht hoe het proces van delen werkt en of daad een extra waarschuwing voor kan worden gegeven.

8.3 Internationale aspecten

Heeft de inbreuk zich voorgedaan in een grensoverschrijdende gegevensverwerking, en is de AP voor deze verwerking de leidende toezichthouder?	Nee
Heeft uw organisatie of bedrijf, het datalek gemeld bij privacytoezichthouders in een of meer	Nee

andere EU-landen, of gaat u dat nog doen?	
Heeft uw organisatie of bedrijf, het datalek gemeld bij Europese toezichthouders op andere meldplichten, of gaat u dat nog doen?	Nee

9. Overig

Is naar uw mening deze melding compleet?	Nee, er komt later een vervolgmelding met aanvullende informatie over deze inbreuk

Privacy

Van: Privacy
Verzonden: maandag 9 november 2020 16:57
Aan: 5.1.2.e
CC: Privacy ESG
Onderwerp: Intrekken datalek
Bijlagen: 20201109_intrekken_open_OneDrive.pdf

Ha 5.1.2.e,

Hierbij de ingetrokken datalekmelding van Jana Verboom (die haar privé OneDrive had gedeeld in een MS Teams omgeving). Nader onderzoek door 5.1.2.e wijst uit dat er geen sprake is geweest van onrechtmatige verwerking.

Vriendelijke groet,
5.1.2.e

5.1.2.e

Van: 5.1.2.e
Verzonden: maandag 9 november 2020 16:02
Aan: Privacy ESG
CC: 5.1.2.e
Onderwerp: RE: Vermeend datalek 5.1.2.e ESG

Dank je, 5.1.2.e. Lijkt mij een goede conclusie. Ik zal de melding intrekken.

5.1.2.e
Corporate Governance & Legal Services

Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e, Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 5.1.2.e
www.wur.nl/disclaimer

Van: Privacy ESG <privacy.esg@wur.nl>
Verzonden: maandag 9 november 2020 14:51
Aan: 5.1.2.e @wur.nl>
CC: 5.1.2.e @wur.nl>
Onderwerp: Vermeend datalek 5.1.2.e ESG

Hallo 5.1.2.e,
Zoals beloofd hierbij de relevante mailwisseling mbt 5.1.2.e. Er is geen reden aan te nemen dat er een datalek is geweest.
Groet, 5.1.2.e

5.1.2.e
Privacy Officer Social Sciences Group / Environmental Sciences Group
Wageningen University & Research
5.1.2.e, continues to mobile
5.1.2.e @wur.nl

I am available on Monday, Tuesday and Thursday.
Meer privacy informatie vind je hier

Privacy

Van: 5.1.2.e
Verzonden: woensdag 23 september 2020 17:46
Aan: 5.1.2.e Privacy; Functionarisgegevensbescherming
CC: Privacy ESG; 5.1.2.e
Onderwerp: Security incident ESG

Categorieën: 5.1.2.e

Goedemiddag 5.1.2.e

Vanmiddag is er bij de Autoriteit Persoonsgegevens een voorlopige melding gedaan van een potentieel datalek. Deze melding is gedaan, omdat we in ons – 5.1.2.e en ik – onderzoek nog onvoldoende antwoorden hebben waarbij we kunnen uitsluiten dat de betreffende data niet is ingezien.

Resumé van de casus en acties.
Op de Onedrive van een ESG lecturer hebben een aantal mappen met daarin een groot aantal documenten open gestaan voor een aantal collega's en studenten. Dit is waargenomen door 2 studenten, die dit bij haar gemeld hebben. Dit is door de betreffende lecturer zondag gedeeld met de WUR, waarna een incident is aangemaakt bij IT. Inmiddels heeft 5.1.2.e vanuit de studenten en de lecturer een mondelinge verklaring dat er door hen niets met de bestanden is gedaan. De lecturer heeft de betreffende mappen inmiddels ontoegankelijk gemaakt. Ondertussen is er een verzoek gedaan om een schriftelijke verklaring te krijgen van de studenten, waarmee we bewijslast hebben dat zij niets hebben ingezien (of gewijzigd).

Bij IT is het verzoek gedaan om de logfiles in te zien, zodat we vanuit deze kant ook kunnen uitsluiten dat derde toegang hebben gehad tot de bestanden en/of de bestanden zijn gemanipuleerd. Dit laatste is belangrijk, omdat er bestanden bij zitten met beoordelingen van studenten. Dit kost helaas extra tijd vanwege een rechtenkwestie bij IT. Hier heb ik nauw contact over met het betreffende team binnen IT, zodat dit zo snel mogelijk opgelost wordt.

Wij verwachten momenteel dat het risico voor betrokkenen beperkt is gebleven, maar moeten de resultaten van het onderzoek afwachten om tot een definitieve conclusie te komen. Omdat de 72 uur voor het melden van een datalek verstreken zijn, hebben we een voorlopige melding gedaan bij de Autoriteit Persoonsgegevens.

With kind regards,

5.1.2.e
Privacy Officer
Wageningen University & Research
Education & Student Affairs, Social Sciences Group,
Environmental Sciences Group & Agrotechnology & Food Sciences Group
PO Box 9100, 6700 HA Wageningen
Wageningen Campus, Atlas Building, Droevendaalsesteeg 4, 6708 PB Wageningen
5.1.2.e

Privacy

Van: Privacy ESG
Verzonden: woensdag 28 oktober 2020 12:10
Aan: Privacy; 5.1.2.e
CC: Functionarisgegevensbescherming
Onderwerp: RE: Update security incident

Hallo 5.1.2.e,
Ja dat doe ik. Ik meen dat 5.1.2.e nog iets wilde checken, maar ik heb inmiddels gevraagd of dat nog open staat. Wordt vervolgd...
Groet, 5.1.2.e

5.1.2.e
Privacy Officer Social Sciences Group / Environmental Sciences Group
Wageningen University & Research
5.1.2.e, continues to mobile
5.1.2.e @wur.nl

I am available on Monday, Tuesday and Thursday.
Meer privacy informatie vind je hier

From: Privacy <privacy@wur.nl>
Sent: dinsdag 27 oktober 2020 19:55
To: Privacy ESG <privacy.esg@wur.nl>; 5.1.2.e @wur.nl>
Cc: Functionarisgegevensbescherming <functionarisgegevensbescherming@wur.nl>
Subject: RE: Update security incident

Ha 5.1.2.e,

Wellicht is dit een beetje naar de achtergrond verschoven, maar het is belangrijk dit incident finaal af te wikkelen (en hopelijk af te melden bij de AP). Kun jij mij deze week berichten over hoe verder te gaan?

Groet, 5.1.2.e

Van: Privacy ESG <privacy.esg@wur.nl>
Verzonden: dinsdag 6 oktober 2020 13:48
Aan: Privacy <privacy@wur.nl>; 5.1.2.e @wur.nl>
CC: Functionarisgegevensbescherming <functionarisgegevensbescherming@wur.nl>
Onderwerp: RE: Update security incident

Hallo 5.1.2.e

We zijn er bijna :) 5.1.2.e heeft de logfiles bekeken en de laatste vragen zijn vandaag naar 5.1.2.e gestuurd ter beantwoording.
Als de antwoorden binnen zijn kunnen we deze beoordelen en het incident afronden.

Groet, 5.1.2.e

5.1.2.e
Privacy Officer Social Sciences Group / Environmental Sciences Group
Wageningen University & Research
5.1.2.e, continues to mobile
5.1.2.e @wur.nl

I am available on Monday, Tuesday and Thursday.
Meer privacy informatie vind je hier

From: Privacy <privacy@wur.nl>
Sent: woensdag 30 september 2020 14:37
To: Privacy ESG <privacy.esg@wur.nl>; 5.1.2.e @wur.nl>
Cc: Privacy <privacy@wur.nl>; Functionarisgegevensbescherming <functionarisgegevensbescherming@wur.nl>
Subject: RE: Update security incident

Ha 5.1.2.e

Kunnen jullie inmiddels een wat meer definitieve terugkoppeling geven over het incident? Of een termijn waarbinnen wij het incident finaal kunnen afwikkelen?

Groet, 5.1.2.e

Van: 5.1.2.e @wur.nl>
Verzonden: donderdag 24 september 2020 16:43
Aan: Privacy <privacy@wur.nl>; Functionarisgegevensbescherming <functionarisgegevensbescherming@wur.nl>; 5.1.2.e @wur.nl>
CC: Privacy ESG <privacy.esg@wur.nl>; 5.1.2.e @wur.nl>
Onderwerp: Update security incident

Goedemiddag allen,

Inmiddels zijn de eerste logbestanden aangeleverd. Hier moeten nog wel dingen gecheckt worden, maar eerste indicatie ziet er positief uit. Ook is gevraagd om een logging over een periode van 30 dagen. Er is met 1 non WUR e-mailadres ingelogd. Dit moeten we nog verifiëren als zijnde het account van 5.1.2.e. Mocht dat positief zijn, dan kunnen we redelijkerwijs uitsluiten dat derden de bestanden hebben geopend.

Daarnaast is 5.1.2.e nog bezig met een verklaring van de studenten die dit voorval bij 5.1.2.e gemeld hebben.

Al met al verwachten we het onderzoek naar dit incident op korte termijn te kunnen sluiten. De verwachting op dit moment is dat er geen reden is om aan te nemen dat de bestanden door derden zijn ingezien of bewerkt. Na bovenstaande stappen kunnen we tot een definitieve conclusie komen.

With kind regards,

5.1.2.e
Privacy Officer
Wageningen University & Research
Education & Student Affairs, Social Sciences Group,
Environmental Sciences Group & Agrotechnology & Food Sciences Group
PO Box 9100, 6700 HA Wageningen
Wageningen Campus, Atlas Building, Droevendaalsesteeg 4, 6708 PB Wageningen
5.1.2.e

Ontvangstbevestiging

Uw verzoek tot het intrekken van een melding is succesvol verstuurd. Als uw verzoek niet meteen kan worden verwerkt, bijvoorbeeld omdat het meldingsnummer dat u heeft opgegeven niet bekend is bij de Autoriteit Persoonsgegevens, dan ontvangt u daarover zo spoedig mogelijk bericht.
U kunt de melding niet online raadplegen. Maak daarom een print voor uw eigen administratie. Doe dit voordat u deze pagina afsluit. Na het afsluiten van deze pagina zijn de gegevens die u heeft opgegeven niet meer beschikbaar. Onder het onderstaande meldingsnummer is de melding bekend bij de Autoriteit Persoonsgegevens. U heeft het meldingsnummer nodig om de melding aan te kunnen passen of in te kunnen trekken. Vermeld het meldingsnummer bij eventuele correspondentie met de Autoriteit Persoonsgegevens over de melding.

Tijdstip ontvangst	09-11-2020 16:55:21

0. Over deze melding

Gaat het om een nieuwe of bestaande melding?	
Wat is het meldingsnummer van de oorspronkelijke melding?	5.1.2.e
Wat is de reden van intrekking?	Nader onderzoek (logbestanden en persoonlijke gesprekken) heeft uitgewezen dat onbevoegden geen toegang hebben gehad tot de bestanden van de betrokken medewerker.

1. Contactgegevens en overige algemene informatie

1.1 Contactgegevens

Over welke organisatie of welk bedrijf gaat het?

Naam van het bedrijf of de organisatie	Wageningen University

Wie meldt het datalek?

Naam	5.1.2.e
Functie	corporate privacy officer
E-mailadres	privacy@wur.nl
Telefoonnummer	5.1.2.e

FORMULIER MELDING DATALEKKEN

In geval van een beveiligings~~security~~ incident waarbij ~~mogelijk~~ persoonsgegevens ~~verloren~~ betrokken zijn ~~gegaan~~ (ook als je dat niet zeker weet) gebruik je het datalekformulier om een melding te doen. ~~Dat dient binnen 48 uur na constatering van het incident te gebeuren.~~

Het is van belang dit formulier zo volledig en nauwkeurig mogelijk in te vullen. Op basis van dit formulier maakt de functionaris voor de gegevensbescherming (F-G) een afweging of het incident gemeld moet worden aan de Autoriteit Persoonsgegevens en/of betrokken personen.

Alle communicatie over dit incident met betrokkenen of toezichthouders dient vooraf afgestemd te worden met de F-G via 0317 of privacy@wur.nl.

FORMULIER

Contactgegevens melder			
Naam	5.1.2.e		
Functie	5.1.2.e		
E-mailadres	5.1.2.e @wur.nl		
Telefoonnummer	5.1.2.e		
Gegevens over het incident (omschrijving van het incident)	Microsoft Stream is out-of-the-box met default instellingen beschikbaar gesteld voor WUR. Het is gebleken dat opgenomen video's standaard voor "Everyone in your company" te zien zou zijn. Deze instelling staat nu op "Specific groups and people" (de enige andere optie).		
Samenvatting van het incident	Zie hierboven		
Toelichting	*De video opname kan onbedoeld beschikbaar komen voor andere WUR medewerkers die niet deelgenomen hebben aan de meeting.~~[wat is er gebeurd (diefstal of verlies van gegevens, malware/hack/DDoS, gegevens per ongeluk gepubliceerd, etc.), op welke manier (bijv. via internet, e-mail, aanval van buitenaf, etc.) en hoe is het incident ontdekt]~~*		
Aard van het incident			
Toelichting	Onbedoelde toegang tot een video opname*~~[bijv. inzage door onbevoegden, gegevens gekopieerd/gedownload, wijzigingen aangebracht, gegevens verwijderd of vernietigd, diefstal van gegevens of nog niet bekend]~~*		
Datum en tijdstip van het incident	Exacte datum van incident is onbekend. Dit incident is via Security coördinator gemeld bij de interne leverancier van de dienst.		
Toelichting	*[op welk moment of gedurende welke periode vond het incident plaats]*		
Datum en tijdstip van ontdekking	Woe 22/04/2020		
Toelichting	*~~[wanneer is het incident ontdekt]~~onbekend*		
Betrokkenen	Security coördinator en 5.1.2.e		
Toelichting	*~~[van welke personen (medewerkers, studenten, proefpersonen etc) zijn gegevens betrokken bij het incident]~~onbekend*		
Aantal betrokkenen	onbekend		
Toelichting	*~~[eventueel een schatting van minimaal/maximaal aantal personen]~~onbekend*		
Welke soorten persoonsgegevens (aankruisen)		Ja	Nee
	naam, adres, woonplaats (zakelijk en/of privé):		x
	contactgegevens (telefoonnummer, e-mailadres, etc.):	x	

	geboortedatum en -plaats		x
	nationaliteit		x
	geslacht		x
	identificatiegegevens (login, wachtwoord):		x
	financiële- of HRM-gegevens		x
	persoonsgebonden nummers (BSN, onderwijsnummer, etc.)		x
	strafrechtelijke gegevens (veroordelingen, berispingen, etc.)		x
	kopie paspoort		x
	kopie rijbewijs		x
	foto	x	
	medische gegevens		x
	godsdienst, politieke voorkeur, vakbondslidmaatschap		x
	anders, namelijk:		
Mogelijke gevolgen (aankruisen)		Ja	Nee
	stigmatisering of uitsluiting		x
	schade aan de gezondheid		x
	blootstelling aan (identiteits)fraude		x
	blootstelling aan spam of phishing		x
	anders, namelijk:		
Welke acties zijn genomen	Er is een configuratie wijziging doorgevoerd om dergelijke onbedoelde delen van video opname te verhinderen.		
Toelichting	~~*[beschrijving welke acties zijn getroffen om het incident te adresseren en om verdere incidenten te voorkomen]*~~*nvt*		
Welke maatregelen zijn getroffen	Zie hierboven		
Toelichting	~~*[beschrijving en toelichting welke beveiligingsmaatregelen van toepassing zijn op de betrokken persoonsgegevens; zijn die bijv. versleuteld, gehasht, gepseudonimiseerd of anderszins ontoegankelijk gemaakt]*~~*nvt*		
Internationale aspecten	nvt		
Toelichting	~~*[heeft het incident betrekking op personen in andere EER-landen [Europese Unie, Liechtenstein, Noorwegen of IJsland]:*~~*nee*		

Stuur dit formulier zo snel mogelijk~~, doch uiterlijk binnen 48 uur~~ na het constateren van een datalek naar **servicedesk.it@wur.nl**. ~~Dan wordt uw melding afgehandeld volgens het datalekkenprotocol.~~

Privacy

Van: Servicedesk IT
Verzonden: maandag 25 mei 2020 10:20
Aan: 5.1.2.e Privacy
Onderwerp: Datalek formulier invullen nav mailbox hack 14/5
Bijlagen: Formulier datalekken WUR.docx

Urgentie: Hoog

Goedemorgen 5.1.2.e,

Zoals telefonisch besproken, moet bijgevoegd datalek formulier ingevuld worden naar aanleiding van jouw mailbox hack op 14 of 15 mei. Graag bijgevoegd formulier zsm invullen en sturen naar privacy@wur.nl

Onderstaande informatie is tbv Privacy:

Op 14 mei heeft 5.1.2.e phishing mails ontvangen en bij een van deze mails heeft ze waarschijnlijk het WUR wachtwoord ingevuld omdat deze site leek op een Microsoft website.
(analyse van deze eerste mail kan hier bekeken worden: https://app.any.run/tasks/a1f03245-df65-4313-b161-3ce77f876f7f)

Vanaf 15 mei zijn er vervolgens tot en met vandaag diverse andere phishing mails uit gestuurd vanaf het wur mailadres van 5.1.2.e Geen van deze adressen lijken op contacten van 5.1.2.e

We hebben zojuist het wachtwoord gereset in een compleet nieuw wachtwoord. Er waren geen bestanden door de hacker in OneDrive aangemaakt en ook was er geen forward rule van mails aangemaakt in Outlook en/of webmail.

Enkele voorbeelden van verzonden mails na de hack:

IT Service [redacted]

AN Automated NOREPIY <alli@corperatassist.com>
To [redacted]

This message was sent with High importance.

AUDIO3057-39121.htm
8 KB

Microsoft

Dear [redacted]

Your caller left you a Voice Message.

From: 902382938
Duration: 0.59 Sec

Time: 06:45

Download the above attachment to listen

Delivery for [redacted]

FORMULIER MELDING DATALEKKEN

In geval van een security incident waarbij mogelijk persoonsgegevens verloren zijn gegaan (ook als je dat niet zeker weet) gebruik je het datalekformulier om een melding te doen. Dat dient binnen 48 uur na constatering van het incident te gebeuren.

Contactgegevens melder			
Naam	5.1.2.e		
Functie	5.1.2.e , Wageningen University & Research		
E-mailadres	5.1.2.e @wur.nl		
Telefoonnummer	5.1.2.e		
Gegevens over het incident (omschrijving van het incident)	Phishing mail has been send from my mail adress		
Samenvatting van het incident	Phishing mail has been send from my mail adress and the Servicedesk IT removed the rule in my outlook that has been sending these phishing mails		
Toelichting	*The Servicedesk found out that* Phishing mail has been send from my mail adress		
Aard van het incident	Phishing mail		
Toelichting	*Unknown*		
Datum en tijdstip van het incident	23-07-2020 in the morning		
Toelichting	*In the morning*		
Datum en tijdstip van ontdekking	23-07-2020 at 14:00		
Toelichting	*23-07-2020 at 14:00*		
Betrokkenen	Unknown		
Toelichting	*Unknown*		
Aantal betrokkenen	*Unknown*		
Toelichting	*[eventueel een schatting van minimaal/maximaal aantal personen]*		
Welke soorten persoonsgegevens (aankruisen)		Ja	Nee
	naam, adres, woonplaats (zakelijk en/of privé):		
	contactgegevens (telefoonnummer, e-mailadres, etc.):		
	geboortedatum en -plaats		
	nationaliteit		
	geslacht		
	identificatiegegevens (login, wachtwoord):		
	financiële- of HRM-gegevens		

	persoonsgebonden nummers (BSN, onderwijsnummer, etc.)		
	strafrechtelijke gegevens (veroordelingen, berispingen, etc.)		
	kopie paspoort		
	kopie rijbewijs		
	foto		
	medische gegevens		
	godsdienst, politieke voorkeur, vakbondslidmaatschap		
	anders, namelijk: *Unknown*		
Mogelijke gevolgen (aankruisen)		Ja	Nee
	stigmatisering of uitsluiting		
	schade aan de gezondheid		
	blootstelling aan (identiteits)fraude		
	blootstelling aan spam of phishing		
	anders, namelijk: *Unknown*		
Welke acties zijn genomen			
Toelichting	*[beschrijving welke acties zijn getroffen om het incident te adresseren en om verdere incidenten te voorkomen]*		
Welke maatregelen zijn getroffen	The Servicedesk IT removed the rule in your outlook that has been sending these phishing mails. I reset my password.		
Toelichting	*Unknown*		
Internationale aspecten	Unknown		
Toelichting	Unknown		

Stuur dit formulier zo snel mogelijk, doch uiterlijk binnen 48 uur na het constateren van een datalek naar **servicedesk.it@wur.nl**. Dan wordt uw melding afgehandeld volgens het datalekkenprotocol.

Privacy

Van: 5.1.2.e
Verzonden: dinsdag 19 mei 2020 10:15
Aan: Privacy
CC: 5.1.2.e
Onderwerp: Mogelijk datalek AFSG

Urgentie: Hoog

Hoi 5.1.2.e

Zie onderstaande mailwisseling ter informatie. 5.1.2.e heeft gelijk dat dit een klassiek datalek is.

Ik ga 5.1.2.e adviseren om het gebruik van CC zoveel mogelijk te vermijden (tenzij het uitsluitend om WUR-mailadressen gaat en het handig is dat de collega's onderling kunnen zien wie er uitgenodigd is).

Moeten wij nog stappen ondernemen richting de persoon van Unilever die hierin ook meegenomen is?

Met vriendelijke groet, 5.1.2.e

****
5.1.2.e I Privacy Officer / 5.1.2.e

T: 5.1.2.e
E-mail 5.1.2.e @wur.nl ***Ik ben niet aanwezig: woensdag NM en vrijdag***
E-mail privacy: privacy.afsg@wur.nl

Input nodig m.b.t. privacy binnen WUR? Klik hier voor meer informatie en templates

---

From: 5.1.2.e
Sent: dinsdag 19 mei 2020 10:06
To: 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
Subject: RE: Mutaties ivm Corona

Hoi 5.1.2.e

Ik snap je punt en zal 5.1.2.e benaderen om advies hierover te geven.

Nu gaat het vooral om mailadressen van WUR en is dat op zich niet zo spannend (niet echt een datalek), maar dat er ook een externe bij zit maakt het al anders.

Groet, 5.1.2.e

From: 5.1.2.e
Sent: dinsdag 19 mei 2020 10:01
To: 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
Subject: FW: Mutaties ivm Corona

Hi 5.1.2.e

Onderstaande mail van [redacted] is overigens een klassiek datalek volgens mij. Mailadressen niet in de bcc en er staat een extern-adres tussen...

Grt [redacted]

From: [redacted]
Sent: Monday, May 18, 2020 1:19 PM
To: [redacted]@wur.nl>; [redacted]@wur.nl>
Cc: [redacted]@wur.nl>
Subject: FW: Mutaties ivm Corona

Hallo [redacted] en [redacted]
Ter info onderstaande procedure.
De directie is op de hoogte en betrokken bij het afwegingskader.

Grt [redacted]

From: [redacted]
Sent: dinsdag 12 mei 2020 16:51
To: [redacted]@wur.nl>; [redacted]@unilever.com' [redacted]@unilever.com>; [redacted]@wur.nl>
Cc: [redacted]@wur.nl>; [redacted]@wur.nl>; [redacted]@wur.nl>; [redacted]@wur.nl>; [redacted]@wur.nl>; [redacted]@wur.nl>; [redacted]@wur.nl>; [redacted]@wur.nl>; [redacted]@wur.nl>; [redacted]@wur.nl>; [redacted]@wur.nl>; [redacted]@wur.nl>; [redacted]@wur.nl>; [redacted]@wur.nl>; [redacted]@wur.nl>; [redacted]@wur.nl>; [redacted]

5.1.2.e @wur.nl>;5.1.2.e @wur.nl>;5.1.2.e @wur.nl>;5.1.2.e @wur.nl>;5.1.2.e @wur.nl>;5.1.2.e @wur.nl>;5.1.2.e @wur.nl>
Subject: Mutaties ivm Corona

Beste AFSG-projectleiders,

Een aantal PPS-en heeft te maken met effecten van de Corona-crisis. Dat kan variëren in vertraging in de uitvoering tot wegvallende bijdrage van private partners.
TKI-A&F heeft in overleg met de algemeen directeuren van de kenniseenheden een procedure ontwikkeld om corona-effecten aan te melden.

In het bijgevoegde afwegingskader staat de procedure omschreven. Het bijgevoegde mutatieformulier kun je gebruiken om te beschrijven wat er aan de hand is binnen jouw project. Belangrijk is dat je daarbij gebruik maakt van het afwegingskader en dat je dit afstemt met jouw leidinggevende en de WR-themasecretaris (BU-manager of hoogleraar).

Lever het mutatieformulier uiterlijk 25 mei in bij 5.1.2.e . Zet jouw leidinggevende (BU-manager of hoogleraar) in de cc zodat wij kunnen zien dat hij/zij geïnformeerd is.

Als jouw project nog (geen) effecten ondervindt van de Corona-crisis hoef je nu niets te doen.
Bij vragen kun je bij ons terecht.

Al vast bedankt voor jullie medewerking!

Hartelijke groeten
5.1.2.e en 5.1.2.e
5.1.2.e AFSG

From: 5.1.2.e
Sent: vrijdag 8 mei 2020 16:12
To: 5.1.2.e @wur.nl>;5.1.2.e @wur.nl>;5.1.2.e @wur.nl>;5.1.2.e @wur.nl>;5.1.2.e @wur.nl>;5.1.2.e @wur.nl>;5.1.2.e @wur.nl>;5.1.2.e @wur.nl>;5.1.2.e @wur.nl>; Topsector-PSG <tss.psg@wur.nl>
Cc: 5.1.2.e @wur.nl>
Subject: Mutaties ivm Corona

Beste Topsectorsecretarissen,

In de bijlage stuur ik jullie het afwegingskader en het aangepaste mutatieformulier voor de mutaties in verband met Corona maatregelen. In dit afwegingskader staat ook het proces aangegeven. Belangrijke elementen binnen dit afwegingskader zijn dat Business Unit Manager en Thema secretarissen zijn betrokken bij de beoordeling van de mutaties ivm Corona.

De belangrijkste stappen zijn

- Vanaf 8 mei uitzetten van mutatieformulieren bij projectleiders met de vraag deze in te vullen indien er wijzigingen zijn die veroorzaakt zijn door de Corona maatregelen.
- Tot 25 mei verzamelen mutatie formulieren en interne toetsing door projectleider bij themasecretaris en BUM. Het is de taak van de topsectorsecretaris om na te gaan of dit is gebeurd en de mutatieformulieren op de share te zetten in deze speciaal daarvoor aangemaakte map Mutatieformulieren Corona (de titel van het bestand altijd beginnen met de projectcode). De projecten kunnen worden geregistreerd in het document 'aanvraag mutaties Corona' op de share. (Kolom A t/m I)
- Op 27 mei zal de complete lijst met aanvragen intern worden beoordeeld.
- 1 juni bespreking en accordering WR, TKI en LNV.
- Daarna verwerking in de moedertabel.

Ik hoop dat deze procedure werkbaar is. Mochten projecten niet voor 25 mei in staat zijn een mutatieformulier in te leveren dan kunnen we overwegen een extra ronde te doen.

Mochten er nog veel vragen zijn dan kunnen we misschien volgende week nog een kort overleg inschieten om het toe te lichten.

Met vriendelijke groet,

5.1.2.e

Wageningen University & Research - Corporate Strategy & Accounts

Tel: 5.1.2.e
e-mail: 5.1.2.e @wur.nl

Postbus 9101
6708 PB Wageningen,
Bezoekadres: Wageningen Campus, Atlas gebouw 104
Droevendaalsesteeg 4, Wageningen

Privacy

Van: Privacy
Verzonden: woensdag 9 december 2020 13:59
Aan: Privacy AFSG
Onderwerp: RE: Report data leak - thesis platform Food Sciences

Ha 5.1.2.e,

Deze was bij mij niet bekend. Lijkt mij wel goed om nog een follow-up aan te geven. Ik denk dat we twee dingen moeten vaststellen:

1. Zijn er afgezien van de inzage ook bijzondere gevoeligheden? Kunnen studenten bijv. uitgesloten worden van andere courses of kunnen zij een conflict krijgen doordat anderen konden zien welke thesis-onderwerpen zij hadden geselecteerd?
2. Gezien de aard van het incident: zou jij contact willen opnemen met IT om te kijken of nog vastgesteld kan worden wie er na 17/11 toegang heeft gehad tot deze per ongeluk gepubliceerde share?

Ik ga er gezien de aard van de gegevens van uit dat geen sprake is van mogelijke ernstige gevolgen en dus dat het niet gemeld hoeft te worden bij de AP, maar wacht jouw reactie toch graag met belangstelling af.

Groet, 5.1.2.e

Van: Privacy AFSG <privacy.afsg@wur.nl>
Verzonden: dinsdag 8 december 2020 14:59
Aan: Privacy <privacy@wur.nl>
Onderwerp: FW: Report data leak - thesis platform Food Sciences

Is dit datalek al bij jullie bekend? Wellicht al door 5.1.2.e gemeld?
Groet, 5.1.2.e

From: 5.1.2.e @wur.nl>
Sent: dinsdag 8 december 2020 13:31
To: Privacy AFSG <privacy.afsg@wur.nl>
Cc: 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
Subject: RE: Report data leak - thesis platform Food Sciences

Beste lezer,

Bij deze een kleine herinnering over onderstaande email. We horen graag wat er in deze situatie nodig is. Alvast bedankt.

Met vriendelijke groet,
5.1.2.e

From: Studyadvice Food
Sent: maandag 30 november 2020 12:38
To: Privacy AFSG <privacy.afsg@wur.nl>
Cc: 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
Subject: FW: Report data leak - thesis platform Food Sciences
Importance: High

Beste 5.1.2.e

Bij deze wil ik helaas melden dat wij bij de thesis procedure voor Food Sciences te maken hebben gehad met een datalek. Afgelopen vrijdag hebben we onderstaande email ontvangen van een student. Bij het aanmaken van de afhandellijst (op 18/11) heeft de groep "ViewersOnly" leesrechten gekregen. In die groep zat iedereen met een WUR account. Vanochtend heeft 5.1.2.e het probleem direct verholpen, de studenten hebben nu geen toegang meer tot het Thesis Platform op Sharepoint.

De volgende gegevens zijn zichtbaar geweest voor iedereen met een wur-account:
First name
Last name
Email address
Student Registration number
Programme
Specialisation
Chosen thesis topics
Prerequisite courses
Relevant Courses
Start date
Personal remarks

Aangezien de studenten vanaf dat moment het platform al niet meer nodig hadden (17/11 was de deadline om in te schrijven), zijn er hopelijk niet veel mensen geweest die het ook daadwerkelijk hebben gezien.

Ik hoor graag wat de eventuele vervolgstappen nu zijn. Alvast bedankt.

Met vriendelijke groet,

5.1.2.e

From: 5.1.2.e @wur.nl>
Sent: vrijdag 27 november 2020 21:43
To: Studyadvice Food <studyadvice.food@wur.nl>; OWI Food Science <food.science@wur.nl>; Servicedesk IT <servicedesk.it@wur.nl>
Subject: Report data leak - thesis platform Food Sciences
Importance: High

Hi,

I would like to report a data leak from the Thesis Platform for Food Sciences. Any WUR student or employee is able to view thesis applications from those that applied for a thesis starting period 4, 5 or 6. They can do this by going to sharepoint.wur.nl/sites/FT_ThesisTopics , and then clicking in the menu on the left on 'ManageApplicationsNovember2020'. They can then see the applicant's name and registration number, email address, study programme information, personal remarks, and thesis topics the student is interested in.

This data should not be visible to all students.

I trust I've provided you with enough information at this point in time. Don't hesitate to reach out if you need more information.

5.1.2.e

MSc Student Food Technology | Wageningen University & Research | LinkedIn |5.1.2.e .nl | ☎ Tel. 5.1.2.e

Privacy

Van: Privacy
Verzonden: dinsdag 27 oktober 2020 17:21
Aan: 5.1.2.e
Onderwerp: FW: Possible databreach after phishing
Bijlagen: Form_reporting_databreaches_WUR.docx

Urgentie: Hoog

Van: Servicedesk IT <servicedesk.it@wur.nl>
Verzonden: dinsdag 27 oktober 2020 9:24
Aan: Privacy <privacy@wur.nl>
Onderwerp: FW: Possible databreach after phishing
Urgentie: Hoog

Dag 5.1.2.e

Account van deze persoon is gehackt geweest waar vandaan een phishing is verstuurd naar WUR adressen. Mails zijn verwijderd uit de mailboxen, account is geblokkeerd geweest en wachtwoord is gewijzigd.

Groeten,
5.1.2.e
Servicedesk IT

From: 5.1.2.e @wur.nl>
Sent: 26 October 2020 15:00
To: Servicedesk IT <servicedesk.it@wur.nl>
Subject: Re: Possible databreach after phishing

Dear 5.1.2.e

Hereby the databreaches reporting form.

Best regards,
5.1.2.e

From: Servicedesk IT <servicedesk.it@wur.nl>
Sent: Monday, October 26, 2020 14:21
To: 5.1.2.e @wur.nl>
Subject: Possible databreach after phishing

Dear 5.1.2.e

Your account was hacked after you have left your credentials by a phishing e-mail.

Every notification related to the possible loss of data must be registered with Wageningen University & Research as a security incident.
Fill in the included form reporting databreaches and send it back to us as soon as possible but within the next 48 hours;

Also read intranet about the obligations concerning reporting databreaches:
https://intranet.wur.nl/umbraco/en/frequently-asked-questions/how-do-i-report-a-data-breach/

With kind regards,

5.1.2.e
Servicedesk IT

FORM FOR REPORTING DATA BREACHES

In the event of a security incident in which personal data may have been lost (even if you are not sure of this), you should use the data breach form to make a report of this incident. This must happen within 48 hours after detecting the incident.

Contact details of reporting employee			
Name	5.1.2.e		
Job title	Student		
E-mail address	5.1.2.e @wur.nl		
Phone number	5.1.2.e		
Details about the incident (description of the incident)	On last Friday, I entered my e-mail account and password in the link that one of my WUR friend send to me. Later I found out that my friend account was also hacked. Today, somebody used my e-mail to send a strange document to other WUR account. So I think my account is hacked too.		
Summary of the incident	My e-mail account is hacked and it has been used to send some sort of document to other WUR account.		
Explanation	*[What happened (theft or loss of data, malware/hack/DDoS, data accidentally published, etc.), how did the breach occur (e.g. via internet, e-mail, attack from outside, etc.), and how was the breach detected?]*		
Nature of the incident	Not yet known		
Explanation	*[e.g. unauthorised access, data was copied/downloaded, data was modified, deleted or destroyed, data theft, or not yet known]*		
Date and time of the incident	26 October 20202 around 12.30		
Explanation	*[At what time or during which period did the incident take place?]*		
Date and time of the discovery	26 October 20202 around 13.00		
Explanation	*[When was the breach detected?]*		
Persons involved	WUR student and staff		
Explanation	*[Whose (i.e. staff, students, test subjects, etc.) data is involved in the incident?]*		
Number of persons involved	Around 500 persons receive the hacked mail from my account		
Explanation	*[Possibly an estimation of the minimum/maximum number of persons]*		
What types of personal data? (tick box)		Yes	No
	Name, address, place of residence (business and/or private):		✓
	Contact details (phone number, e-mail address, etc.):	✓	
	Date and place of birth		✓
	Nationality		✓
	Gender		✓

	Identification details (login, password):	✓	
	Financial details or data from Human Resources Management		✓
	Personal identification numbers (BSN, education number, etc.)		✓
	Criminal justice information (convictions, reprimands, etc.)		✓
	Copy of passport		✓
	Copy of drivers licence		✓
	Photo		✓
	Medical data		✓
	Religion, political affiliation, trade union membership		✓
	Other, namely:		
Possible consequences (tick box)		Yes	No
	Stigmatisation or exclusion		✓
	Damage to health		✓
	Exposure to (identity) fraud		✓
	Exposure to spam or phishing	✓	
	Other, namely:		
What actions have been taken?	I have reported the incident to the Servicedesk IT		
Explanation	*[Description of the actions that have been taken to address the incident and to prevent further incidents]*		
What measures have been taken?	The password of the e-mail account has been changed.		
Explanation	*[Description and explanation of the security measures taken regarding the personal data involved in the incident; for example, have these been encrypted, hashed, pseudonymised or otherwise made inaccessible]*		
International aspects	No		
Explanation	*[Does the incident concern persons in other EEA countries (European Union, Liechtenstein, Norway, or Iceland)?]:*		

Send this form to **servicedesk.it@wur.nl** as soon as possible, but no later than 48 hours after the detection of a data breach. Your report will be dealt with in accordance with the data breach protocol.

Ontvangstbevestiging

Uw verzoek tot het indienen van een melding wordt in behandeling genomen.
U kunt de melding niet online raadplegen. Maak daarom een print voor uw eigen administratie. Doe dit voordat u deze pagina afsluit. Na het afsluiten van deze pagina zijn de gegevens die u heeft opgegeven niet meer beschikbaar. Onder het onderstaande meldingsnummer is de melding bekend bij de Autoriteit Persoonsgegevens. U heeft het meldingsnummer nodig om de melding aan te kunnen passen of in te kunnen trekken. Vermeld het meldingsnummer bij eventuele correspondentie met de Autoriteit Persoonsgegevens over de melding.

Tijdstip ontvangst	28-10-2020 20:55:51
Uniek nummer	5.1.2.e [redacted]

0. Over deze melding

Gaat het om een nieuwe of bestaande melding?	Een nieuwe melding indienen
Op grond van welke wettelijke bepaling doet u deze melding?	Algemene verordening gegevensbescherming (AVG)

1. Contactgegevens en overige algemene informatie

1.1 Contactgegevens

Over welke organisatie of welk bedrijf gaat het?

Registratienummer bij de Kamer van Koophandel	09215846
Naam van het bedrijf of de organisatie	Wageningen University
Adres	Droevendaalsesteeg 4
Postcode	6708PB
Plaats	Wageningen

In welke sector is de organisatie of het bedrijf actief?	Onderwijs - Tertiair onderwijs

Wie meldt het datalek?

Naam	5.1.2.e
Functie	corporate privacy officer
E-mailadres	5.1.2.e @wur.nl
Telefoonnummer	5.1.2.e

Met wie kan de Autoriteit Persoonsgegevens contact opnemen voor nadere informatie over de melding?

De melder is contactpersoon	Nee
Naam contactpersoon	5.1.2.e
Functie contactpersoon	functionaris gegevensbescherming
E-mailadres contactpersoon	dpo@wur.nl
Telefoonnummer contactpersoon	5.1.2.e

1.2 Betrokkenheid andere organisatie

Was er een andere organisatie betrokken bij de inbreuk?	Nee

2. Tijdlijn

Exacte datum waarop de inbreuk was, indien bekend	26-10-2020
Duurt de inbreuk op dit moment nog voort?	Nee
Wanneer werd de inbreuk ontdekt?	26-10-2020

3. Gegevens over het datalek

3.1 Aard van de inbreuk

Inbreuk op de vertrouwelijkheid van de gegevens	Ja
Inbreuk op de integriteit van de gegevens	Nee
Inbreuk op de beschikbaarheid van de gegevens	Nee

3.2 Aard van het incident

Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest?	Hacking, malware (bijv. ransomware) en/of phishing

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest

Op 26 oktober jl. constateerden drie studenten van Wageningen University dat hun e-mailaccounts waren gehackt. Onderzoek wijst uit dat een onbevoegde persoon gebruik heeft gemaakt van het e-mailaccount van de betreffende studenten. In de verzonden items stonden e-mails naar contactpersonen (binnen en buiten de organisatie).

4. Persoonsgegevens die betrokken zijn bij het datalek

4.1 Persoonsgegevens in het algemeen

Naam	Ja
Geslacht, geboortedatum en/of leeftijd	Nee
Burgerservicenummer (BSN)	Nee
Contactgegevens	Ja
Toegangs- of identificatiegegevens	Ja
Financiële gegevens	Nee
(Kopieën van) paspoorten of andere legitimatiebewijzen	Nee
Locatiegegevens	Nee
Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen	Nee
Onbekend / anders, namelijk:	Het betreft inlog/ww van één persoon (de gehackte medewerker); voor het overige alleen naam/e-mail-combinaties

4.2 Bijzondere categorieën van persoonsgegevens

Persoonsgegevens waaruit iemands ras of etnische afkomst blijkt	Nee
Persoonsgegevens waaruit iemands politieke opvattingen blijken	Nee
Persoonsgegevens waaruit iemands religieuze of levensbeschouwelijke overtuigingen blijken	Nee
Persoonsgegevens waaruit iemands lidmaatschap van een vakbond blijkt	Nee
Gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid	Nee
Gegevens over iemands gezondheid	Nee
Genetische gegevens	Nee
Biometrische gegevens	Nee

4.3 Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords ("gegevensregisters") zijn getroffen door de inbreuk	3

5. De groep mensen van wie persoonsgegevens betrokken zijn bij het datalek

Werknemers	Ja
Klanten (huidig en potentieel)	Nee
Leerlingen of studenten	Ja
Patiënten	Nee
Minderjarigen	Nee
Personen uit kwetsbare groepen	Nee

Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk.
Het betreft voornamelijk medewerkers en studenten van Wageningen University, alsmede privécontacten van de studenten.

Van minimaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?	2295

Van maximaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?	2295

6. Maatregelen die zijn getroffen voordat het datalek plaatsvond

Waren de persoonsgegevens op het moment dat de inbreuk zich voordeed versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk voor onbevoegden?	Nee

7. Gevolgen van het datalek

7.1 Gevolgen van de inbreuk op de vertrouwelijkheid, de integriteit en/of de beschikbaarheid van de gegevens.

Onbevoegden hebben kennis kunnen nemen van de gegevens	Ja
De gegevens kunnen op een onbehoorlijke of onrechtmatige manier worden misbruikt	Ja
Er worden binnen uw eigen organisatie mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens gebruikt	Nee
Er worden mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens hergebruikt voor andere doeleinden of doorgegeven aan andere organisaties	Nee
Een essentiële dienst kan tijdelijk niet meer worden verleend aan de betrokkenen	Nee
Een essentiële dienst kan permanent niet meer worden verleend aan de betrokkenen	Nee

7.2 Lichamelijke, materiële en immateriële schade voor de betrokkenen

Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkenen?

Discriminatie	Nee
Identiteitsdiefstal of -fraude	Ja
Financiële verliezen	Nee
Reputatieschade	Nee
Verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens	Nee
Ongeoorloofde ongedaanmaking van pseudonimisering	Nee
Betrokkenen kunnen hun rechten en vrijheden niet uitoefenen	Nee
Betrokkenen worden verhinderd controle over hun persoonsgegevens uit te oefenen	Nee
Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkenen	2. Beperkt

8. Vervolgacties naar aanleiding van het datalek

8.1 Informeren van de betrokkenen

Heeft u het datalek gemeld aan de betrokkenen of bent u van plan dat te gaan doen?	Ja
Wanneer heeft u het datalek gemeld aan de betrokkenen?	28-10-2020

Wat is de inhoud van de melding aan de betrokkenen?

Afhankelijk van de betrokken student: Op [datum] om [tijd] is vanaf een WUR e-mailadres onderstaande phishing e-mail aan je verzonden: onderwerp: Remittance Report [afbeelding van de e-mail] Mocht je een van de links geopend hebben gehad en je gegevens hebben ingevuld meld dat dan per omgaande bij de Servicedesk IT en wijzig meteen je wachtwoord. De links zijn ondertussen onklaar gemaakt. Mocht je het bericht nog in je mailbox hebben staan dan verwijder je het daar het beste uit: je

hoeft het niet meer aan te melden bij ons. Onze excuses voor de eventuele overlast die dit heeft veroorzaakt. Met vriendelijke groet, Servicedesk IT Wageningen University & Research Facilitair Bedrijf - Informatie Technologie Maandag t/m vrijdag: 08:00 - 17:30 E Servicedesk.IT@wur.nl W ITsupport.wur.nl

Hoeveel betrokkenen heeft u geïnformeerd of gaat u informeren?	2295
Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken om de betrokkenen te informeren?	E-mail

8.2 Maatregelen om de inbreuk aan te pakken

Welke technische en organisatorische maatregelen heeft uw organisatie getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?
Wij hebben het wachtwoord gereset, een malware/virusscan uitgevoerd, een scan uitgevoerd op de initiële link in de phishingmail, de phishingmail verwijderd en de geadresseerden gewaarschuwd via een e-mail. Daarnaast hebben wij direct meer urgentie gegeven aan inloggen via een multi-factor authenticatie (een aantal medewerkers is met onmiddellijke ingang onderworpen aan deze extra beveiligingsstap).

8.3 Internationale aspecten

Heeft de inbreuk zich voorgedaan in een grensoverschrijdende gegevensverwerking, en is de AP voor deze verwerking de leidende toezichthouder?	Nee
Heeft uw organisatie of bedrijf, het datalek gemeld bij privacytoezichthouders in een of meer andere EU-landen, of gaat u dat nog doen?	Nee
Heeft uw organisatie of bedrijf, het datalek gemeld bij Europese toezichthouders op andere meldplichten, of gaat u dat nog doen?	Nee

9. Overig

Is naar uw mening deze melding compleet?	Ja, de vereiste informatie is verstrekt en er is geen vervolgmelding nodig

FORM FOR REPORTING DATA BREACHES

In the event of a security incident in which personal data may have been lost (even if you are not sure of this), you should use the data breach form to make a report of this incident. This must happen within 48 hours after detecting the incident.

Contact details of reporting employee			
Name	5.1.2.e		
Job title	Scientist in AI and Machine learning		
E-mail address	5.1.2.e @wur.nl		
Phone number	5.1.2.e		
Details about the incident (description of the incident)	We noted that there is a text file in the C drive saying that the data on the virtual machine was encrypted and all encrypted files for this computer have the extension: .972f1d		
Summary of the incident	5.1.2.e reported on 6/25/2020 at 11:18 AM that the MetAlignVM3, a Virtual Machine (a virtual server, hereinafter referred to as VM), was encrypted in Azure (Microsoft Cloud). This server itself was managed by 5.1.2.e and the group at WFSR where he works. 5.1.2.e noted that there is a text file in the C drive saying that the data on the virtual machine was encrypted and all encrypted files for this computer have the extension: .972f1d. After speaking to the IT Service Desk, some experts in this area were brought together to see what was going on. They soon found that a standard account on the server was abused by malicious parties and that they were able to encrypt the machine via that account.		
Explanation	*[What happened (theft or loss of data, malware/hack/DDoS, data accidentally published, etc.), how did the breach occur (e.g. via internet, e-mail, attack from outside, etc.), and how was the breach detected?]*		
Nature of the incident	The VM account was abused by malicious parties and that they were able to encrypt the machine via that account.		
Explanation	all encrypted files for this computer have the extension: .972f1d		
Date and time of the incident	26/06/2020 at around 10:00		
Explanation	26/06/2020 at around 10:00		
Date and time of the discovery	26/06/2020 at around 10:00		
Explanation	26/06/2020 at around 10:00		
Persons involved	5.1.2.e and 5.1.2.e		
Explanation	5.1.2.e *is the designer of the VM and* 5.1.2.e *is the main user*		
Number of persons involved	1		
Explanation	*1*		
What types of personal data? (tick box)		Yes	No
	Name, address, place of residence (business and/or private):		X
	Contact details (phone number, e-mail address, etc.):		X
	Date and place of birth		X
	Nationality		X
	Gender		X
	Identification details (login, password):		X

	Financial details or data from Human Resources Management		X
	Personal identification numbers (BSN, education number, etc.)		X
	Criminal justice information (convictions, reprimands, etc.)		X
	Copy of passport		X
	Copy of drivers licence		X
	Photo		X
	Medical data		X
	Religion, political affiliation, trade union membership		X
	Other, namely:		
Possible consequences (tick box)		Yes	No
	Stigmatisation or exclusion		X
	Damage to health		X
	Exposure to (identity) fraud		X
	Exposure to spam or phishing		X
	Other, namely:		
What actions have been taken?	5.1.2.e has disabled the affected VM at our request so that the content is retained for further investigation. To be sure, there is also a check going on to the data on the machine to see whether a report should be made to the authority for personal data (data leak) for the data present. The first estimate is that this is not necessary, but the request has yet to be made.		
Explanation			
What measures have been taken?	5.1.2.e has disabled the affected VM at our request so that the content is retained for further investigation. To be sure, there is also a check going on to the data on the machine to see whether a report should be made to the authority for personal data (data leak) for the data present. The first estimate is that this is not necessary, but the request has yet to be made.		
Explanation	*No personal data*		
International aspects	No		
Explanation	*No*		

Send this form to **servicedesk.it@wur.nl** as soon as possible, but no later than 48 hours after the detection of a data breach. Your report will be dealt with in accordance with the data breach protocol.

Privacy

Van: 5.1.2.e
Verzonden: donderdag 2 juli 2020 8:51
Aan: Privacy
Onderwerp: RE: Please fill in data breach form because of the Securtiy incident 470558.00

Hoi 5.1.2.e

Van dit incident was ik al op de hoogte, heb het er ook al met 5.1.2.e over gehad. Er stonden geen persoonsgegevens op de VM, er is geen sprake van een meldplichtig incident.

We gaan dit als aanleiding gebruiken om FB IT security zover proberen te krijgen een seminar te geven voor WFSR over de security richtlijnen en best practices voor eigen systemen. Die ransomware aanvallen zijn echt een groot risico.

Met vriendelijke groet,

5.1.2.e

From: Privacy
Sent: woensdag 1 juli 2020 17:01
To: 5.1.2.e @wur.nl>
Subject: FW: Please fill in data breach form because of the Securtiy incident 470558.00

Ha 5.1.2.e ,

Een vraagje: ik kreeg dit datalekmeldformulier, maar kan hier weinig kaas van maken. Jij bent een stuk technischer onderlegd. Zou jij eens willen nagaan of hier sprake is van een meldplichtig incident? Wellicht met name nagaan of er persoonsgegevens inzichtelijk zijn geweest?

Groet, 5.1.2.e

Van: Servicedesk IT
Verzonden: maandag 29 juni 2020 9:26
Aan: Privacy <privacy@wur.nl>
CC: 5.1.2.e @wur.nl>
Onderwerp: FW: Please fill in data breach form because of the Securtiy incident 470558.00

Dear Privacy,

Please find enclosed the databreach form of 5.1.2.e. Can you please handle this and for any questions, contact Yamine?

Best regards,
5.1.2.e
Servicedesk IT

From: 5.1.2.e @wur.nl>
Sent: 29 June 2020 08:54
To: 5.1.2.e @wur.nl>
Subject: RE: Please fill in data breach form because of the Securtiy incident 470558.00

Hi 5.1.2.e;
Thanks for your email!
Here is the filled in form.
Please let me know if you have any other questions.
Gr
5.1.2.e

From: 5.1.2.e
Sent: maandag 29 juni 2020 8:11
To: 5.1.2.e @wur.nl>
Cc: Privacy <privacy@wur.nl>
Subject: Please fill in data breach form because of the Securtiy incident 470558.00
Importance: High

Dear 5.1.2.e

Please fill in the attached databreach form as soon as possible and send this form to Privacy@wur.nl because of your Security incident that your cloud hosted (non WUR) VM Ware server in Azure was encrypted.

Best regards,
5.1.2.e
Servicedesk IT

Privacy

Van: 5.1.2.e
Verzonden: donderdag 10 september 2020 16:36
Aan: 5.1.2.e
Onderwerp: FW: incident persoonsgegevens
Bijlagen: Visma Idella Incident Verslag ZWERD Datalek 4-9-2020 - klant (1).pdf

Hallo 5.1.2.e

I.t.t. wat ik aangaf in ons gesprek betreft het hier geen WW maar ZW. Het gaat hier om medewerkers die ziek uit dienst zijn gegaan en waarvoor WUR verplichtingen draagt die worden uitgevoerd door Visma.
Deze groep is in aantallen stukken kleiner dan de medewerkers met WW rechten waarover ik sprak.

Met vriendelijke groet,

5.1.2.e
Aanwezig: maandag t/m vrijdag
Wageningen University & Research
Afdeling Corporate HR
Postbus 9101, 6700 HB Wageningen
Gebouw 104 (Atlas), Droevendaalsesteeg 4, 6708 PB Wageningen
Tel.: 0031-6 5.1.2.e
5.1.2.e 5.1.2.e @wur.nl
www.wur.nl
www.disclaimer-nl.wur.nl

From: 5.1.2.e @wur.nl>
Sent: Wednesday, September 09, 2020 9:50 AM
To: 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
Subject: FW: incident persoonsgegevens

Ter info (en actie ?)

5.1.2.e

Van: 5.1.2.e
Verzonden: donderdag 24 september 2020 13:59
Aan: 5.1.2.e
Onderwerp: RE: incident persoonsgegevens

Ha 5.1.2.e

Dat mag je zeker bij mij melden (liefst via de privacy officer van CHR of anders via privacy@wur.nl).

5.1.2.e had dat gelukkig ook al gedaan, anders waren wij te laat geweest. Wij 5.1.2.e en ik) hebben hier verder onderzoek naar gedaan met de conclusie dat wij dit incident niet hoeven te melden bij de toezichthouder.

Groet, 5.1.2.e

5.1.2.e
5.1.2.e Corporate Governance & Legal Services

Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e, Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317-5.1.2.e
www.wur.nl/disclaimer

Van: 5.1.2.e @wur.nl>
Verzonden: donderdag 24 september 2020 13:55
Aan: 5.1.2.e @wur.nl>
Onderwerp: FW: incident persoonsgegevens

Hallo 5.1.2.e

In mijn vakantieperiode heb ik onderstaand bericht ontvangen. Kan ik dit bij jou melden?

Met vriendelijke groet,

5.1.2.e
5.1.2.e
Wageningen University & Research
Corporate HR, Rechtsposities en Arbeidsvoorwaarden
Postbus 9101, 6700 HB, Wageningen

Atlas, gebouw 104, 5.1.2.e
Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. +316 5.1.2.e email: 5.1.2.e @wur.nl
www.wur.nl
www.disclaimer-nl.wur.nl

HR EXCELLENCE IN RESEARCH

Privacy

Van: 5.1.2.e
Verzonden: dinsdag 15 september 2020 13:01
Aan: Privacy
Onderwerp: RE: Incident persoonsgegevens

Nee, nog niet, ik mail zo een reminder.

From: Privacy <privacy@wur.nl>
Sent: Tuesday, September 15, 2020 11:47 AM
To: 5.1.2.e @wur.nl>
Subject: RE: Incident persoonsgegevens

Ha 5.1.2.e weten wij al meer over dit incident? Hebben wij al reactie vanuit Visma?

Groet, 5.1.2.e

Van: 5.1.2.e @wur.nl>
Verzonden: donderdag 10 september 2020 15:18
Aan: 5.1.2.e @visma.com
CC: 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
Onderwerp: Incident persoonsgegevens
Urgentie: Hoog

Geachte heer 5.1.2.e

N.a.v. onderstaande melding heb ik enkele vragen waarvan ik hoop dat u mij kunt voorzien van de antwoorden.

1. Is van de situatie melding gemaakt bij de Autoriteit Persoonsgegevens (AP) en zo nee wat is daarvoor de motivatie?
2. Wat is de reden van de tijd die er zit tussen het incident (signalering) en uw melding hiervan aan ons op 8 september 2020 via onderstaande mail?
3. Kunt u uitsluiten dat gegevens van ex-werknemers van WUR bij derden zijn aangeleverd via het betreffende overzicht, of is dit beperkt tot een data uitwisseling tussen alleen ex-WUR medewerkers?

Met vriendelijke groet,

5.1.2.e
Aanwezig: maandag t/m vrijdag
Wageningen University & Research
Afdeling Corporate HR
Postbus 9101, 6700 HB Wageningen
Gebouw 104 (Atlas), Droevendaalsesteeg 4, 6708 PB Wageningen
Tel.: 0031-6 5.1.2.e
5.1.2.e 5.1.2.e @wur.nl
www.wur.nl
www.disclaimer-nl.wur.nl

Van: 5.1.2.e @visma.com>
Verzonden: dinsdag 8 september 2020 13:44
Onderwerp: Fwd: incident persoonsgegevens

Dag,

Tijdens de opvolging van een verzoek van een klant aan afdeling ZW-ERD van Visma Idella heeft een medewerker van Visma Idella per abuis een overzicht verstuurd met persoonsgegevens, resulterend in een potentieel datalek. Dat betreuren wij zeer. Aangezien dit persoonsgegevens betreft van uw ex-werknemers informeren wij u met bijgaand document over de aard en oorzaak van dit incident en over onze mitigerende maatregelen.

Indien u meer informatie wenst, zijn wij uiteraard beschikbaar voor een nadere toelichting. Wilt u in dat geval alstublieft contact opnemen met:
5.1.2.e Data Protection Officer
06-5.1.2.e
email:5.1.2.e @visma.com

Met vriendelijke groet.

5.1.2.e
Service Delivery Manager

Mobile 06 5.1.2.e

Visma Idella

Plotterweg 38, Amersfoort | visma-idella.nl

.

Privacy

Van: 5.1.2.e
Verzonden: vrijdag 11 september 2020 8:16
Aan: 5.1.2.e
Onderwerp: RE: incident persoonsgegevens

Hallo 5.1.2.e

Medewerkers die ziek uit dienst gaan blijven onze verantwoordelijkheid, zowel t.a.v. een juiste re-integratie in het werkproces (buitenWUR) als het doorbetalen van ziekengeld uitkering. Beide hebben we ondergebracht bij deze externe partij.

Zodra ik antwoord heb op de gestelde vragen zal ik vragen om het lijstje namen. Dat kunnen we ook zelf produceren want we weten wie van onze ex-medewerkers bij Visma zijn ondergebracht. Maar beter is dat zij die lijst leveren lijkt me.

Groeten,

5.1.2.e

From: 5.1.2.e @wur.nl>
Sent: Thursday, September 10, 2020 6:01 PM
To: 5.1.2.e @wur.nl>
Subject: RE: incident persoonsgegevens

Ha 5.1.2.e, dat is mooi. Het is nog steeds bovenwettelijk/vrijwillig neem ik aan.

Het zou in aanvulling op je vragen denk ik ook nuttig zijn als wij uiteindelijk op een beveiligde wijze ook van Visma/Raet een lijstje krijgen met mensen, zodat wij die – indien nodig, maar die analyse moeten wij uiteraard nog samen maken – kunnen benaderen.

Groet, 5.1.2.e

5.1.2.e
5.1.2.e | Corporate Governance & Legal Services

Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317-5.1.2.e
www.wur.nl/disclaimer

Privacy

Van: Privacy
Verzonden: donderdag 17 september 2020 16:01
Aan: 5.1.2.e
Onderwerp: RE: REeminder: Incident persoonsgegevens

Ha 5.1.2.e
Heb net met 5.1.2.e besproken en afgestemd met andere universiteiten. Wij komen er op uit dat wij niet hoeven te melden en vertrouwen op de vaststelling van Visma.
Terzijde, dit krijgt nog wel een staartje in de zin dat sommige uni's een wat diepgravendere audit gaan uitvoeren bij Visma, nu dit soort knulligheden niet getuigen van een goed privacy/security-bewustzijn. Wij doen daar vooralsnog niet in mee.
Heb jij ook nog de contracten met Visma boven water kunnen krijgen?
Groet, 5.1.2.e

Van: 5.1.2.e @wur.nl>
Verzonden: woensdag 16 september 2020 12:14
Aan: 5.1.2.e @wur.nl>
Onderwerp: FW: REeminder: Incident persoonsgegevens
Hallo 5.1.2.e
Hierbij de reactie van Visma. Zie punt 3. Is dit voor ons voldoende en is het daarmee case closed?
Met vriendelijke groet,

5.1.2.e
5.1.2.e
Aanwezig: maandag t/m vrijdag
Wageningen University & Research
Afdeling Corporate HR
Postbus 9101, 6700 HB Wageningen
Gebouw 104 (Atlas), Droevendaalsesteeg 4, 6708 PB Wageningen
Tel.: 0031-6 5.1.2.e
5.1.2.e @wur.nl
www.wur.nl
www.disclaimer-nl.wur.nl

From: 5.1.2.e @visma.com>
Sent: Wednesday, September 16, 2020 10:30 AM
To: 5.1.2.e @wur.nl>
Cc: 5.1.2.e @visma.com>; 5.1.2.e @visma.com>
Subject: Re: REeminder: Incident persoonsgegevens
Geachte 5.1.2.e

Allereerst excuses. Uw bericht van afgelopen donderdag is mij helaas ontschoten. Ik heb de antwoorden op uw vragen hieronder verwerkt.

1. Is van de situatie melding gemaakt bij de Autoriteit Persoonsgegevens (AP) en zo nee wat is daarvoor de motivatie?
   Nee, hier is geen melding gedaan bij de Autoriteit Persoonsgegevens. Primair omdat dit door de data verantwoordelijke gedaan moet worden en Visma Idella is de verwerkende partij.
   Ook is er op basis van de beslisboom gepubliceerd door de Autoriteit Persoonsgegevens naar onze mening geen noodzaak geweest tot melden bij de AP. De gegevens zijn niet ingezien door derden en zijn definitief verwijderd. Er kan dus redelijkerwijs uitgesloten worden dat er geen onrechtmatige verwerking plaats gevonden heeft.
2. Wat is de reden van de tijd die er zit tussen het incident (signalering) en uw melding hiervan aan ons op 8 september 2020 via onderstaande mail?
   Er is verwarring geweest binnen onze organisatie over wie hoort te communiceren en wie de contactpersonen voor meldingen rondom AVG incidenten bij de klant was. De Service Delivery Manager heeft het op zich genomen om te communiceren, maar was zich onvoldoende bewust over de tijdslijn die gevolgd diende te worden. Voor toekomstige situaties rondom (mogelijke) datalekken is het protocol aangescherpt en zijn de communicatielijnen duidelijker omschreven. Onze excuses hiervoor.
3. Kunt u uitsluiten dat gegevens van ex-werknemers van WUR bij derden zijn aangeleverd via het betreffende overzicht, of is dit beperkt tot een data uitwisseling tussen alleen ex-WUR medewerkers?
   Via deze weg kunnen wij bevestigen dat de medewerkers van de andere klant, die de e-mail met vertrouwelijke en gevoelige gegevens van onder meer uw instelling per abuis toegezonden hebben gekregen, de desbetreffende e-mail met gegevens van uw instellingen inderdaad ongeopend en definitief hebben weggegooid.

Hopende u hiermee voldoende geïnformeerd te hebben.
Met vriendelijke groet,

5.1.2.e
Security Manager

Switchboard +31 5.1.2.e
Visma Idella

Kerkstraat 56 - Almere-Haven - NL | www.visma-idella.nl

On Tue, 15 Sep 2020 at 13:02, Ligt, Ron de <ron.deligt@wur.nl> wrote:

> Geachte 5.1.2.e ,
>
> Afgelopen donderdag mailde ik u onderstaande vragen. Graag verneem ik per omgaande de antwoorden. Dank u.
>
> Met vriendelijke groet,
>
> 5.1.2.e
>
> 5.1.2.e
>
> *Aanwezig: maandag t/m vrijdag*

Wageningen University & Research

Afdeling Corporate HR

Postbus 9101, 6700 HB Wageningen

Gebouw 104 (Atlas), Droevendaalsesteeg 4, 6708 PB Wageningen

Tel.: 0031-6 1853 4070

5.1.2.e @wur.nl

www.wur.nl

Reeds beoordeeld

5.1.2.e

Van: 5.1.2.e
Verzonden: woensdag 16 september 2020 12:19
Aan: 5.1.2.e
Onderwerp: RE: REeminder: Incident persoonsgegevens

Ha 5.1.2.e heldere antwoorden, al is de stelligheid dat geen onrechtmatige verwerking heeft plaatsgevonden wel volledig afhankelijk van vertrouwen op de ontvangers en (logischerwijs) niet op een andere manier geverifieerd of afgedekt. Ik zal het nog even met 5.1.2.e bespreken en koppel dan nog even terug.

Groet, 5.1.2.e

5.1.2.e
Corporate Governance & Legal Services

Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e, Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317-5.1.2.e
www.wur.nl/disclaimer

Incident verslag

VISMA | idella

Datalek in ZW-ERD 04/09/2020

MSP #88926

07-09-2020

Vertrouwelijk

Table of contents

Inleiding

Tijdens de opvolging van een verzoek door een klant aan de afdeling Ziektewet Eigen Risico Drager (ZW-ERD) bij Visma Idella heeft een medewerker van Visma Idella per abuis een overzicht verstuurd waarbij persoonsgegevens blootgesteld hebben gestaan aan onrechtmatige verwerking, resulterende in een (potentieel) datalek. Met dit document informeren wij u over de aard, oorzaak en mitigerende maatregelen. Aangezien dit (potentiële) datalek persoonsgegevens betreft welke tot uw deelnemers behoren, informeren wij u bij deze over dit incident.

Aard van het incident

Vrijdagmiddag 4 september jl. om 13:23 is een email bericht verstuurd aan 3 medewerkers van een klant van Visma idella, welk een Excel bestand bevatte bestaande uit 2 tabbladen.

Het eerste tabblad was op verzoek van deze klant en bevatte een lijst met dossiergegevens (van uitkeringsgerechtigden gekoppeld aan de klant) zonder herleidbare persoonsgegevens.

Het tweede tabblad was toegevoegd ten tijde van het samenstellen van deze eerder genoemde lijst en bevatte een overzicht van alle uitkeringsgerechtigden voor alle klanten. Deze lijst bevatte persoonsgegevens zoals NAW, geboortedatum, geslacht, telefoonnummer, BSN en IBAN.

De medewerker van Visma Idella verzuimde dit tweede tabblad te verwijderen voor het versturen van het bestand naar de klant medewerkers.

Ongeveer 20 minuten na het versturen ontdekte de medewerker de fout en is direct (om 13:52) een urgent bericht verstuurd aan de ontvangers met het verzoek het eerder verstuurde bericht ongeopend te verwijderen.

Eén ontvanger heeft dit ook direct bevestigd. De andere ontvangers waren niet aanwezig en heeft Visma Idella een “out of office reply” ontvangen. Hierop is een dringend bericht verstuurd aan deze medewerkers met een niet te miskennen onderwerp om dat bericht eerste te lezen. Ten tijde van het opstellen van dit verslag hebben alle ontvangers bevestigd dat het ontvangen bericht verwijderd is.

Oorzaak

De medewerker van Visma Idella heeft acties ondernomen die kunnen worden opgevat als strijdig met de huidige procedures en die mogelijk hebben geleid tot 'lekken' van persoonsgegevens tijdens de uitvoering van de opdracht door de klant.

- Allereerst heeft de verwerkingsmedewerker op de afdeling binnen Visma Idella onzorgvuldig gehandeld door in hetzelfde bestand dat voorbereid werd voor een specifieke klant gegevens te verwerken van alle klanten.

- Daarnaast heeft de medewerker onvoldoende aandacht besteed aan de bijgevoegde bijlage ten tijde van het versturen van het e-mailbericht. Er is niet gecontroleerd of het bijgevoegde bestand uitsluitend de benodigde gegevens bevatte.

Mitigerende maatregelen

In het kader van de Oorzaak heeft Visma Idella de volgende mitigerende maatregelen toegepast om de gevolgen van een potentieel vergelijkbare situatie te beperken en toekomstige vergelijkbare situaties te vermijden:
Met betrekking tot dit specifieke incident:

1. Aanroepen Richtlijn Datalekken, resulterende in betrokkenheid en regiefunctie door de Data Protection Officer (DPO).
2. De betreffende afdeling heeft direct na ontdekking een bericht verstuurd aan de ontvangers om het eerder verstuurde bericht inclusief bijlage ongeopend te verwijderen.
3. Voor de afwezige ontvangers is een bericht verstuurd met een duidelijk onderwerp om aandacht te trekken en het bericht te verwijderen zonder inzage.
   De opvolging van dit punt wordt bewaakt door de DPO.

Met betrekking tot beleid en procedures:

1. Bewustwording van de risico's van bijlagen en de mogelijkheid van het bevatten van persoonsgegevens wordt versneld en vernieuwd onder de aandacht gebracht van alle medewerkers.
2. De mogelijkheid om rapportages te genereren moet verbeterd worden zodat er geen handmatige selectie of filtering hoeft plaats te vinden.
3. De wijze van samenstellen van een bestand moet verbeterd worden, waarbij het brondocument niet wordt gebruikt als definitief document.

Impact

Hoewel er geen impact is op het gebied van Beschikbaarheid of Integriteit van de data, is er wel een impact op het gebied van Vertrouwelijkheid. Niet-geanonimiseerde persoonsgegevens zijn onjuist verwerkt. Tot op heden zijn er geen aanwijzingen dat gegevens die bij de derde zijn terechtgekomen, onjuist zijn verwerkt, maar deze mogelijkheid kan niet worden uitgesloten. De opvolging van dit punt wordt bewaakt door de DPO.

Conclusie

Er zijn geen aanwijzingen dat de gegevens op enigerlei wijze zijn verwerkt door de derde partij die de gegevens - ten onrechte - heeft ontvangen. Dit kan echter niet helemaal worden uitgesloten.

De relevante gegevens zijn op een onbeschermde manier verstuurd door Visma idella. De relevante gegevens zijn onjuist verwerkt door een medewerker van Visma Idella.

In overleg met de Divisional Data Protection Officer is op basis van de richtlijnen in de Algemene Verordening Gegevensbescherming vastgesteld dat het bij dit incident om een "potentieel datalek" gaat. De uiteindelijke beslissing om te classificeren als datalek ligt bij de klant. Wij verzoeken u hiertoe dan ook kennis te nemen van het voorgaande en aan de hand van de Algemene Verordening Persoonsgegevens en uw interne beleidsrichtlijnen, tot een afweging met betrekking tot opvolging richting de Autoriteit Persoonsgegevens te komen.

Op basis van de Oorzaak- en Risicoanalyse zal Visma Idella mitigerende maatregelen in de procedures gaan toepassen en zal zij een aangescherpt organisatiebeleid hanteren voor de omgang met gegevens per e-mail.

Aandachtspunten - “lessons learned”

- Er is momenteel geen adequate rapportage mogelijkheid in de applicatie aanwezig om rapporten specifiek voor 1 klant aan te maken.
- Medewerkers zijn onvoldoende gecontroleerd bij het verwerken van gegevens en het vervolgens versturen hiervan (4-ogen principe).

Wat moet u doen?

In het kader van het voorgaande, informeert Visma Idella u proactief over de ontstane situatie. Indien u meer informatie wenst, zijn wij uiteraard beschikbaar voor een nadere toelichting

- 5.1.2.e - Data Protection Officer (06-5.1.2.e , email: 5.1.2.e @visma.com)

Wij verzoeken u kennis te nemen van het voorgaande en aan de hand van de Algemene Verordening Persoonsgegevens en uw interne beleidsrichtlijnen, tot een afweging met betrekking tot opvolging richting de Autoriteit Persoonsgegevens te komen.

Privacy

Van: WUR-CERT
Verzonden: donderdag 9 april 2020 10:18
Aan: Privacy
Onderwerp: Fwd: FW: Mogelijk datalek/autorisatiefout MyHR
Bijlagen: screenshot MyHR.jpg

Alvast ter info.

Groeten, 5.1.2.e

-------- Forwarded Message --------
Subject: FW: Mogelijk datalek/autorisatiefout MyHR
Date: Thu, 9 Apr 2020 09:09:47 +0200
From: 5.1.2.e @wur.nl>
To: WUR-CERT <cert@wur.nl>

Er is een datalek binnen MyHR.
Zelf gecheckt en je kan op deze manier gegevens van anderen inzien.
5.1.2.e meldt jij dit naar Legal?

From: 5.1.2.e @wur.nl>
Sent: woensdag 8 april 2020 21:52
To: Servicedesk IT <servicedesk.it@wur.nl>
Cc: 5.1.2.e @wur.nl>
Subject: Mogelijk datalek/autorisatiefout MyHR
Beste collega,
Via deze mail (CC aan 5.1.2.e , mijn leidinggevende) wil ik graag een mogelijk datalek melden die ik ontdekte toen ik gebruikmaakte van MyHR.
Onder de tegel Personalia > Mijn dossier heb ik naast mijn Personeelsdossier ook toegang tot een map Organisatie, met diverse submappen, zie bijgevoegde printscreen. Hierin staan documenten met gegevens van medewerkers rond Optare keuzes (inclusief namen en bedragen). Ik weet niet of het alleen bij mij het geval is (een autorisatiefout?) of bij meerdere medewerkers, maar dit lijkt mij zeker niet de bedoeling, vandaar deze melding.
Als je nog meer informatie nodig hebt, dan hoor ik het graag.
Hartelijke groet,

5.1.2.e
Met vriendelijke groet,
5.1.2.e
Student Service Centre | Medewerker beurzenprogramma's
Wageningen University
Droevendaalsesteeg 2
6708 PB Wageningen
Tel. 0317 5.1.2.e
5.1.2.e @wur.nl

https://workforce.adp.nl/PV_Web/ Automatic D... Maintenance NLP610 - ADP Workforce 5....

Home | Terug | Taken | Overzichten

Mijn dossier

VERVERSEN | INFO | BEKIJKEN | TOEVOEGEN | ZOEKEN | INSTELLINGEN

Documenten

- Documenten
  - Organisatie
    - Interfaces
      - **Flexarbvw**
      - Mendix Mail
      - Projectcodes
      - WBA
  - Log bestanden
    - Interfaces
      - Flexarbvw
      - Mendix Mail
- Personeelsdossier

NAAM	TYPE	WERK
Optare_verwerkte_aanvragen_psa	xls	
Optare_doel_fiets	xls	
Optare_doel_extra_verlofuren	xls	
Optare_doel_vakbond	xls	
Optare_varw_eju_vu_salaris	xls	
Optare_varw_reiskosten	xls	
Optare_bronnen_vakbondscontributie	xls	
Optare_bronnen_fietsvergoeding	xls	
Optare_bronnen_extra_verlofuren	xls	
optare_bruto_salaris	xls	
optare_mutaties_reiskosten	xls	
optare_bronnen_reiskosten	xls	
optare_doel_reiskosten	xls	
optare_vaste_toelagen	xls	
optare_opbouw_min_vu	xls	
opt_part_salaris	xls	

Privacy

Van: 5.1.2.e
Verzonden: donderdag 9 april 2020 11:45
Aan: 5.1.2.e
CC: 5.1.2.e Buchwaldt, Rens
Onderwerp: security breach Workforce

Beste 5.1.2.e

Vanochtend begreep ik van IT dat er een ernstig datalek via Workforce aan de orde is waarbij de salarisgegevens van een grote groep medewerkers waren in te zien. Waarschijnlijk allen Optare gerelateerd. De nodige maatregelen vanuit FB-IT zijn, voor zover mogelijk, in gang gezet. Graag zie ik dat er minutieus record bijgehouden wordt van de stappen die genomen worden vanuit ADP. We zullen dit datalek moeten melden bij de AP en alle betrokkenen zullen wellicht een melding moeten krijgen van dit datalek. Dat kan alle medewerkers van WUR betreffen.

Vriendelijke groet,
5.1.2.e

5.1.2.e | Functionaris Gegevensbescherming | Wageningen University & Research | Postbus 9101, 6700 HB Wageningen | +31 (0)317 5.1.2.e | www.wur.nl

Privacy

Van: 5.1.2.e
Verzonden: donderdag 9 april 2020 12:00
Aan: 5.1.2.e
CC: 5.1.2.e Buchwaldt, Rens; 5.1.2.e
Onderwerp: RE: security breach Workforce

Zegt niet alles over hoelang het voor de signalering heeft opengestaan. Ik haak zo meteen in de call aan vanwege het feit dat 5.1.2.e (CPO) vanochtend vrij heeft.

From: 5.1.2.e
Sent: Thursday, April 09, 2020 11:58 AM
To: 5.1.2.e @wur.nl>
Cc: 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>; Buchwaldt, Rens 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
Subject: RE: security breach Workforce

Hallo 5.1.2.e
Gaan we zeker doen. Om 12.00 overleg met ADP. Voor de geruststelling: signalering was om 9.28 uur. Bevestiging lek gedicht om 10.02 uur.
Met vriendelijke groet,

5.1.2.e
Aanwezig: maandag t/m vrijdag
Wageningen University & Research
Afdeling Corporate HR
Postbus 9101, 6700 HB Wageningen
Gebouw 104 (Atlas), Droevendaalsesteeg 4, 6708 PB Wageningen
Tel.: 0031-6 5.1.2.e
5.1.2.e @wur.nl
www.wur.nl

Reeds beoordeeld

FORMULIER MELDING DATALEKKEN

In geval van een security incident waarbij mogelijk persoonsgegevens verloren zijn gegaan (ook als je dat niet zeker weet) gebruik je het datalekformulier om een melding te doen. Dat dient binnen 48 uur na constatering van het incident te gebeuren.

Contactgegevens melder	
Naam	5.1.2.e
Functie	5.1.2.e
E-mailadres	5.1.2.e @wur.nl
Telefoonnummer	06-5.1.2.e
Gegevens over het incident (omschrijving van het incident)	Op 31 maart jl. heeft ADP NL i.o. van de Wageningen UR een transitie uitgevoerd en klantgegevens van Wageningen UR verplaatst van een lokale omgeving naar de gehoste SaaS omgeving van ADP. Een onderdeel van deze transitie is het opnieuw definiëren van alle koppelingen met externe systemen inclusief de bijbehorende documentypes. Hierbij is door ADP verzuimd de autorisaties van de documenten op de juisten manier in te richten. Hierdoor hebben medewerkers via het Workforce portal met de rechten ESS, MSS en PSS mogelijk inzicht gehad mogelijk inzicht gehad in “Interfaces” en “Logbestanden”.
Samenvatting van het incident	Autorisaties incorrect waardoor toegang onbevoegde(n) op medewerker gegevens.
Toelichting	*[wat is er gebeurd (diefstal of verlies van gegevens, malware/hack/DDoS, gegevens per ongeluk gepubliceerd, etc.), op welke manier (bijv. via internet, e-mail, aanval van buitenaf, etc.) en hoe is het incident ontdekt]*
Aard van het incident	Inzage door onbevoegde(n) met mogelijkheid van downloaden van gegevens.
Toelichting	*[bijv. inzage door onbevoegden, gegevens gekopieerd/gedownload, wijzigingen aangebracht, gegevens verwijderd of vernietigd, diefstal van gegevens of nog niet bekend]*
Datum en tijdstip van het incident	9 april 2020
Toelichting	*[op welk moment of gedurende welke periode vond het incident plaats]*
Datum en tijdstip van ontdekking	9 april 2020 09:28 uur
Toelichting	*[wanneer is het incident ontdekt]*
Betrokkenen	Nog onbekend - ADP is een onderzoek gestart over de periode 25 maart tot 9 april welke documenttypes de properties niet goed waren ingericht. (Oplevering 10 april) - ADP onderzoekt wie er in de periode 25 maart tot 9 april onrechtmatig bestanden heeft gedownload.(Oplevering 10 April)
Toelichting	*[van welke personen (medewerkers, studenten, proefpersonen etc) zijn gegevens betrokken bij het incident]*
Aantal betrokkenen	Onbekend, zie hiervoor.

Toelichting	*[eventueel een schatting van minimaal/maximaal aantal personen]*		
Welke soorten persoonsgegevens (aankruisen)		Ja	Nee
	naam, adres, woonplaats (zakelijk en/of privé):	x	
	contactgegevens (telefoonnummer, e-mailadres, etc.):	x	
	geboortedatum en -plaats		x
	nationaliteit		x
	geslacht		x
	identificatiegegevens (login, wachtwoord):		x
	financiële- of HRM-gegevens	x	
	persoonsgebonden nummers (BSN, onderwijsnummer, etc.)		x
	strafrechtelijke gegevens (veroordelingen, berispingen, etc.)		x
	kopie paspoort		x
	kopie rijbewijs		x
	foto		x
	medische gegevens		x
	godsdienst, politieke voorkeur, vakbondslidmaatschap		x
	anders, namelijk: gegevens keuze model Optare (onduidelijk in welke omvang, zie onderzoek ADP)		
Mogelijke gevolgen (aankruisen)		Ja	Nee
	stigmatisering of uitsluiting		x
	schade aan de gezondheid		x
	blootstelling aan (identiteits)fraude		x
	blootstelling aan spam of phishing		x
	anders, namelijk:		
Welke acties zijn genomen	Er is melding gedaan bij leverancier ADP en opvolgend daaraan heeft diezelfde dag een call plaatsgevonden tussen security officers van WUR en ADP om de omvang van de problematiek te bespreken, de direkt te nemen en genomen maatregelen en het onderzoek op de impact te bespreken.		
Toelichting	*[beschrijving welke acties zijn getroffen om het incident te adresseren en om verdere incidenten te voorkomen]*		
Welke maatregelen zijn getroffen	Direct na de melding heeft ADP per documenttype de autorisaties aangepast waardoor medewerkers geen toegang meer hadden tot deze dossiers.		
Toelichting	*[beschrijving en toelichting welke beveiligingsmaatregelen van toepassing zijn op de betrokken persoonsgegevens; zijn die bijv. versleuteld, gehasht, gepseudonimiseerd of anderszins ontoegankelijk gemaakt]*		
Internationale aspecten	n.v.t.		
Toelichting	*[heeft het incident betrekking op personen in andere EER-landen [Europese Unie, Liechtenstein, Noorwegen of IJsland]:*		

Stuur dit formulier zo snel mogelijk, doch uiterlijk binnen 48 uur na het constateren van een datalek naar **servicedesk.it@wur.nl**. Dan wordt uw melding afgehandeld volgens het datalekkenprotocol.

Ontvangstbevestiging

Uw verzoek tot het indienen van een melding wordt in behandeling genomen.
U kunt de melding niet online raadplegen. Maak daarom een print voor uw eigen administratie. Doe dit voordat u deze pagina afsluit. Na het afsluiten van deze pagina zijn de gegevens die u heeft opgegeven niet meer beschikbaar. Onder het onderstaande meldingsnummer is de melding bekend bij de Autoriteit Persoonsgegevens. U heeft het meldingsnummer nodig om de melding aan te kunnen passen of in te kunnen trekken. Vermeld het meldingsnummer bij eventuele correspondentie met de Autoriteit Persoonsgegevens over de melding.

Tijdstip ontvangst	10-04-2020 13:41:38
Uniek nummer	5.1.2.e

0. Over deze melding

Gaat het om een nieuwe of bestaande melding?	Een nieuwe melding indienen
Op grond van welke wettelijke bepaling doet u deze melding?	Algemene verordening gegevensbescherming (AVG)

1. Contactgegevens en overige algemene informatie

1.1 Contactgegevens

Over welke organisatie of welk bedrijf gaat het?

Registratienummer bij de Kamer van Koophandel	09215846
Naam van het bedrijf of de organisatie	Wageningen University
Adres	Droevendaalsesteeg 4
Postcode	6708PB
Plaats	Wageningen
In welke sector is de organisatie of het bedrijf actief?	Onderwijs - Tertiair onderwijs

Wie meldt het datalek?

Naam	5.1.2.e
Functie	corporate privacy officer
E-mailadres	privacy@wur.nl
Telefoonnummer	0317 5.1.2.e

Met wie kan de Autoriteit Persoonsgegevens contact opnemen voor nadere informatie over de melding?

De melder is contactpersoon	Nee
Naam contactpersoon	5.1.2.e
Functie contactpersoon	functionaris gegevensbescherming
E-mailadres contactpersoon	dpo@wur.nl
Telefoonnummer contactpersoon	0317 5.1.2.e

1.2 Betrokkenheid andere organisatie

Was er een andere organisatie betrokken bij de inbreuk?	Ja, namelijk:
Naam van de andere organisatie die betrokken was bij de inbreuk	ADP, LLC.

In welke hoedanigheid was de andere organisatie betrokken bij de inbreuk?
ADP is de verwerker waar de inbreuk veroorzaakt is.

2. Tijdlijn

Exacte datum waarop de inbreuk was, indien bekend	09-04-2020
Startdatum van de periode waarbinnen de inbreuk was	23-03-2020
Einddatum van de periode waarbinnen de inbreuk was	09-04-2020
Duurt de inbreuk op dit moment nog voort?	Nee
Wanneer werd de inbreuk ontdekt?	09-04-2020

3. Gegevens over het datalek

3.1 Aard van de inbreuk

Inbreuk op de vertrouwelijkheid van de gegevens	Ja
Inbreuk op de integriteit van de gegevens	Nee
Inbreuk op de beschikbaarheid van de gegevens	Nee

3.2 Aard van het incident

Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest?	Persoonsgegevens per ongeluk gepubliceerd

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest

Op 31 maart jl. heeft ADP in opdracht van WUR een transitie uitgevoerd en klantgegevens van WUR verplaatst van een lokale omgeving naar de gehoste SaaS omgeving van ADP. Onderdeel van deze transitie is het opnieuw definiëren van alle koppelingen met externe systemen inclusief de bijbehorende "documentypes" (mappen met Excelbestanden). Hierbij is door ADP verzuimd de autorisaties van de documenten op de juiste manier in te richten, waardoor medewerkers van WUR inzicht hebben gehad in ”Interfaces” en ”Logbestanden”, met de mogelijkheid van downloaden van Excelbestanden met persoonsgegevens over andere medewerkers. Door sluitende logging is inmiddels duidelijk dat ca. 14 medewerkers van WUR inzicht hebben gehad in (enkele) persoonsgegevens van (in het ergste geval) alle medewerkers in loondienst van WUR (ca. 5100) en bestanden met persoonsgegevens hebben gedownload. Dit betreft salarisgegevens, uitruil van arbeidsvoorwaarden (bijv. fietsregeling), vakbondscontributie en personeelsnummers. Direct na de melding heeft ADP per documenttype de autorisaties aangepast waardoor medewerkers geen toegang meer hadden tot deze dossiers. Nader onderzoek vindt op dit moment plaats naar het aantal betrokkenen dat precies is geraakt door het incident en naar de vraag of het incident waarschijnlijk ernstige gevolgen heeft voor de rechten en vrijheden van betrokkenen (c.q. of een melding aan betrokkenen moet plaatsvinden).

4. Persoonsgegevens die betrokken zijn bij het datalek

4.1 Persoonsgegevens in het algemeen

Naam	Ja
Geslacht, geboortedatum en/of leeftijd	Nee
Burgerservicenummer (BSN)	Nee
Contactgegevens	Nee
Toegangs- of identificatiegegevens	Nee
Financiële gegevens	Ja
(Kopieën van) paspoorten of andere legitimatiebewijzen	Nee
Locatiegegevens	Nee
Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen	Nee
Onbekend / anders, namelijk:	deels nog niet bekend

4.2 Bijzondere categorieën van persoonsgegevens

Persoonsgegevens waaruit iemands ras of etnische afkomst blijkt	Nee
Persoonsgegevens waaruit iemands politieke opvattingen blijken	Nee
Persoonsgegevens waaruit iemands religieuze of levensbeschouwelijke overtuigingen blijken	Nee
Persoonsgegevens waaruit iemands lidmaatschap van een vakbond blijkt	Ja
Gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid	Nee
Gegevens over iemands gezondheid	Nee
Genetische gegevens	Nee
Biometrische gegevens	Nee

4.3 Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords ("gegevensregisters") zijn getroffen door de inbreuk	5100

5. De groep mensen van wie persoonsgegevens betrokken zijn bij het datalek

Werknemers	Ja
Klanten (huidig en potentieel)	Nee
Leerlingen of studenten	Nee
Patiënten	Nee
Minderjarigen	Nee
Personen uit kwetsbare groepen	Nee

Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk.

Medewerkers in loondienst bij Wageningen University en/of Stichting Wageningen Research.

Van minimaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?	14
Van maximaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?	5100

6. Maatregelen die zijn getroffen voordat het datalek plaatsvond

Waren de persoonsgegevens op het moment dat de inbreuk zich voordeed versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk voor onbevoegden?	Nee

7. Gevolgen van het datalek

7.1 Gevolgen van de inbreuk op de vertrouwelijkheid, de integriteit en/of de beschikbaarheid van de gegevens.

Onbevoegden hebben kennis kunnen nemen van de gegevens	Ja
De gegevens kunnen op een onbehoorlijke of onrechtmatige manier	Nee

worden misbruikt	
Er worden binnen uw eigen organisatie mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens gebruikt	Nee
Er worden mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens hergebruikt voor andere doeleinden of doorgegeven aan andere organisaties	Nee
Een essentiële dienst kan tijdelijk niet meer worden verleend aan de betrokkenen	Nee
Een essentiële dienst kan permanent niet meer worden verleend aan de betrokkenen	Nee

7.2 Lichamelijke, materiële en immateriële schade voor de betrokkenen

Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkenen?

Discriminatie	Ja
Identiteitsdiefstal of -fraude	Nee
Financiële verliezen	Nee
Reputatieschade	Nee
Verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens	Nee
Ongeoorloofde ongedaanmaking van pseudonimisering	Nee
Betrokkenen kunnen hun rechten en vrijheden niet uitoefenen	Nee
Betrokkenen worden verhinderd controle over hun persoonsgegevens uit te oefenen	Nee
Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkenen	1. Verwaarloosbaar

8. Vervolgacties naar aanleiding van het datalek

8.1 Informeren van de betrokkenen

Heeft u het datalek gemeld aan de betrokkenen of bent u van plan dat te gaan doen?	Nog niet bekend

Wat is de inhoud van de melding aan de betrokkenen?
nog niet bekend

Hoeveel betrokkenen heeft u geïnformeerd of gaat u informeren?	0
Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken om de betrokkenen te informeren?	nog niet bekend (vermoedelijk e-mail)

8.2 Maatregelen om de inbreuk aan te pakken

Welke technische en organisatorische maatregelen heeft uw organisatie getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?
Direct na de melding heeft ADP per documenttype de autorisaties aangepast waardoor medewerkers geen toegang meer hadden tot deze dossiers. ADP is een onderzoek gestart over de periode 25 maart tot 9 april welke documenttypes de properties niet goed waren ingericht. ADP onderzoekt wie er in de periode 25 maart tot 9 april onrechtmatig bestanden heeft gedownload. Naar aanleiding van dit incident zal er binnen ADP een onderzoek uitgevoerd worden naar de gevolgde procedure en zullen aanpassingen worden doorgevoerd om dit soort incidenten te voorkomen.

8.3 Internationale aspecten

Heeft de inbreuk zich voorgedaan in een grensoverschrijdende gegevensverwerking, en is de AP voor deze verwerking de leidende toezichthouder?	Nee
Heeft uw organisatie of bedrijf, het datalek gemeld bij privacytoezichthouders in een of meer	Nee

andere EU-landen, of gaat u dat nog doen?	
Heeft uw organisatie of bedrijf, het datalek gemeld bij Europese toezichthouders op andere meldplichten, of gaat u dat nog doen?	Nee

9. Overig

Is naar uw mening deze melding compleet?	Nee, er komt later een vervolgmelding met aanvullende informatie over deze inbreuk

ADP Workforce

Impact analyse toegang tot documenttypes

10-4-2020

Always Designing for People™

Vragen

- Wat is er exact gebeurd en waar is het misgegaan?
- Welke document types betrof het?
- Wie hadden mogelijk toegang tot de bewuste Document types?
- Wat was de inhoud van deze documenttypes?
- Welke info heeft men ingezien op man/vrouw niveau?
- Aanvullend willen wij natuurlijk graag weten waar in het proces het is misgegaan en welke stappen R&D gaat ondernemen om dit soort incidenten in de toekomst te voorkomen.

Wat is er exact gebeurd en waar is het misgegaan?

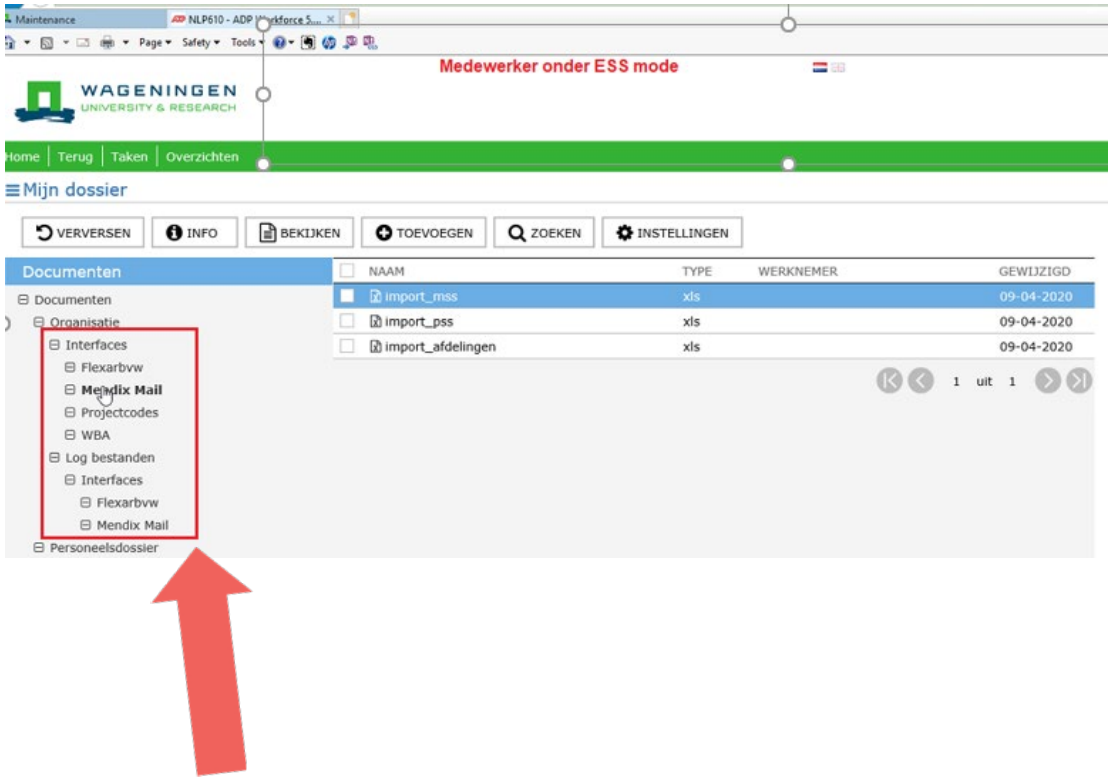
- Bij 11 nieuw ontwikkelde doctypes, benodigd voor het versturen/ontvangen en loggen van data die wordt verzonden van/naar externe systemen, zijn onterechte autorisaties uitgedeeld aan ESS, MSS, PSS.
- Deze doctypes zijn aangemaakt door een ontwikkelaar van ADP R&D vanwege de transitie lokaal naar hosting.

Hier is het fout gegaan. Deze vinkjes moesten aangevinkt worden.

- Hier is dus 5.1.5 [redacted] geen sprake van een software fout
- De fouten zijn niet naar boven gekomen bij de interne testen en de klant acceptatietesten.

Wie hadden mogelijk toegang tot de bewuste Document types?

- Als gevolg hiervan hebben alle medewerkers (rol ESS, MSS, PSS) toegang gekregen tot doctypes in de periode livegang tot 9 April 2020 9.45uur
- Niet iedereen die toegang had heeft de documenten ook gezien.
- De analyse heeft zich toegespitst op 2 zaken:
  - 1) Wie hebben de documenten geopend?
  - 2) Wat was de inhoud van de documenten die geopend zijn?



Om welke doctypes gaat het?

INTERFACE_BRIEFKOPP_LOG
INTERFACE_FLEXARBVW_DATA
INTERFACE_FLEXARBVW_LOG
INTERFACE_MEDINACTIEF_DATA
INTERFACE_MEDINACTIEF_LOG
INTERFACE_MENDIX_MAIL_DATA
INTERFACE_MENDIX_MAIL_LOG
INTERFACE_PROJECTCODES_DATA
INTERFACE_PROJECTCODES_LOG
INTERFACE_WBA_DATA
INTERFACE_WBA_LOG

Achter elk doctype worden diverse files gecreëerd, bijvoorbeeld logverslagen, Excel lijsten

Inhoud: welke informatie is zichtbaar geweest?

- ADP heeft data opgehaald uit de logtabellen van de genoemde doctypes die geopend zijn in de periode van 23 maart tot en met 9 april 2020
- Het gaat hier om 11 doctypes die relevant zijn
- 37 files achterliggende files die zichtbaar zijn geweest voor iedereen met toegang tot Workforce en een ESS, MSS, PSS rol hebben.
- Deze 37 verschillende files bevatten verschillende informatie en zijn geclassificeerd in de volgende slide
- In de bijgeleverde excel is de inhoud van de files verder gespecificeerd op veld niveau.

Welke files zijn geopend en wat is de inhoud?

Classificatie	Soort informatie zichtbaar voor niet geautoriseerde personen	Aantal files
Totaal aantal type files geopend door medewerkers ZONDER persoons gerelateerde data	Log files, afdelingen, projectnummers	25
Totaal aantal type files geopend door medewerker MET persoons gerelateerde data	Naam, uitruil arbeidsvoorwaarden (fiets, vakbond, verlof), personeelsnummer, toelage van alle medewerker	9
Totaal aantal type files MET salaris gerelateerde data voor alle medewerkers	Salaris van alle medewerkers	3

Wie heeft files geopend?

!! In totaal hebben 20 unieke medewerkers de files geopend.

Classificatie	Soort informatie zichtbaar voor niet geautoriseerde personen	Aantal unieke medewerkers die deze files hebben geopend
Totaal aantal type files geopend door medewerkers ZONDER persoons gerelateerde data	Log files, afdelingen, projectnummers	15
Totaal aantal type files geopend door medewerker MET persoons gerelateerde data	Naam, uitruil arbeidsvoorwaarden (fiets, vakbond, verlof), personeelsnummer, toelage	12
Totaal aantal type files MET salaris gerelateerde data voor alle medewerkers	Salaris van alle medewerkers	8

!! Een lijst van de desbetreffende medewerker die documenten hebben geopend is meegeleverd in de excel (loginnamen)

Acties ADP

1. Onderzoek nav het niet juist configureren van de doctypes. Hier kunnen proceswijzigingen uit voortkomen.

2. Wijziging in de software: nieuwe doctypes worden onzichtbaar opgeleverd en dienen actief geautoriseerd te worden. Oplevering in de eerstvolgende release.

Aanvullende opmerkingen

- Het is niet vast te stellen of desbetreffende medewerkers de files hebben opgeslagen of hebben verspreid omdat dit niet in ADP Workforce wordt vastgelegd.

- Iedere medewerker heeft waarschijnlijk een download directory. Hierin landen de bestanden die van het internet komen (browser afhankelijk). Advies: delete de inhoud van de download directory bij alle medewerkers.

Privacy

Van: 5.1.2.e
Verzonden: vrijdag 10 april 2020 13:48
Aan: 5.1.2.e
Onderwerp: Melding AP
Bijlagen: 20200410_voorlopige_melding_ADP.pdf

Ha 5.1.2.e hierbij de melding bij de AP van vandaag naar aanleiding van het ADP-incident.

Groet, 5.1.2.e

5.1.2.e
5.1.2.e | Corporate Governance & Legal Services
Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e | Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. +31 317 5.1.2.e

Privacy

Van: 5.1.2.e
Verzonden: vrijdag 10 april 2020 11:19
Aan: 5.1.2.e
Onderwerp: FW: SPOED!! Datalek in Workforce!

Urgentie: Hoog

Met vriendelijke groet,

5.1.2.e

From: 5.1.2.e
Sent: donderdag 9 april 2020 9:19
To: 5.1.2.e @wur.nl>
Subject: FW: SPOED!! Datalek in Workforce!
Importance: High

Hoi 5.1.2.e

Ter info.

Met vriendelijke groet/Kind regards,

5.1.2.e
Senior Functioneel Applicatiebeheerder

Aanwezig: maandag t/m vrijdag
Wageningen University & Research
Corporate HR - Shared Service Center
Postbus 9101, 6700 HB Wageningen
Wageningen Campus - Gebouw 104 (Atlas)
Droevendaalsesteeg 4, 6708 PB Wageningen
T: 0317 5.1.2.e
E: 5.1.2.e @wur.nl
www.disclaimer-nl.wur.nl

www.wur.nl

bijzondere) persoonsgegevens kunnen. Sla niet méér persoonsgegevens op dan je strikt genomen nodig hebt en vernietig wat je niet (meer) nodig hebt.
Voor meer informatie: https://intranet.wur.nl/umbraco/nl/over-wur/beleid-regelingen/privacy-persoonsgegevens-avg/ en https://www.wur.nl/nl/Over-Wageningen/Integriteit-en-privacy.htm

---

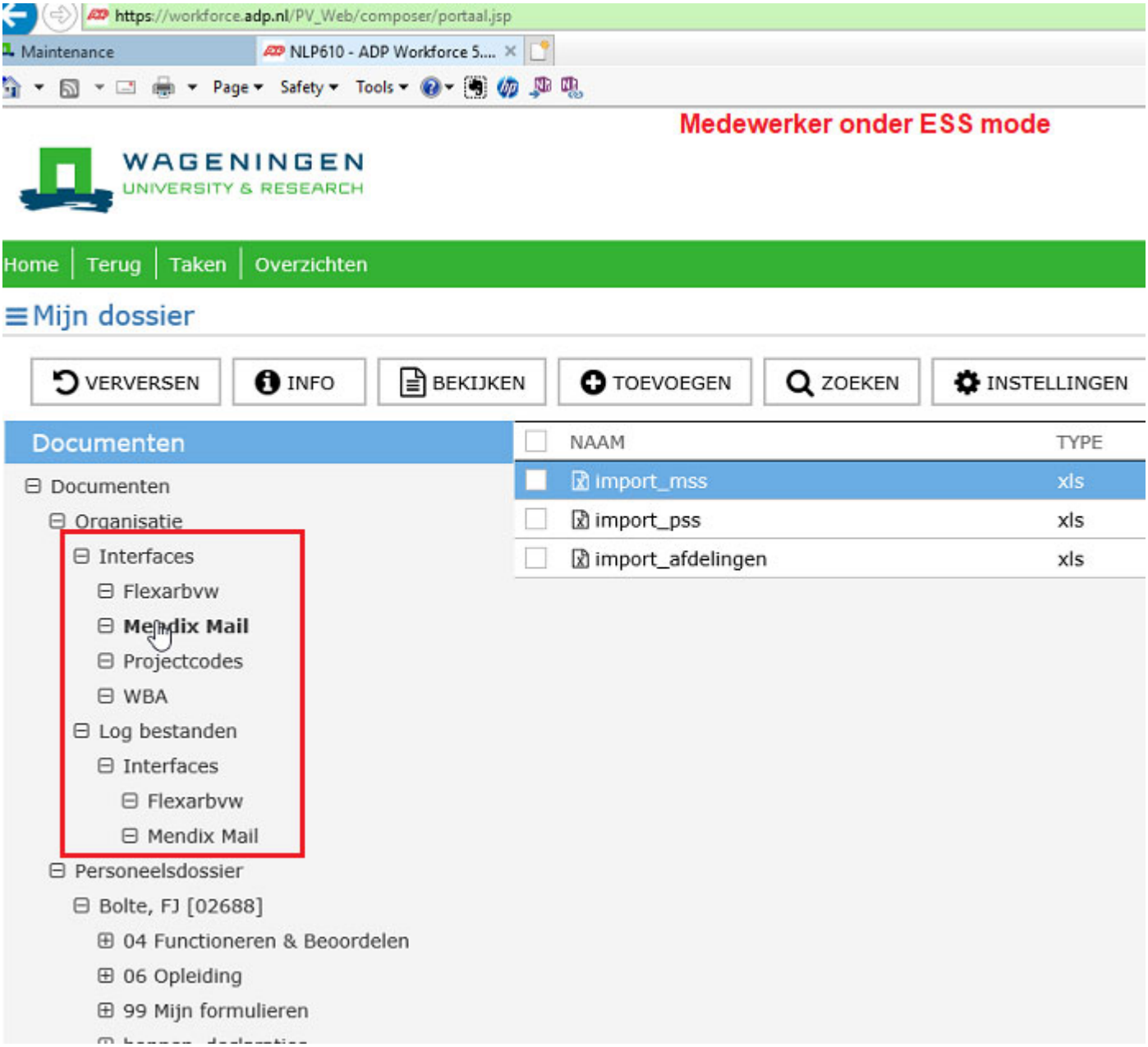
Van: 5.1.2.e
Verzonden: donderdag 9 april 2020 09:15
Aan: 5.1.2.e @adp.com) 5.1.2.e @adp.com>
CC: 5.1.2.e @adp.com) 5.1.2.e @adp.com>; 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>; 5.1.2.e @adp.com>
Onderwerp: SPOED!! Datalek in Workforce!
Urgentie: Hoog

Goedemorgen 5.1.2.e

Ik ben zojuist gebeld door onze Servicedesk IT met de mededeling dat er een datalek is geconstateerd in Workforce.

Zie onderstaand screenshot. Alle medewerkers hebben inzage op de folders “Interfaces” en “Logbestanden”. Hierin staan allerlei persoonsgegevens erin. Graag dit onmiddelijk laten afschermen. De rest van de folders zijn gelukkig wel afgeschermd.

Kunnen we ook eventueel zien, welke medewerkers deze folders hebben geraadpleegd?



Met vriendelijke groet/Kind regards,

5.1.2.e
Senior Functioneel Applicatiebeheerder

Aanwezig: maandag t/m vrijdag
Wageningen University & Research
Corporate HR - Shared Service Center
Postbus 9101, 6700 HB Wageningen
Wageningen Campus - Gebouw 104 (Atlas)
Droevendaalsesteeg 4, 6708 PB Wageningen
T: 0317-5.1.2.e
E: 5.1.2.e @wur.nl
www.disclaimer-nl.wur.nl

WAGENINGEN
UNIVERSITY & RESEARCH

www.wur.nl

Betreft dit een bericht verzonden van een noreply@WUR.nl of niet persoonlijk e-mailadres verzoeken wij u de melding te doen aan hr.servicedesk@WUR.nl

HR privacy disclaimer
Wageningen University & Research heeft een zorgplicht voor persoonsgegevens die wij nodig hebben van onze medewerkers en studenten. Op 25 mei 2018 is het wettelijk kader van de Algemene verordening gegevensbescherming (AVG) van toepassing. Mocht dit e-mailbericht of een bijgesloten bijlage persoonsgegevens bevatten leg hiervan dan geen schaduwdossiers aan, werk zoveel mogelijk in een (extra) beveiligde digitale omgeving en zorg dat alleen geautoriseerde medewerkers bij (gevoelige of bijzondere) persoonsgegevens kunnen. Sla niet méér persoonsgegevens op dan je strikt genomen nodig hebt en vernietig wat je niet (meer) nodig hebt.
Voor meer informatie: https://intranet.wur.nl/umbraco/nl/over-wur/beleid-regelingen/privacy-persoonsgegevens-avg/ en https://www.wur.nl/nl/Over-Wageningen/Integriteit-en-privacy.htm

Privacy

Van: 5.1.2.e
Verzonden: donderdag 9 april 2020 9:19
Aan: 5.1.2.e
Onderwerp: Datalek

Urgentie: Hoog

Hoi beide,

Er is op dit moment een datalek aanwezig in workforce waardoor een hoop persoonsgegevens ingezien kunnen worden.
Dit wordt z.s.m. gerepareerd, daarna gaan we kijken of we in logs kunnen terugzien wie de bestanden geopend heeft.
Ik wil graag even met een van jullie overleggen maar krijg jullie telefonisch niet te pakken.

Met vriendelijke groet,

5.1.2.e
Proces manager

Aanwezig: maandag t/m donderdag
Wageningen University & Research
Afdeling Informatie Technologie
Postbus 59, 6700 AB, Wageningen
Gebouw 116, Akkermaalsbos 12, 6708 WB Wageningen
Tel: 0317-5.1.2.e
5.1.2.e @wur.nl
www.wur.nl

Privacy

Van: 5.1.2.e
Verzonden: vrijdag 10 april 2020 13:48
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: RE: Datalek WUR SSC HR 9 april 2020

Beste heren,

Ik heb het incident voorlopig gemeld bij de AP. Wat mij betreft is er nog een aantal zaken nodig om die melding definitief te maken:

1. Hoeveel betrokkenen zijn precies geraakt door het incident (hoeveel records per medewerker stonden in de gedownloade files)?
2. Betreft het maximaal 5131 medewerkers? Hoeveel medewerkers heeft WUR nu?
3. Heeft het incident waarschijnlijk ernstige gevolgen voor de rechten en vrijheden van medewerkers (c.q. moet een melding aan betrokkenen plaatsvinden)? Dat hangt met name af of de Exceldocumenten kunnen worden teruggehaald/verwijderd en de medewerkers bevestigen niets met de data te hebben gedaan. ADP's suggestie om de 'downloadmap' leeg te gooien bij iedereen kan natuurlijk niet zomaar. Mijn suggestie is om de 14 medewerkers die bestanden hebben gedownload (buiten IT) persoonlijk te benaderen. Met name de personen die Optare_bronnen_vakbondscontributie.xls hebben gedownload. Maar wellicht hebben jullie hier nog een betere suggestie voor.

Groet, 5.1.2.e

5.1.2.e
5.1.2.e | Corporate Governance & Legal Services

Wageningen University & Research
P.O. Box 9101, 6700 HB Wageningen, The Netherlands
B:104 (Atlas) | 5.1.2.e Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. +31 317 5.1.2.e
www.wur.nl/disclaimer

Van: 5.1.2.e @wur.nl>
Verzonden: vrijdag 10 april 2020 12:32
Aan: 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
Onderwerp: RE: Datalek WUR SSC HR 9 april 2020

Dag heren,

Ik heb zojuist de impact analyse i.v.m. datalek van ADP ontvangen, zie powerpoint bijlage. Tevens hebben ze ook een excelbestand meegeleverd waarop te zien welke medewerkers de betreffende document(en) hebben de geraadpleegd. Zoals 5.1.2.e had al aangegeven heb ik de excellijst voorzien van extra info, zie geel gearceerde kolommen.

Groet,

5.1.2.e

Van: 5.1.2.e
Verzonden: vrijdag 10 april 2020 12:28
Aan: 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>; R 5.1.2.e @wur.nl>

CC: 5.1.2.e @wur.nl>
Onderwerp: RE: Datalek WUR SSC HR 9 april 2020

Hoi 5.1.2.e
Ik hoor net dat 5.1.2.e de analyse ontvangen heeft.
Hij stuurt hem naar jullie door met aanvullingen welke gebruikers achter de genoemde ADP accounts staan.
Groet, 5.1.2.e

Van: 5.1.2.e
Verzonden: vrijdag 10 april 2020 12:08
Aan: 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
CC: 5.1.2.e @wur.nl>
Onderwerp: RE: Datalek WUR SSC HR 9 april 2020

Hoi 5.1.2.e

Ik probeerde je net even kort te bellen.
Ik ga er even vanuit dat jij dit formulier zelf hebt gevuld? Of was dit de eerste inschatting/analyse vanuit adp al?

Als de analyse van adp nog moet komen kan die dan z.s.m. worden doorgestuurd, ook naar 5.1.2.e (legal services), we wachten nog op deze voor het doen van de aanmelding bij de Autoriteit Persoonsgegevens.

Met vriendelijke groet,

5.1.2.e

From: 5.1.2.e
Sent: vrijdag 10 april 2020 10:10
To: 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
Subject: RE: Datalek WUR SSC HR 9 april 2020

Hallo 5.1.2.e

Klopt, MyHr is voorbehouden aan WUR medewerkers in verschillende rollen (medewerkers, HR professionals, leidinggevenden enz.)

Met vriendelijke groet,

5.1.2.e
Aanwezig: maandag t/m vrijdag
Wageningen University & Research
Afdeling Corporate HR
Postbus 9101, 6700 HB Wageningen
Gebouw 104 (Atlas), Droevendaalsesteeg 4, 6708 PB Wageningen
Tel.: 0031-6 5.1.2.e
5.1.2.e @wur.nl
www.wur.nl
www.disclaimer-nl.wur.nl

From: 5.1.2.e
Sent: Friday, April 10, 2020 9:32 AM
To: 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
Subject: RE: Datalek WUR SSC HR 9 april 2020

Hoi Beide,

Ik zal het meenemen naar 5.1.2.e . We hebben er al een ticket van dus de servicedesk hoeft niet in communicatie meegenomen te worden.
Bij de vraag over de gebruikersgroep was het alleen inzichtelijk voor mensen die in MyHR kunnen. Dit zijn naar mijn weten alleen medewerkers WUR toch?

Met vriendelijke groet,

5.1.2.e

From: 5.1.2.e
Sent: vrijdag 10 april 2020 8:45
To: 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
Subject: RE: Datalek WUR SSC HR 9 april 2020

5.1.2.e
Hoe loopt de procedure verder?
Lever jij het aan bij 5.1.2.e die de voorlopige melding doet?
Groet, 5.1.2.e

Van: 5.1.2.e
Verzonden: vrijdag 10 april 2020 08:36
Aan: Servicedesk IT <servicedesk.it@wur.nl>
CC: 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
Onderwerp: Datalek WUR SSC HR 9 april 2020

Hallo collega,

Hierbij een meldingsformulier datalek

Met vriendelijke groet,

5.1.2.e

Aanwezig: maandag t/m vrijdag
Wageningen University & Research
Afdeling Corporate HR
Postbus 9101, 6700 HB Wageningen
Gebouw 104 (Atlas), Droevendaalsesteeg 4, 6708 PB Wageningen
*Tel.: 0031-*5.1.2.e
5.1.2.e @wur.nl
www.wur.nl
www.disclaimer-nl.wur.nl

Privacy

Van: Functionarisgegevensbescherming
Verzonden: maandag 12 oktober 2020 19:14
Aan: 5.1.2.e
Onderwerp: RE: Melding datalek bij AP - verzoek accountant
Bijlagen: 20200410_voorlopige_melding_ADP.pdf; 20200424_vervolgmelding_ADP.pdf

Hallo 5.1.2.e

Zie bijgaand de stukken. Het is overigens de Autoriteit Persoonsgegevens (AP) en niet de APG.

Met vriendelijke groet,

5.1.2.e

WAGENINGEN
UNIVERSITY & RESEARCH

5.1.2.e | Functionaris Gegevensbescherming | Wageningen University & Research | Postbus 9101, 6700 HB Wageningen | +31 (0)317 5.1.2.e | www.wur.nl

---

From: 5.1.2.e @wur.nl>
Sent: Monday, October 12, 2020 6:13 PM
To: 5.1.2.e @wur.nl>
Subject: Melding datalek bij AP - verzoek accountant

Beste 5.1.2.e

Tbv de interimcontrole bekijkt de externe accountant altijd de RvB notulen.
N.a.v. onderstaande uit de notulen willen ze graag 'het bewijs' dat het datalek is gemeld aan de APG.
Kan jij de mail of andere documentatie aan me toesturen die je daartoe aan de APG hebt verzonden?

Dank, 5.1.2.e

RvB 20 april 2020:
10.04 Er wordt kort genoemd dat er zich een **datalek** heeft voorgedaan. Dit is reeds bij de APG gemeld. Het behoeft nadere communicatie, dat wordt 22 april in de RvB besproken.

RvB 22 april 2020:
3. Onderwerpen Corporate Human Resource
3.01 Datalek
De RvB neemt kennis van de rapportage inzake de analyse van het datalek, ontstaan door een menselijke fout bij de leverancier van het personeels- en salarissysteem. De RvB besluit tot verspreiding van het communicatiebericht hierover naar 5.131 actieve medewerkers in de database. De RvB verzoekt te verduidelijken waarom de overige medewerkers niet zijn betrokken en te overwegen om het bericht naar alle medewerkers toe te zenden.

5.1.2.e
Governance & Legal Services

Wageningen University & Research
Postbus 9101, 6700 HB, Wageningen
Droevendaalsesteeg 4, Gebouw 104, 6708 PB, Wageningen
Tel.: 0317 - 5.1.2.e
Mail: 5.1.2.e @wur.nl
www.wur.nl
www.wur.nl/nl/disclaimer.htm

Privacy

Van: 5.1.2.e
Verzonden: dinsdag 14 april 2020 12:01
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: RE: Datalek WUR SSC HR 9 april 2020

Dag 5.1.2.e

Ik heb de bestanden geanalyseerd en in kaart gebracht om hoeveel medewerkers dit gaat.

1. **Hoeveel betrokkenen zijn precies geraakt door het incident (hoeveel records per medewerker stonden in de gedownloade files)?**

    - 1) opt_part_salaris.xls = aantal medewerkers 6525
    - 2) optare_bruto_salaris.xls = aantal medewerkers 4975
    - 3) optare_doel_extra_verlofuren.xls = aantal medewerkers 473
    - 4) optare_doel_fiets.xls =aantal medewerkers 460
    - 5) optare_doel_reiskosten.xls =aantal medewerkers 2689
    - 6) optare_doel_vakbond.xls = aantal medewerkers 347
    - 7) optare_mutaties_reiskosten.xls = aantal medewerkers 6125
    - 8) optare_opbouw_min_vu.xls = aantal medewerkers 6567
    - 9) optare_vaste_toelagen.xls = aantal medewerkers 743
    - 10) Import MSS = aantal medewerkers 507 (Dit bestand bevat niet echt persoonsgegevens. De naam en emailadressen staan ook in We@WUR/outlook adressenbestand)
    - 11) Import PSS = aantal medewerkers 359 (Dit bestand bevat niet echt persoonsgegevens. De naam en emailadressen staan ook in We@WUR/outlook adressenbestand)

Van al deze bestanden dat onder hoger risico zou kunnen vallen zijn de bruto salaris gegevens.

2. **Betreft het maximaal 5131 medewerkers? Hoeveel medewerkers heeft WUR nu?**

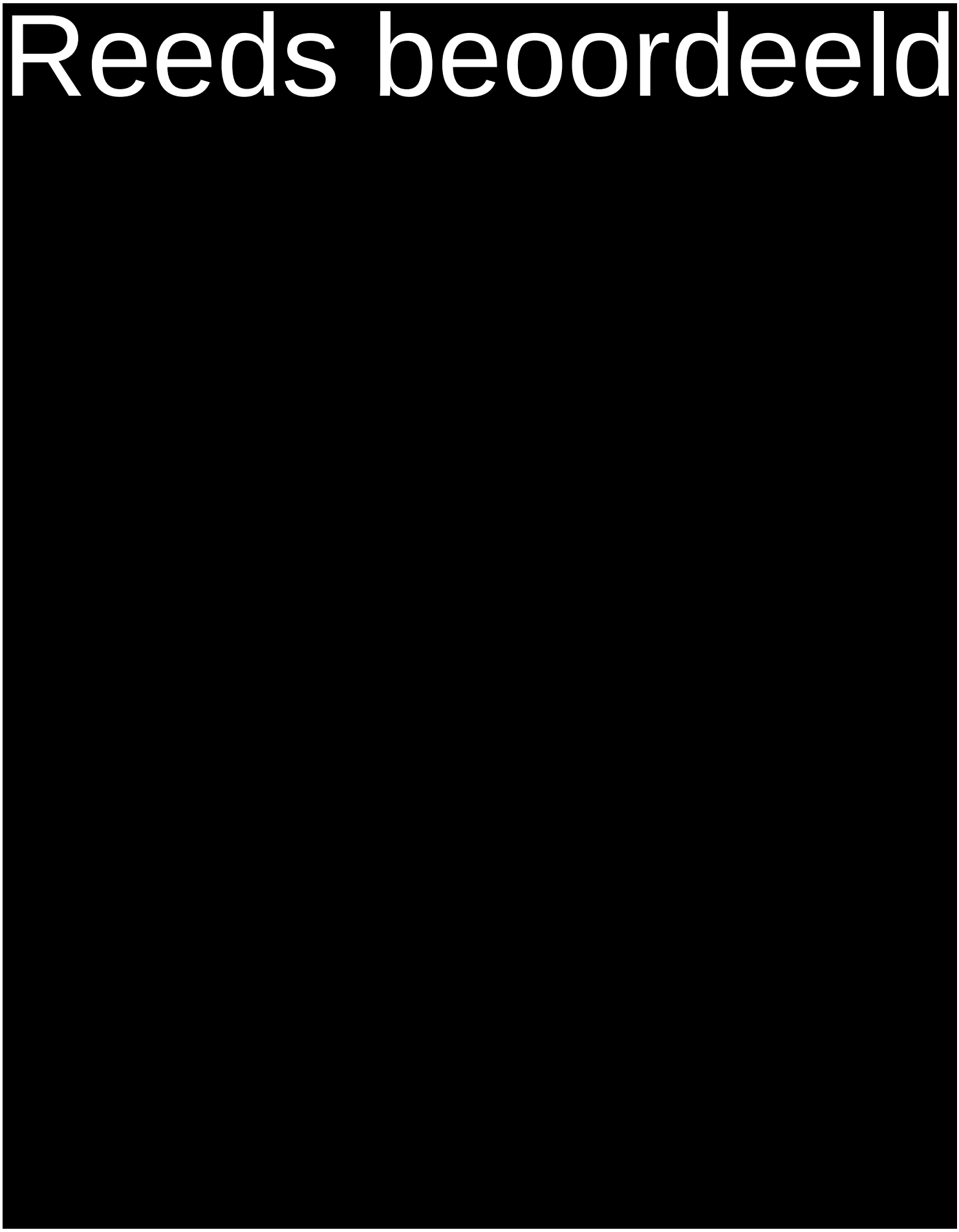
Volgens peilmoment 13-04-2020 zijn bij 6567 medewerkers soort Flexibele arbeidsvoorwaarden regeling tot nu toe gemuteerd. Dit wilt niet zeggen dat al deze medewerkers daadwerkelijk een optare keuze hebben gemaakt. De soort code dat ingevuld is in element Flexibele regeling bepaalt de condities welke keuzes de medewerker mag maken. Voorbeeld medewerkers met een lease auto mogen geen gebruik maken van fiscale uitruil voor extra reiskosten. Tevens bepaalt het bestand hoeveel een medewerker aan minimum vakantie-uitkering moest overhouden. Op basis van brutosalaris kon dit worden berekend.

3. **Heeft het incident waarschijnlijk ernstige gevolgen voor de rechten en vrijheden van medewerkers (c.q. moet een melding aan betrokkenen plaatsvinden)? Dat hangt met name af of de Exceldocumenten kunnen worden teruggehaald/verwijderd en de medewerkers bevestigen niets met de data te hebben gedaan. ADP's suggestie om de 'downloadmap' leeg te gooien bij iedereen kan natuurlijk niet zomaar. Mijn suggestie is om de 14 medewerkers die bestanden hebben gedownload (buiten IT) persoonlijk te benaderen. Met name de personen die Optare_bronnen_vakbondscontributie.xls hebben gedownload. Maar wellicht hebben jullie hier nog een betere suggestie voor.**

Het enige wat we kunnen doen om iedere medewerker die mogelijk de bestand(en) heeft gedownload persoonlijk te benaderen. Dit moeten we nog intern afstemmen.

Vriendelijke groet,

5.1.2.e



ADP Workforce

Impact analyse toegang tot documenttypes

15 april 2020

Vragen

- Wat is er exact gebeurd en waar is het misgegaan?
- Welke document types betrof het?
- Wie hadden mogelijk toegang tot de bewuste document types?
- Wat was de inhoud van deze documenttypes?
- Aanvullend wil WUR natuurlijk graag weten waar in het proces het is misgegaan en welke stappen ADP gaat ondernemen om dit soort incidenten in de toekomst te voorkomen.

Wat is er exact gebeurd en waar is het misgegaan?

- Bij 11 nieuw ontwikkelde doctypes, benodigd voor het versturen/ontvangen en loggen van data die wordt verzonden van/naar externe systemen, zijn onterechte autorisaties uitgedeeld aan ESS, MSS, PSS (rollen op nivo: employee, manager en HR professional).

- Deze doctypes zijn aangemaakt door een ontwikkelaar van ADP R&D vanwege de transitie lokaal naar cloud.

Hier is het fout gegaan. Deze vinkjes moesten aangevinkt worden.

- Hier is dus 5.1.5 geen sprake van een software fout

Opmerking 5.1.2.e: Alle vinkjes Standaard mogen niet aangezet worden!

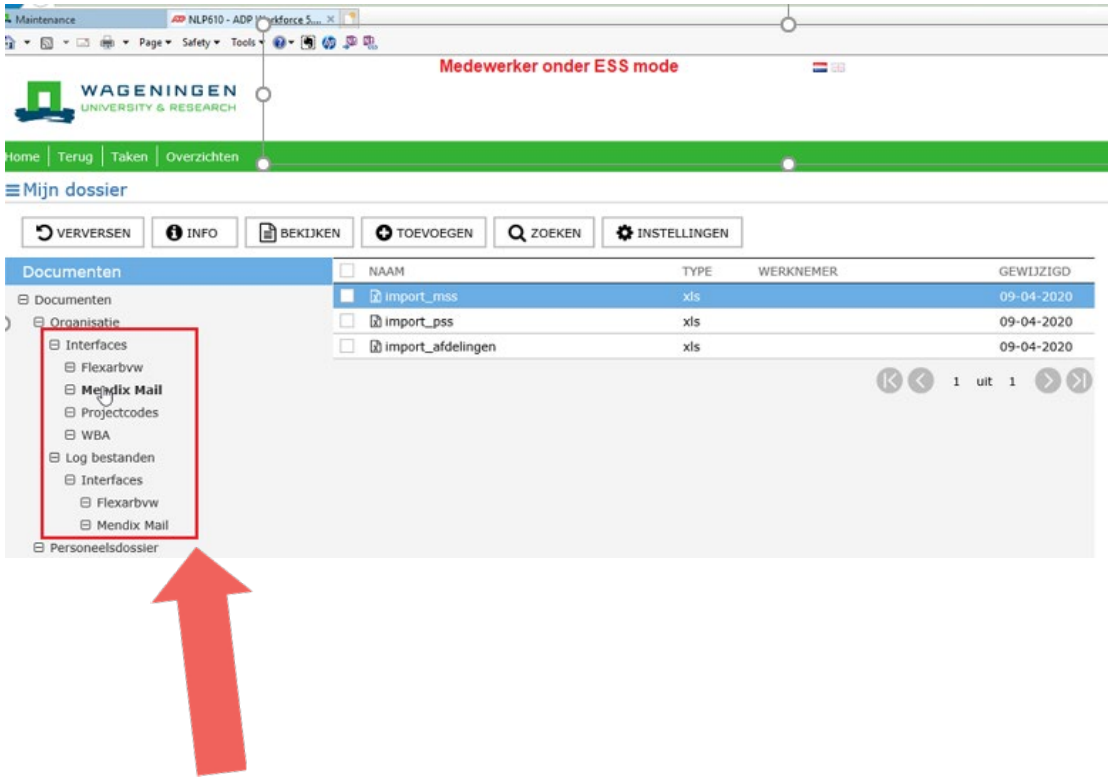
- De fouten zijn niet naar boven gekomen bij de interne testen ADP en de klant acceptatietesten. In tegenstelling tot de lokale omgeving waarbij deze bestanden op een beveiligde omgeving werden opgeslagen is er in de cloud situatie sprake van dat deze bestanden worden opgeslagen in de digitale dossier omgeving. Deze veranderende werkwijze was wel bekend bij WUR maar niet bekend als een documenttype, maar PPL files en derhalve ook niet getest.

Wie hadden mogelijk toegang tot de bewuste Document types?

- Als gevolg hiervan hebben alle medewerkers (rol ESS, MSS, PSS) toegang gekregen tot doctypes in de periode livegang (25 maart 2020) tot 9 April 2020 9.45 uur

- Niet iedereen die toegang had heeft de documenten ook gezien.

- De analyse heeft zich toegespitst op 2 zaken:
  - 1) Wie hebben de documenten geopend?
  - 2) Wat was de inhoud van de documenten die geopend zijn?



Inhoud: welke informatie is zichtbaar geweest?

- ADP heeft data opgehaald uit de logtabellen van de genoemde doctypes die geopend zijn in de periode van 23 maart tot en met 9 april 2020
- Het gaat hier om 11 doctypes die relevant zijn
- 37 files achterliggende files die zichtbaar zijn geweest voor iedereen met toegang tot Workforce en een ESS, MSS, PSS rol hebben. Op peildatum 13 april 2020 had WUR 6567 actieve medewerkers in dienst. Hiervan hebben op basis van hun rol 5131 medewerkers toegang tot de achterliggende files. Hiervan hebben er 14 daadwerkelijke toegang gehad
- Deze 37 verschillende files bevatten verschillende informatie en zijn geclassificeerd in de volgende slide
- ADP heeft de inhoud van de files verder gespecificeerd op veld niveau.

Welke files zijn geopend en wat is de inhoud?

Classificatie	Soort informatie zichtbaar voor niet geautoriseerde personen	Aantal files
Totaal aantal type files geopend door medewerkers ZONDER persoons gerelateerde data	Log files, afdelingen, projectnummers	25
Totaal aantal type files geopend door medewerker MET persoons gerelateerde data	Naam, uitruil arbeidsvoorwaarden (fiets, vakbond, verlof), personeelsnummer, toelage van alle medewerkers	9
Totaal aantal type files MET salaris gerelateerde data voor alle medewerkers	Salaris van alle medewerkers	3

Wie heeft files geopend?

!! In totaal hebben 20 unieke medewerkers de files geopend (waarvan 6 medewerkers vanuit rollen IT na melding).

Classificatie	Soort informatie zichtbaar voor niet geautoriseerde personen	Aantal unieke medewerkers die deze files hebben geopend
Totaal aantal type files geopend door medewerkers ZONDER persoons gerelateerde data	Log files, afdelingen, projectnummers	15
Totaal aantal type files geopend door medewerker MET persoons gerelateerde data	Naam, uitruil arbeidsvoorwaarden (fiets, vakbond, verlof), personeelsnummer, toelage	12
Totaal aantal type files MET salaris gerelateerde data voor alle medewerkers	Salaris van alle medewerkers	8

!! Een lijst van de desbetreffende medewerkers die documenten hebben geopend is aangeleverd in separate opgave

Acties ADP

1. Onderzoek nav het niet juist configureren van de doctypes.

2. Verslaglegging naar WUR van de bevindingen door ADP

3. Wijziging in de software: nieuwe doctypes worden onzichtbaar opgeleverd en dienen actief geautoriseerd te worden. Oplevering in de eerstvolgende release.

Acties WUR

- Melding datalek via de daarvoor gestelde procedure op 10 april 2020
- Melding (voorlopig in afwachting nadere informatie) Autoriteit Persoonsgegevens op 10 april 2020.
- Definitieve Analyse ADP ontvangen op 14 april 2020
- Het is niet vast te stellen of desbetreffende medewerkers de files hebben opgeslagen of hebben verspreid omdat dit niet in ADP Workforce wordt vastgelegd. WUR (IT) heeft hierop (op 15 april 2020) de betreffende 14 gebruikers verzocht om het (eventueel gedownloade) bestand(en) per direct te verwijderen, gevraagd of ze het niet verder verspreid hebben, en IT dit via email te bevestigen.
- Bespreekpunten 16 april 2020: vervolgactie AP, communicatie organisatie, reactie naar ADP direktie etc.

Van: 5.1.2.e
Aan: 5.1.2.e
Onderwerp: Datalek ADP / melding betrokkenen

Beste allen,

Op 9 april jl. is een datalek gesignaleerd met betrekking tot personeelsgegevens van (medewerkers van) WUR. Hierbij is door een aantal medewerkers van WUR o.a. een bestand gedownload met salarisgegevens van 6525 medewerkers van WUR, een bestand met verlofuren van 473 medewerkers en een bestand met 347 specificaties voor vakbondscontributies.

5.1.2.e en ik hebben de situatie beoordeeld en hebben het incident gemeld aan de Autoriteit Persoonsgegevens.

Wij komen tot de conclusie dat dit incident gemeld moet worden aan alle betrokkenen binnen WUR. Met name gezien de aard (salaris, vakbondslidmaatschap, arbeidsvoorwaarden) en omvang van het lek en omdat niet met zekerheid uit te sluiten valt dat de medewerkers die dit bestand hebben gedownload het niet verwijderen en verwijderd houden. Dit betekent dat een melding gedaan moet worden aan de 6525 medewerkers.

Overeenkomstig het beleid voor dit soort incidenten escaleren 5.1.2.e en ik dit naar deze groep. Dit team bestaat uit de FG, CPO, de ISO, de woordvoerder en situationele eigenaar.

Ik stel voor a.s. donderdag te bespreken hoe (e-mail?) en wat we aan betrokkenen gaan melden.

Vriendelijke groet,
5.1.2.e

.....

Join Skype Meeting <https://meet.wur.nl/peter.ras/S9W44NFK>

Trouble Joining? Try Skype Web App <https://meet.wur.nl/peter.ras/S9W44NFK?sl=1>

Join by phone

+31317489100 <tel:+31317489100> (31) Engels (Verenigd Koninkrijk)

Find a local number <https://dialin.wur.nl>

Conference ID: 7609261

Forgot your dial-in PIN? <https://dialin.wur.nl> |Help <https://o15.officeredir.microsoft.com/r/rlidLync15?clid=1043&p1=5&p2=2009>

If you are unable to connect from your videoconferencing equipment using the Join Skype Meeting link above, you can join the meeting by connecting to: wur@vc.wur.nl <mailto:wur@vc.wur.nl> and enter the Conference ID followed by #.

[!OC([1033])!]

.....

Privacy

Van: 5.1.2.e
Verzonden: vrijdag 15 mei 2020 11:00
Aan: Privacy
Onderwerp: RE: Datalek / Data breach

Opvolgingsvlag: Opvolgen
Vlagstatus: Voltooid

Hallo 5.1.2.e

Dank voor je snelle reactie en duidelijke antwoorden. Mochten er nog aanvullende vragen komen vanuit de medezeggenschap dan neem ik contact met je op.

Met vriendelijke groet,
5.1.2.e

Wageningen University & Research
T: +31 320 5.1.2.e (schakelt door naar mobiel)
M: +31 6 5.1.2.e (sms, app, facetime)

From: Privacy
Sent: vrijdag 15 mei 2020 9:06
To: 5.1.2.e @wur.nl>
Cc: 5.1.2.e @wur.nl>; HR Servicedesk <hr.servicedesk@wur.nl>
Subject: RE: Datalek / Data breach

Beste 5.1.2.e

Hieronder ga ik in op de vragen in je e-mail. Ik vertrouw erop hiermee je vragen voldoende te hebben beantwoord.

Vriendelijke groet,
5.1.2.e

5.1.2.e
Corporate Privacy Officer 5.1.2.e
Tel. +31 317 5.1.2.e

Van: 5.1.2.e @wur.nl>
Verzonden: donderdag 14 mei 2020 11:32
Aan: Privacy <privacy@wur.nl>
CC: 5.1.2.e @wur.nl>
Onderwerp: FW: Datalek / Data breach

Hallo 5.1.2.e
Nav onderstaand bericht heeft de medezeggenschap van WUR een aantal vragen:

1. **Hoe heeft dit kunnen gebeuren?**
2. **Zat de fout, bij de werkzaamheden, bij WUR of bij ADP/leverancier?**

Op 25 maart jl. heeft ADP in opdracht van WUR een transitie uitgevoerd en klantgegevens van WUR verplaatst van een lokale omgeving naar de gehoste SaaS omgeving van ADP. Onderdeel van deze transitie is het opnieuw definiëren van alle koppelingen met externe systemen inclusief de

bijbehorende "documenttypes" (mappen met Excelbestanden). Hierbij is door ADP door een menselijke fout verzuimd de autorisaties van de documenttypes op de juiste manier in te richten, waardoor medewerkers van WUR inzicht hebben gehad in bestanden waar zij niet toe geautoriseerd waren.

3. Van hoeveel mensen is er informatie gedownload en hebben al deze medewerkers onderstaand bericht ontvangen?

De gegevens van iedereen die de datalekmelding heeft ontvangen zijn betrokken in de gecompromitteerde verzamelbestanden. Het gaat daarbij om alle medewerkers van WUR die op basis van de arbeidsovereenkomsten rechten kunnen doen gelden op Optare 'verruilen woon werk vergoeding'.

4. Welke gegevens konden worden gedownload en ging het hier om verzamelbestanden of individuele bestanden?

Er zijn geen individuele bestanden of salarisstroken ingezien. Het gaat om inzage in een groot verzamelbestand met een aantal categorieën persoonsgegevens, waaronder naam, salaris en recente Optare-uitruil.

5. In welke periode was downloaden van deze informatie mogelijk, door hoeveel personen is dit gedaan en hoe is met hen hierover gecommuniceerd?

Het incident heeft plaatsgevonden in de periode tussen 25 maart en 9 april jl. Wij hebben vastgesteld dat in totaal acht niet-geautoriseerde personen binnen WUR in die periode toegang hebben gehad tot deze persoonsgegevens. Wij verstrekken geen verdere details over hun identiteit. Wij hebben contact opgenomen met de betreffende personen, de gedownloade bestanden verwijderd en van hen de bevestiging ontvangen dat de bestanden verwijderd zijn en niet verder zijn verspreid. Overigens is er geen enkele indicatie van kwade opzet; het was niet op voorhand duidelijk welke gegevens in de verzamelbestanden stonden.

6. Hoe en door welke partij is het lek ontdekt en gemeld?

Het incident is gemeld door één van de medewerkers die ontdekte dat hij/zij bij bestanden kon waar hij/zij normaal niet bij zou moeten kunnen.

7. Welke acties zijn er na melding van het lek (naast onderstaand bericht) uitgevoerd in het kader van ons AVG beleid?

Overeenkomstig de AVG/ons beleid hebben wij de Autoriteit Persoonsgegevens en alle betrokkenen geïnformeerd.

8. Wat wordt er gedaan om te voorkomen dat dit nogmaals gebeurt?

Direct na de melding heeft ADP per documenttype de autorisaties aangepast waardoor medewerkers geen toegang meer hadden tot deze dossiers. ADP is een onderzoek gestart over de periode 25 maart tot 9 april welke documenttypes de properties niet goed waren ingericht. ADP heeft onderzocht wie er in de periode 25 maart tot 9 april 2020 onrechtmatig bestanden heeft gedownload. Naar aanleiding van dit incident zal er binnen ADP een onderzoek uitgevoerd worden naar de gevolgde procedure en zullen aanpassingen worden doorgevoerd om dit soort incidenten te voorkomen.

Graag ontvang ik je reactie zodat ik deze kan delen met de centrale MZ.

Met vriendelijke groet,
5.1.2.e

WAGENINGEN

5.1.2.e

Wageningen University & Research
Business Unit Open Teelten
Postbus 430, 8200 AK Lelystad
Edelhertweg 1, 8219 PH Lelystad → route
T +31 320 5.1.2.e (schakelt door naar mobiel)
M +31 6 5.1.2.e (sms, app, facetime)
E 5.1.2.e @wur.nl
W wur.nl/openteelten
Skype 5.1.2.e
Over mij


From: HR Servicedesk
Sent: donderdag 23 april 2020 21:26
Cc: HR Servicedesk <hr.servicedesk@wur.nl>
Subject: Datalek / Data breach

Beste collega,

Onlangs is, tijdens werkzaamheden aan het salarissysteem, een fout gemaakt. Daardoor was het korte tijd mogelijk voor niet geautoriseerde medewerkers van WUR om de gedetailleerde salarisgegevens van alle personeelsleden in te zien.
Inzage was mogelijk bij medewerkers die op basis van onze arbeidsvoorwaarden recht kunnen doen gelden op uitruil woon-werkverkeer Optare. De menselijke fout werd binnen een half uur na ontdekking hersteld.

We hebben kunnen nagaan dat een klein aantal collega's daadwerkelijk bestanden heeft bekeken en/of gedownload. Na contact met deze collega's hebben we kunnen vaststellen dat er niets met deze gegevens is gedaan en dat ze niet verder zijn gedeeld.

We bieden onze welgemeende excuses aan voor het ontstaan van dit incident. Uiteraard zijn we in gesprek met de leverancier van het systeem over het ontstaan van deze (menselijke) fout en over de maatregelen om herhaling te voorkomen.

We hopen u voldoende te hebben geïnformeerd en rekenen op uw begrip. Voor vragen of opmerkingen kunt u zich wenden tot de functionaris voor de gegevensbescherming via privacy@wur.nl

Met vriendelijke groet,

HR Servicedesk
T: 0317-481111
E: hr.servicedesk@wur.nl

==========

Dear colleague,

Unfortunately an error has recently been made during work on the salary system. The human error was corrected within half an hour after discovery.
This error has made it possible that for a short period of time, unauthorized employees of WUR, were able to view detailed salary data of all employees in the Optare tool within MyHR.

We were able to verify that only a small number of colleagues actually viewed and / or downloaded files. After contacting these colleagues, we were able to establish that nothing has been done with these data and that the data has not been shared.

We sincerely apologize for the occurrence of this incident. We are of course in discussion with the supplier of the system about the origin of this human error and about the measures to prevent repetition.

We hope to have informed you sufficiently and count on your understanding. For questions or comments, please contact the data protection officer via privacy@wur.nl

Kind regards,

HR Servicedesk
T: 0317-481111
E: hr.servicedesk@wur.nl

Privacy

Van: 5.1.2.e
Verzonden: maandag 20 april 2020 8:51
Aan: 5.1.2.e
Onderwerp: RE: Document3 Compatibility Mode_5.1.2.e.docx

Opvolgingsvlag: Opvolgen
Vlagstatus: Voltooid

Ha collega's,

Met de aanpassingen van 5.1.2.e en 5.1.2.e prima bericht. Dank 5.1.2.e. 5.1.2.e en ik bereiden een korte notitie voor de RvB voor (inclusief voorgestelde communicatie), geagendeerd voor de RvB a.s. donderdag. We willen daar de bevindingen van het onderzoekje onder de ' 14 illegale bezoekers' in meenemen. Na akkoord RvB donderdagochtend, kan de mail worden verzonden. Kan dat via jou 5.1.2.e?

Gr 5.1.2.e

Van: 5.1.2.e
Verzonden: zondag 19 april 2020 14:03
Aan: 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
Onderwerp: RE: Document3 Compatibility Mode_5.1.2.e.docx

Heel bondig, mooi gedaan. Ik heb er een opmerking bijgezet om aan te geven aan wat 'vaststellen' in dit geval inhoud.

Groeten, 5.1.2.e

From: 5.1.2.e @wur.nl>
Sent: Sunday, April 19, 2020 13:50
To: 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
Cc: 5.1.2.e @wur.nl>
Subject: Document3 Compatibility Mode_5.1.2.e.docx

Beste mensen,
Mijn voorzet voor een bericht aan onze personeelsleden (inclusief student-assistenten etc)
Met vriendelijke groet
5.1.2.e

Privacy

Van: 5.1.2.e
Verzonden: dinsdag 21 april 2020 8:56
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: RvB 22 april 2020 datalek, akkoord met dit definitieve exemplaar?
Bijlagen: RvB 22 april 2020 datalek.pdf

Opvolgingsvlag: Opvolgen
Vlagstatus: Voltooid

Hallo 5.1.2.e

Ben jij het eens met dit definitieve exemplaar? Dan kan ik het indienen voor 12:00 uur. Thanx!

WAGENINGEN
UNIVERSITY & RESEARCH

AANBIEDINGSFORMULIER

Raad van Bestuur d.d.: 22 april 2020 **AGENDAPUNT:**

1. **Onderwerp: Datalek**

2. **Status** ☒ ter besluitvorming ☐ ter bespreking ☐ ter kennisname

3. **Afgestemd met portefeuillehouder RvB**
   ☒ Buchwaldt ☐ Fresco ☐ Mol

4. **Indiener :** Directeur: 5.1.2.e
   Redacteur: 5.1.2.e
   Organisatieonderdeel: cHR

5. **Voorstel**
   (Indien dit meer dat 1 A-4 beslaat dan hier een samenvatting opnemen en het voorstel als bijlage toevoegen)

Inleiding
Op 9 april 2020 is door middel van een melding van een WUR medewerker bij de IT helpdesk duidelijk geworden dat er sprake was van een datalek. Dit datalek was ontstaan door een menselijke fout bij de leverancier van het personeels- en salarissyteem. Bij het inregelen van zgn. digitale formulieren (doctypes) was abusievelijk vergeten bepaalde inzage rechten af te sluiten. Hierdoor konden in aanleg 5131 actieve medewerkers in de database gegevens inzien waartoe ze op basis van hun rol geen recht hadden. Het betreft de periode tussen 23 maart 2020 en 9 april 2020.

Data
Naast gegevens zonder persoonsgerelateerde data betrof het ook gegevens met persoonsgerelateerde data. Van deze laatste was het belangrijkste gegeven het (eventuele) uitruilen van vakbondscontributie binnen het cafetariamodel en de bruto salaris gegevens per medewerker.

Na analyse is duidelijk geworden dat 20 WUR medewerkers data hebben ingezien. Hiervan waren 6 medewerkers vanuit hun rol binnen de IT helpdesk hiervoor geautoriseerd. Er zijn uiteindelijk 8 medewerkers die ongeautoriseerd persoonsgerelateerde data hebben ingezien.
De IT helpdesk heeft een analyse gemaakt wat de ongeautoriseerde medewerkers met deze data hebben gedaan. Samenvattend is dit als volgt:

Er waren (buiten FB-IT om) 2 gebruikers die het bestand met salarisinformatie hebben benaderd.
1. Mevrouw xx, zij was de eerste persoon die achter deze toegang kwam en heeft toen direct FB-IT en haar leidinggevende op de hoogte gebracht. Zij is telefonisch bedankt voor het direct melden van dit lek en ze heeft schriftelijk bevestigd de bestanden niet meer te hebben en niet te hebben gedeeld.
2.Leidinggevende mevrouw xx, heeft gekeken nadat hij de mail kreeg van mevrouw xx en hij wilde kijken of het openstond voor iedereen. Ook hij is telefonisch benaderd en de bestanden zijn verwijderd. Dit is ook nog schriftelijk bevestigd.

3 servicedesk medewerkers hebben deze bestanden proberen te openen om het lek te verifiëren en hebben toen de incident manager (en tevens CERT-lid) ingeschakeld
Binnen FB-IT hebben 3 CERT (Computer Emergency Response Team) leden gekeken naar wat voor data er beschikbaar was voor gebruikers. Het CERT handelt verzoeken met een gevoelige aard of beveiligingslekken altijd af.

6 andere gebruikers hebben enkele Persoonsgegevens ingezien en zij hebben schriftelijk aangegeven dat ze de bestanden niet meer hebben.

Melding Autoriteit Persoonsgegevens
Van hiervoor genoemd datalek is op 10 april 2020 volgens de daarvoor gestelde procedure melding gemaakt bij de Autoriteit Persoonsgegevens.
De procedure schrijft voor dat, indien een datalek zich hiervoor kwalificeert, er een bericht dient uit te gaan naar alle medewerkers hierbij in principe betrokken.

WAGENINGEN
UNIVERSITY & RESEARCH

AANBIEDINGSFORMULIER

Communicatie naar organisatie
In overleg met Simon Vink (Corporate Communications) is onderstaande tekst opgesteld.

"Beste collega,
Onlangs is, tijdens werkzaamheden aan het salarissysteem, een fout gemaakt. Daardoor was het korte tijd mogelijk voor niet geautoriseerde medewerkers van WUR om de gedetailleerde salarisgegevens van alle personeelsleden in te zien. De menselijke fout werd binnen een half uur na ontdekking hersteld.
We hebben kunnen nagaan dat een klein aantal collega's daadwerkelijk bestanden heeft bekeken en/of gedownload. Na contact met deze collega's hebben we kunnen vastgestellen dat er niets met deze gegevens is gedaan en dat ze niet verder zijn gedeeld.

We bieden onze welgemeende excuses aan voor het ontstaan van dit incident. Uiteraard zijn we in gesprek met de leverancier van het systeem over het ontstaan van deze (menselijke) fout en over de maatregelen om herhaling te voorkomen.
We hopen u voldoende te hebben geïnformeerd en rekenen op uw begrip. Voor vragen of opmerkingen kunt u zich wenden tot de functionaris voor de gegevensbescherming via privacy@wur.nl"

Besluitvorming
Verzoek aan Raad van Bestuur om goedkeuring te verlenen op verspreiding van dit bericht naar 5131 actieve medewerkers in de database.

6. Gevraagd besluit van de RvB
Bericht aan personeel WUR inzake datalek 9 april 2020

7. Financiële consequenties
Geen

8. Betrokken bij totstandkoming van het voorstel
☐ CR ☐ DBO ☒ anderen, nl: Functionaris gegevensbescherming 5.1.2.e
☐ Positief omdat:
☐ Negatief omdat:
Corporate Staf
☐ F&C ☒ HR ☐ CSA ☐ VC
☐ G&LS ☐ ESA ☐ C&M ☒ FG (Privacy)
☒ Positief advies omdat: Tekst noodzakelijk is i.v.m. privacy wetgeving
☐ Negatief advies omdat:

9. Vervolgprocedure besluitvorming / implementatie
☐ Concernraad	☐ advisering	☐ bespreking	☐ kennisname
☐ DBO	☐ advisering	☐ bespreking	☐ kennisname
☐ Raad van Toezicht	☐ goedkeuring	☐ bespreking	☐ kennisname
☐ Medezeggenschap	☐ Ja	☐ Nee	

Toelichting op basis van WOR/WHW:

☐ COR	☐ instemming	☐ advies	☐ kennisname
☐ SR-WU	☐ instemming	☐ advies	☐ kennisname
☐ GV-WU	☐ instemming	☐ advies	☐ kennisname
☐ Opleidingscommissies	☐ instemming	☐ advies	☐ kennisname
☐ Vakbonden, nl:	☐ goedkeuring	☐ bespreking	☐ kennisname
☐ Organisatieonderdeel, nl:		☐ implementatie	☐ verdere uitwerking

10. Communicatie intern/extern
☒ Geschikt voor communicatie na: goedkeuring RvB op bericht aan personeel WUR inzake datalek 9 april 2020
☐ Niet geschikt voor verdere communicatie omdat:

Privacy

Van: 5.1.2.e
Verzonden: woensdag 22 april 2020 16:20
Aan: 5.1.2.e
Onderwerp: RE: Datalek ADP / melding betrokkenen

Opvolgingsvlag: Opvolgen
Vlagstatus: Voltooid

Ik begrijp er even helemaal niets van, maar leg me neer bij elke -kennelijk goed doordachte – beslissing van jullie. (hoor nu voor het eerst van een verband met optare) Ik begrijp overigens dan nog steeds niet waar die 6.400 medewerkers vandaan komen. Dat is toch niet ons formatief personeelsbestand (ik weet de 2019 cijfers niet, maar in 2018 hadden we 5.600 medewerkers – 5100 fte)
Groet
5.1.2.e

From: 5.1.2.e
Sent: woensdag 22 april 2020 15:24
To: 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
Cc: 5.1.2.e @wur.nl>
Subject: RE: Datalek ADP / melding betrokkenen

Was even in-between workspaces, maar ben het graag eens met de conclusies van 5.1.2.e en 5.1.2.e
Groet, 5.1.2.e
5.1.2.e | Corporate Governance & Legal Services
Wageningen University & Research
P.O. Box 9101, 6700 HB Wageningen, The Netherlands
B:104 (Atlas) | 5.1.2.e, Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. +31 317 5.1.2.e
www.wur.nl/disclaimer

Van: 5.1.2.e @wur.nl>
Verzonden: woensdag 22 april 2020 14:43
Aan: 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
CC: 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
Onderwerp: RE: Datalek ADP / melding betrokkenen

Heren,
Zie dat 5.1.2.e niet on line is, dus reageer ik maar even vanwege de snelle afhandeling.
Doelstelling van dit alles is dat betrokkenen geïnformeerd worden. Dat zijn voor zover ik begrijp enkel degenen die een voorziening vanuit Optare hebben aangevraagd. Logisch dus om voor optie 1 te kiezen.
V.G.
5.1.2.e

From: 5.1.2.e
Sent: Wednesday, April 22, 2020 2:23 PM
To: 5.1.2.e @wur.nl>
Cc: 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
Subject: FW: Datalek ADP / melding betrokkenen

Ha 5.1.2.e, ik ben voor optie 1. We kunnen dat toch vrij makkelijk uitleggen in 1 zinnetje?
Gr 5.1.2.e

Van: Buchwaldt, Rens
Verzonden: woensdag 22 april 2020 14:09
Aan: 5.1.2.e @wur.nl>
Onderwerp: RE: Datalek ADP / melding betrokkenen

Hallo 5.1.2.e
In RvB besproken, en de noodzaak van brede communicatie is duidelijk. We hebben alleen een vraag bij de exacte verspreiding: het gaat om iets meer dan 5100 medewerkers, en die krijgen allen de mail. Dat betekent dat er ook een vrij grote groep (1000?) medewerkers geen mail krijgt, want het totaal aantal medewerkers is groter. Dat kan tot vragen (van met name die laatste groep) leiden. We zien twee opties om dat voor te zijn:

(1) In de mail duidelijk maken hoe het komt dat dit een heel grote subgroep is (en daarmee duidelijk maken waarom de anderen daar niet in zitten: we dachten dat dat wellicht komt doordat deze mensen iets in Optare doen, de anderen niet? Dat moet dan wel heel simpel uit te leggen zijn, en geen extra paragraaf aan tekst opleveren.
(2) De mail aan "alle" medewerkers sturen, dus daarmee ook aan mensen die niet getroffen zijn. Vraag is of dat AVG technisch kan, en of je ook dan niet iets moet zeggen dat duidelijk maakt dat niet iedereen die de mail krijgt is getroffen, maar dat zal het binnen AVG juist weer moeilijker maken, schat ik in.

Kun je hier een route in kiezen, of als dat niet tot een beter resultaat leidt, dat laten weten? In dat geval kunnen we leven met het voorstel, en zullen we moeten leven met de vragen/reacties van de niet aangeschreven subgroep die er dan waarschijnlijk komen.
Ik hoor het graag!
Met vriendelijke groet,

L.A.C. (Rens) Buchwaldt
Lid Raad van Bestuur
Wageningen University & Research
Postbus 9101, 6700 HB, Wageningen
Droevendaalsesteeg 4, Gebouw 104, 6708 PB, Wageningen
Tel.: 0317 -5.1.2.e
Mail: 5.1.2.e @wur.nl
www.wur.nl
www.wur.nl/nl/disclaimer.htm

Van: 5.1.2.e
Verzonden: vrijdag 17 april 2020 8:24
Aan: Buchwaldt, Rens 5.1.2.e @wur.nl>
Onderwerp: FW: Datalek ADP / melding betrokkenen
Urgentie: Hoog

Ha Rens,
De migratie van Workforce naar de cloud leek soepel te verlopen, ware het niet dat er door een fout van ADP sprake is geweest van een datalek van persoonlijke arbeidsvoorwaardengegevens en vakbondslidmaatschap vorige week donderdag. Doordat ADP een aantal vinkjes vergeten is aan te zetten, is de mogelijkheid geweest dat je als medewerker niet alleen toegang had tot je eigen bronnen voor Optare, maar ook die van je collega's. 14 medewerkers hebben dat dus ook daadwerkelijk gedaan (en hebben geklikt de namen van collega's, we kunnen dat precies zien in een backlog). Een van de 14 medewerkers heeft een melding gedan en is de fout direct herstelt. Dit datalek is direct aangemeld bij AP en heeft 5.1.2.e onderzoek laten doen naar de toedracht. Bijgevoegd de informatie.
Gisteren heb ik overleg gehad met 5.1.2.e en 5.1.2.e over hoe nu verder. De richtlijnen van de AP schrijven voor dat in principe alle betrokkenen op de hoogte moeten worden gesteld. Een intranet bericht volstaat niet omdat het door te weinig mensen wordt gelezen. Daarom kiezen we ervoor alle betrokken medewerkers een mail te sturen. 5.1.2.e bereidt dit voor, passend bij wat er is gebeurd en het 'risico' dat iemand heeft gelopen. Geen paniek veroorzaken, maar wel transparant zijn over wat er is gebeurd. We hebben besloten eerst nog contact te hebben met de 14 betrokken medewerkers (die dus ten onrechte een open deur zijn binnen gegaan) wat ze hebben gezien en wat ze met de informatie hebben gedaan. Dinsdag versturen we de mail en is dit netjes binnen de 14 dagen na incidentmelding die AP voorschrijft.
Kan er nog wel bij..
Gr 5.1.2.e

Van: 5.1.2.e
Verzonden: woensdag 15 april 2020 19:56
Aan: 5.1.2.e @wur.nl>;5.1.2.e @wur.nl>;5.1.2.e @wur.nl>;5.1.2.e @wur.nl>;5.1.2.e @wur.nl>;
5.1.2.e @wur.nl>
Onderwerp: Datalek ADP / melding betrokkenen
Urgentie: Hoog

Beste allemaal,

Om morgen snel door de materie heen te kunnen en iedereen op gelijk informatie level te krijgen hierbij enkele slides ter verduidelijking.

Met vriendelijke groet,

5.1.2.e

Aanwezig: maandag t/m vrijdag
Wageningen University & Research
Afdeling Corporate HR
Postbus 9101, 6700 HB Wageningen
Gebouw 104 (Atlas), Droevendaalsesteeg 4, 6708 PB Wageningen
*Tel.: 0031-6*5.1.2.e
5.1.2.e wur.nl
www.wur.nl
www.disclaimer-nl.wur.nl

Ontvangstbevestiging

Uw verzoek tot het aanpassen van een melding is succesvol verstuurd. Als uw verzoek niet meteen kan worden verwerkt, bijvoorbeeld omdat het meldingsnummer dat u heeft opgegeven niet bekend is bij de Autoriteit Persoonsgegevens, dan ontvangt u daarover zo spoedig mogelijk bericht.
U kunt de melding niet online raadplegen. Maak daarom een print voor uw eigen administratie. Doe dit voordat u deze pagina afsluit. Na het afsluiten van deze pagina zijn de gegevens die u heeft opgegeven niet meer beschikbaar. Onder het onderstaande meldingsnummer is de melding bekend bij de Autoriteit Persoonsgegevens. U heeft het meldingsnummer nodig om de melding aan te kunnen passen of in te kunnen trekken. Vermeld het meldingsnummer bij eventuele correspondentie met de Autoriteit Persoonsgegevens over de melding.

Tijdstip ontvangst	24-04-2020 12:33:22

0. Over deze melding

Gaat het om een nieuwe of bestaande melding?	Een ingediende melding aanpassen
Wat is het meldingsnummer van de oorspronkelijke melding?	5.1.2.e
Op grond van welke wettelijke bepaling doet u deze melding?	Algemene verordening gegevensbescherming (AVG)

1. Contactgegevens en overige algemene informatie

1.1 Contactgegevens

Over welke organisatie of welk bedrijf gaat het?

Registratienummer bij de Kamer van Koophandel	09215846
Naam van het bedrijf of de organisatie	Wageningen University
Adres	Droevendaalsesteeg 4

Postcode	6708PB
Plaats	Wageningen
In welke sector is de organisatie of het bedrijf actief?	Onderwijs - Tertiair onderwijs

Wie meldt het datalek?

Naam	5.1.2.e
Functie	corporate privacy officer
E-mailadres	privacy@wur.nl
Telefoonnummer	0317 5.1.2.e

Met wie kan de Autoriteit Persoonsgegevens contact opnemen voor nadere informatie over de melding?

De melder is contactpersoon	Nee
Naam contactpersoon	5.1.2.e
Functie contactpersoon	functionaris gegevensbescherming
E-mailadres contactpersoon	dpo@wur.nl
Telefoonnummer contactpersoon	5.1.2.e

1.2 Betrokkenheid andere organisatie

Was er een andere organisatie betrokken bij de inbreuk?	Ja, namelijk:
Naam van de andere organisatie die betrokken was bij de inbreuk	ADP, LLC.

In welke hoedanigheid was de andere organisatie betrokken bij de inbreuk?

ADP is de verwerker waar de inbreuk veroorzaakt is

2. Tijdlijn

Exacte datum waarop de inbreuk was, indien bekend	09-04-2020
Startdatum van de periode waarbinnen de inbreuk was	25-04-2020
Einddatum van de periode waarbinnen de inbreuk was	09-04-2020
Duurt de inbreuk op dit moment nog voort?	Nee
Wanneer werd de inbreuk ontdekt?	09-04-2020

Als u de inbreuk later meldt dan 72 uur na de ontdekking, wat is daarvan dan de reden?	(dit betreft een vervolgmelding)

3. Gegevens over het datalek

3.1 Aard van de inbreuk

Inbreuk op de vertrouwelijkheid van de gegevens	Ja
Inbreuk op de integriteit van de gegevens	Nee
Inbreuk op de beschikbaarheid van de gegevens	Nee

3.2 Aard van het incident

Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest?	Persoonsgegevens per ongeluk gepubliceerd

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest

Op 25 maart jl. heeft ADP in opdracht van WUR een transitie uitgevoerd en klantgegevens van WUR verplaatst van een lokale omgeving naar de gehoste SaaS omgeving van ADP. Onderdeel van deze transitie is het opnieuw definiëren van alle koppelingen met externe systemen inclusief de bijbehorende "documentypes" (mappen met Excelbestanden). Hierbij is door ADP door een menselijke fout verzuimd de autorisaties van de documenten op de juiste manier in te richten, waardoor medewerkers van WUR inzicht hebben gehad in ”Interfaces” en ”Logbestanden”, met de mogelijkheid van downloaden van Excelbestanden met persoonsgegevens over andere medewerkers. Door sluitende logging is inmiddels duidelijk dat 8 medewerkers van WUR inzicht hebben gehad in persoonsgegevens van vrijwel alle medewerkers in loondienst van WUR (5131 van de geregistreerde ca. 6400 personen) en bestanden met persoonsgegevens hebben gedownload. Dit betreft salarisgegevens, uitruil van arbeidsvoorwaarden (bijv. fietsregeling), vakbondscontributie en personeelsnummers. Direct na de melding heeft ADP per documenttype de autorisaties aangepast waardoor medewerkers geen toegang meer hadden tot deze dossiers.

4. Persoonsgegevens die betrokken zijn bij het datalek

4.1 Persoonsgegevens in het algemeen

Naam	Ja
Geslacht, geboortedatum en/of leeftijd	Nee
Burgerservicenummer (BSN)	Nee
Contactgegevens	Nee
Toegangs- of identificatiegegevens	Nee
Financiële gegevens	Ja
(Kopieën van) paspoorten of andere legitimatiebewijzen	Nee
Locatiegegevens	Nee
Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen	Nee

4.2 Bijzondere categorieën van persoonsgegevens

Persoonsgegevens waaruit iemands ras of etnische afkomst blijkt	Nee
Persoonsgegevens waaruit iemands politieke opvattingen blijken	Nee
Persoonsgegevens waaruit iemands religieuze of levensbeschouwelijke overtuigingen blijken	Nee
Persoonsgegevens waaruit iemands lidmaatschap van een vakbond blijkt	Ja
Gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid	Nee
Gegevens over iemands gezondheid	Nee
Genetische gegevens	Nee
Biometrische gegevens	Nee

4.3 Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords ("gegevensregisters") zijn getroffen door de inbreuk	5131

5. De groep mensen van wie persoonsgegevens betrokken zijn bij het datalek

Werknemers	Ja
Klanten (huidig en potentieel)	Nee
Leerlingen of studenten	Nee
Patiënten	Nee
Minderjarigen	Nee
Personen uit kwetsbare groepen	Nee

Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk.

Medewerkers in loondienst bij Wageningen University en/of Stichting Wageningen Research

Van minimaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?	5131
Van maximaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?	5131

6. Maatregelen die zijn getroffen voordat het datalek plaatsvond

Waren de persoonsgegevens op het moment dat de inbreuk zich voordeed versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk voor onbevoegden?	Nee

7. Gevolgen van het datalek

7.1 Gevolgen van de inbreuk op de vertrouwelijkheid, de integriteit en/of de beschikbaarheid van de gegevens.

Onbevoegden hebben kennis kunnen nemen van de gegevens	Ja
De gegevens kunnen op een onbehoorlijke of onrechtmatige manier worden misbruikt	Nee
Er worden binnen uw eigen organisatie mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens gebruikt	Nee
Er worden mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens hergebruikt voor andere doeleinden of doorgegeven aan andere organisaties	Nee
Een essentiële dienst kan tijdelijk niet meer worden verleend aan de betrokkenen	Nee
Een essentiële dienst kan permanent niet meer worden verleend aan de betrokkenen	Nee

7.2 Lichamelijke, materiële en immateriële schade voor de betrokkenen

Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkenen?

Discriminatie	Ja
Identiteitsdiefstal of -fraude	Nee
Financiële verliezen	Nee
Reputatieschade	Nee
Verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens	Nee
Ongeoorloofde ongedaanmaking van pseudonimisering	Nee
Betrokkenen kunnen hun rechten en vrijheden niet uitoefenen	Nee

Betrokkenen worden verhinderd controle over hun persoonsgegevens uit te oefenen	Nee

Andere gevolgen, namelijk:
(NB: discriminatie vanwege bekendheid vakbond-lidmaatschap, maar dat risico is verwaarloosbaar)

Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkenen	1. Verwaarloosbaar

8. Vervolgacties naar aanleiding van het datalek

8.1 Informeren van de betrokkenen

Heeft u het datalek gemeld aan de betrokkenen of bent u van plan dat te gaan doen?	Ja
Wanneer heeft u het datalek gemeld aan de betrokkenen?	23-04-2020

Wat is de inhoud van de melding aan de betrokkenen?
Beste collega, Onlangs is, tijdens werkzaamheden aan het salarissysteem, een fout gemaakt. Daardoor was het korte tijd mogelijk voor niet geautoriseerde medewerkers van WUR om de gedetailleerde salarisgegevens van alle personeelsleden in te zien. Inzage was mogelijk bij medewerkers die op basis van onze arbeidsvoorwaarden recht kunnen doen gelden op uitruil woon-werkverkeer Optare. De menselijke fout werd binnen een half uur na ontdekking hersteld. We hebben kunnen nagaan dat een klein aantal collega’s daadwerkelijk bestanden heeft bekeken en/of gedownload. Na contact met deze collega's hebben we kunnen vaststellen dat er niets met deze gegevens is gedaan en dat ze niet verder zijn gedeeld. We bieden onze welgemeende excuses aan voor het ontstaan van dit incident. Uiteraard zijn we in gesprek met de leverancier van het systeem over het ontstaan van deze (menselijke) fout en over de maatregelen om herhaling te voorkomen. We hopen u voldoende te hebben geïnformeerd en rekenen op uw begrip. Voor vragen of opmerkingen kunt u zich wenden tot de functionaris voor de gegevensbescherming via privacy@wur.nl. Met vriendelijke groet, HR Servicedesk T: 0317-481111 E: hr.servicedesk@wur.nl

Hoeveel betrokkenen heeft u geïnformeerd of gaat u informeren?	5131

Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken om de betrokkenen te informeren?	e-mail

8.2 Maatregelen om de inbreuk aan te pakken

Welke technische en organisatorische maatregelen heeft uw organisatie getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?
Direct na de melding heeft ADP per documenttype de autorisaties aangepast waardoor medewerkers geen toegang meer hadden tot deze dossiers. ADP is een onderzoek gestart over de periode 25 maart tot 9 april welke documenttypes de properties niet goed waren ingericht. ADP heeft onderzocht wie er in de periode 25 maart tot 9 april 2020 onrechtmatig bestanden heeft gedownload. Wij hebben de betreffende (8) medewerkers benaderd, de bestanden verwijderd en bevestiging ontvangen dat de bestanden verwijderd zijn en niet verder zullen worden verspreid. Naar aanleiding van dit incident zal er binnen ADP een onderzoek uitgevoerd worden naar de gevolgde procedure en zullen aanpassingen worden doorgevoerd om dit soort incidenten te voorkomen.

8.3 Internationale aspecten

Heeft de inbreuk zich voorgedaan in een grensoverschrijdende gegevensverwerking, en is de AP voor deze verwerking de leidende toezichthouder?	Nee
Heeft uw organisatie of bedrijf, het datalek gemeld bij privacytoezichthouders in een of meer andere EU-landen, of gaat u dat nog doen?	Nee
Heeft uw organisatie of bedrijf, het datalek gemeld bij Europese toezichthouders op andere meldplichten, of gaat u dat nog doen?	Nee

9. Overig

Is naar uw mening deze melding compleet?	Ja, de vereiste informatie is verstrekt en er is geen vervolgmelding nodig

Privacy

Van: Privacy
Verzonden: vrijdag 24 april 2020 12:36
Aan: 5.1.2.e
Onderwerp: RE: Melding AP
Bijlagen: 20200424_vervolgmelding_ADP.pdf

Ha 5.1.2.e,

Hierbij de definitieve melding in het ADP-dossier.

Groet, 5.1.2.e

5.1.2.e
Corporate Privacy Officer | 5.1.2.e
Tel. +31 317 5.1.2.e

Van: 5.1.2.e @wur.nl>
Verzonden: vrijdag 10 april 2020 14:13
Aan: 5.1.2.e @wur.nl>
Onderwerp: RE: Melding AP

Hoi 5.1.2.e

Dank.

5.1.2.e

From: 5.1.2.e
Sent: Friday, April 10, 2020 1:48 PM
To: 5.1.2.e @wur.nl>
Subject: Melding AP

Ha 5.1.2.e hierbij de melding bij de AP van vandaag naar aanleiding van het ADP-incident.

Groet, 5.1.2.e

5.1.2.e
| Corporate Governance & Legal Services
Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e | Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. +31 317 5.1.2.e

Van: Privacy
Aan: Privacy; 5.1.2.e
Onderwerp: Nieuwe datalekmelding | 4/19/2021 2:30:54 PM | 5.1.2.e @wur.nl
Datum: maandag 19 april 2021 16:30:58
Prioriteit: Hoog

Beste collega,

Zojuist is er een nieuw datalek gemeld via het digitale meldformulier:

* * *

1. Geef een zo gedetailleerd mogelijke omschrijving van het incident
Database Booking kon worden benaderd via SQL injection, databases en tabellen kunnen zijn benaderd en uitgelezen. Kwetsbaarheid is inmiddels dichtgezet (prod en acc/test) met een correct sql prepare statement, programmeur kijkt nog dieper in het systeem of er nog aanpassingen nodig zijn. Datalek oplossing is inmiddels bevestigd door 5.1.2.e op 19 april (16.24h). N.B. informatie van 200 lokale accounts bleek kwetsbaar; dat van ca. 900 SurfConext accounts niet. Het betreft persoonlijke informatie als: username, password, firstname, middlename, lastname, email, telephone en department van 200 lokale accounts. Informatie van 900 SurfConext accounts zijn altijd beschermd gebleven.

2. Wat is de aard van het incident?
Onbekend of hiervan misbruik is gemaakt.

3. Hoelang heeft het incident geduurd?
Meer dan één dag

4a. Gedurende welke periode heeft het incident plaatsgevonden?
Onduidelijk volgens programmeur. De laatste authenticated scan is uitgevoerd door 5.1.2.e in mei 2018.

4b. Op welke datum heeft het incident plaatsgevonden?

5. Van welke categorie personen zijn persoonsgegevens gelekt?
["Externen (partners, leveranciers)","Medewerkers","Studenten"]

6. Van hoeveel personen zijn mogelijk persoonsgegevens gelekt?
200

7. Op welke datum/tijdstip is het incident ontdekt?
16 april 2021, gecommuniceerd door 5.1.2.e op 18 april 2021

8. Wat voor soort persoonsgegevens zijn betrokken in het incident?
["Identificatiegegevens (login/wachtwoord)","naam, emailadres, (werk)telefoonnummer, (WUR) groeps- of bedrijfsnaam"]

9. Welke acties zijn ondernomen naar aanleiding van het incident?
Voor lokale accounts wordt morgen 20 april een aanpassing doorgevoerd (live gezet) volgens WUR-password richtlijnen. Het password moet elke 90 dagen worden gewijzigd. Lokale account holders ontvangen een mail om hun lokale password direct te wijzigen. Lokale account die dat niet doen, worden verplicht om dit bij de eerste inlog te doen. N.B. WUR zal regelmatig authenticated scans moeten uitvoeren om kwetsbaarheden te blijven onderscheppen.

* * *

Met vriendelijke groet,
5.1.2.e

5.1.2.e
Corporate Privacy Officer | 5.1.2.e

Wageningen University & Research

Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e, Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317-5.1.2.e

Privacy

Van: Privacy
Verzonden: maandag 19 april 2021 17:31
Aan: 5.1.2.e
Onderwerp: RE: Datalek

NB: Ik heb 5.1.2.e zojuist niet meer kunnen spreken en de voorlopige melding alvast besproken met de functionaris voor de gegevensbescherming van WUR. Ik hoor graag van je rond de drie aanvullende punten.

Groet, 5.1.2.e

5.1.2.e
Corporate Privacy Officer | Corporate Governance & Legal Services

Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e, Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317-5.1.2.e
www.wur.nl/disclaimer

Van: Privacy
Verzonden: maandag 19 april 2021 17:29
Aan: 5.1.2.e @wur.nl>
Onderwerp: Datalek

Dag 5.1.2.e

Hieronder zoals al even besproken een korte samenvatting die ik zal rapporteren aan de Autoriteit Persoonsgegevens. Vanwege de timing zal ik eerst een voorlopige melding doen, die ik later (zo snel mogelijk) kan aanvullen met de informatie:

a) Of 5.1.2.e nog meer maatregelen nodig acht
b) Of er een sluitende logging beschikbaar is
c) Een afschrift van het bericht dat je aan de betrokken personen gaat sturen (NB: daarin moet dus staan:
    - een omschrijving, in duidelijke en eenvoudige taal, van de aard van het incident
    - de naam en de contactgegevens van een ander contactpunt waar meer informatie kan worden verkregen (je mag eventueel ook privacy@wur.nl toevoegen of in de cc. zetten)
    - de waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens
    - de maatregelen die zijn genomen om het incident aan te pakken en verdere gevolgen te beperken

* * *

Op 16 april jl. is een kwetsbaarheid gesignaleerd binnen het online bookingsysteem voor Shared Research Facilities van WUR. Effectief kon iedereen via een SQL-injectie toegang krijgen tot een database met bestanden van 200 lokale accounts (medewerkers, studenten en externen). In die database stonden de volgende persoonsgegevens: username/password, naam, e-mail, telefoon en afdeling. Voor zover nu bekend is er geen sluitende logging beschikbaar rond de toegang tot deze gegevens. De kwetsbaarheid is inmiddels wel dichtgezet. Op dit moment vindt nader onderzoek plaats naar de eventuele nadere maatregelen die getroffen moeten worden.

* * *

Groet, 5.1.2.e

5.1.2.e
Corporate Privacy Officer | 5.1.2.e
Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e | Droevendaalsesteeg 4
6708 PB Wageningen
Tel. +31 317 5.1.2.e

Ontvangstbevestiging

Uw verzoek tot het indienen van een melding wordt in behandeling genomen. U kunt de melding niet online raadplegen. Maak daarom een print voor uw eigen administratie. Doe dit voordat u deze pagina afsluit. Na het afsluiten van deze pagina zijn de gegevens die u heeft opgegeven niet meer beschikbaar. Onder het onderstaande meldingsnummer is de melding bekend bij de Autoriteit Persoonsgegevens. U heeft het meldingsnummer nodig om de melding aan te kunnen passen of in te kunnen trekken. Vermeld het meldingsnummer bij eventuele correspondentie met de Autoriteit Persoonsgegevens over de melding.

Tijdstip ontvangst	19-04-2021 17:38:28
Uniek nummer	5.1.2.e

0. Over deze melding

Gaat het om een nieuwe of bestaande melding?	Een nieuwe melding indienen
Op grond van welke wettelijke bepaling doet u deze melding?	Algemene verordening gegevensbescherming (AVG)

1. Contactgegevens en overige algemene informatie

1.1 Contactgegevens

Over welke organisatie of welk bedrijf gaat het?

Registratienummer bij de Kamer van Koophandel	09215846
Naam van het bedrijf of de organisatie	Wageningen University
Adres	Droevendaalsesteeg 4
Postcode	6708PB
Plaats	Wageningen

In welke sector is de organisatie of het bedrijf actief?	Onderwijs - Tertiair onderwijs

Wie meldt het datalek?

Naam	5.1.2.e
Functie	Corporate Privacy Officer
E-mailadres	privacy@wur.nl
Telefoonnummer	0317 5.1.2.e

Met wie kan de Autoriteit Persoonsgegevens contact opnemen voor nadere informatie over de melding?

De melder is contactpersoon	Nee
Naam contactpersoon	5.1.2.e
Functie contactpersoon	Functionaris voor de Gegevensbescherming
E-mailadres contactpersoon	dpo@wur.nl
Telefoonnummer contactpersoon	0317 5.1.2.e

1.2 Betrokkenheid andere organisatie

Was er een andere organisatie betrokken bij de inbreuk?	Nee

2. Tijdlijn

Exacte datum waarop de inbreuk was, indien bekend	16-04-2021
Startdatum van de periode waarbinnen de inbreuk was	01-01-2019
Einddatum van de periode waarbinnen de inbreuk was	18-04-2021
Duurt de inbreuk op dit moment nog voort?	Nee
Wanneer werd de inbreuk ontdekt?	16-04-2021

3. Gegevens over het datalek

3.1 Aard van de inbreuk

Inbreuk op de vertrouwelijkheid van de gegevens	Ja
Inbreuk op de integriteit van de gegevens	Nee
Inbreuk op de beschikbaarheid van de gegevens	Nee

3.2 Aard van het incident

Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest?	Persoonsgegevens per ongeluk gepubliceerd

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest

Op 16 april jl. is een kwetsbaarheid gesignaleerd binnen het online bookingsysteem voor Shared Research Facilities van WUR. Effectief kon iedereen via een SQL-injectie toegang krijgen tot een database met bestanden van 200 lokale accounts (medewerkers, studenten en externen). In die database stonden de volgende persoonsgegevens: username/password, naam, e-mail, telefoon en afdeling. Voor zover nu bekend is er geen sluitende logging beschikbaar rond de toegang tot deze gegevens. De kwetsbaarheid is inmiddels dichtgezet. Op dit moment vindt nader onderzoek plaats naar de eventuele nadere maatregelen die getroffen moeten worden.

4. Persoonsgegevens die betrokken zijn bij het datalek

4.1 Persoonsgegevens in het algemeen

Naam	Ja
Geslacht, geboortedatum en/of leeftijd	Nee
Burgerservicenummer (BSN)	Nee
Contactgegevens	Ja
Toegangs- of identificatiegegevens	Ja
Financiële gegevens	Nee
(Kopieën van) paspoorten of andere	Nee

legitimatiebewijzen	
Locatiegegevens	Nee
Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen	Nee

4.2 Bijzondere categorieën van persoonsgegevens

Persoonsgegevens waaruit iemands ras of etnische afkomst blijkt	Nee
Persoonsgegevens waaruit iemands politieke opvattingen blijken	Nee
Persoonsgegevens waaruit iemands religieuze of levensbeschouwelijke overtuigingen blijken	Nee
Persoonsgegevens waaruit iemands lidmaatschap van een vakbond blijkt	Nee
Gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid	Nee
Gegevens over iemands gezondheid	Nee
Genetische gegevens	Nee
Biometrische gegevens	Nee

4.3 Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords ("gegevensregisters") zijn getroffen door de inbreuk	200

5. De groep mensen van wie persoonsgegevens betrokken zijn bij het datalek

Werknemers	Ja
Klanten (huidig en potentieel)	Ja
Leerlingen of studenten	Ja

Patiënten	Nee
Minderjarigen	Nee
Personen uit kwetsbare groepen	Nee

Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk.

Medewerkers, studenten, externen

Van minimaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?	200
Van maximaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?	200

6. Maatregelen die zijn getroffen voordat het datalek plaatsvond

Waren de persoonsgegevens op het moment dat de inbreuk zich voordeed versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk voor onbevoegden?	Nee

7. Gevolgen van het datalek

7.1 Gevolgen van de inbreuk op de vertrouwelijkheid, de integriteit en/of de beschikbaarheid van de gegevens.

Onbevoegden hebben kennis kunnen nemen van de gegevens	Ja
De gegevens kunnen op een onbehoorlijke of onrechtmatige manier worden misbruikt	Ja
Er worden binnen uw eigen organisatie mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens gebruikt	Nee

Er worden mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens hergebruikt voor andere doeleinden of doorgegeven aan andere organisaties	Nee
Een essentiële dienst kan tijdelijk niet meer worden verleend aan de betrokkenen	Nee
Een essentiële dienst kan permanent niet meer worden verleend aan de betrokkenen	Nee

7.2 Lichamelijke, materiële en immateriële schade voor de betrokkenen

Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkenen?

Discriminatie	Nee
Identiteitsdiefstal of -fraude	Ja
Financiële verliezen	Nee
Reputatieschade	Nee
Verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens	Nee
Ongeoorloofde ongedaanmaking van pseudonimisering	Nee
Betrokkenen kunnen hun rechten en vrijheden niet uitoefenen	Nee
Betrokkenen worden verhinderd controle over hun persoonsgegevens uit te oefenen	Nee
Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkenen	2. Beperkt

8. Vervolgacties naar aanleiding van het datalek

8.1 Informeren van de betrokkenen

Heeft u het datalek gemeld aan de betrokkenen of bent u van plan dat te gaan doen?	Ja
Wanneer gaat u het datalek melden aan de betrokkenen?	20-04-2021

Wat is de inhoud van de melding aan de betrokkenen?
[volgt]

Hoeveel betrokkenen heeft u geïnformeerd of gaat u informeren?	200
Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken om de betrokkenen te informeren?	E-mail

8.2 Maatregelen om de inbreuk aan te pakken

Welke technische en organisatorische maatregelen heeft uw organisatie getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?
De kwetsbaarheid is inmiddels dichtgezet. Voor lokale accounts wordt op 20 april a.s. een aanpassing doorgevoerd volgens de WUR-password richtlijnen. Het password moet daarbij elke 90 dagen worden gewijzigd.

8.3 Internationale aspecten

Heeft de inbreuk zich voorgedaan in een grensoverschrijdende gegevensverwerking, en is de AP voor deze verwerking de leidende toezichthouder?	Nee
Heeft uw organisatie of bedrijf, het datalek gemeld bij privacytoezichthouders in een of meer andere EU-landen, of gaat u dat nog doen?	Nee
Heeft uw organisatie of bedrijf, het	Nee

datalek gemeld bij Europese toezichthouders op andere meldplichten, of gaat u dat nog doen?

9. Overig

Is naar uw mening deze melding compleet?	Nee, er komt later een vervolgmelding met aanvullende informatie over deze inbreuk

Ontvangstbevestiging

Uw verzoek tot het aanpassen van een melding is succesvol verstuurd. Als uw verzoek niet meteen kan worden verwerkt, bijvoorbeeld omdat het meldingsnummer dat u heeft opgegeven niet bekend is bij de Autoriteit Persoonsgegevens, dan ontvangt u daarover zo spoedig mogelijk bericht.
U kunt de melding niet online raadplegen. Maak daarom een print voor uw eigen administratie. Doe dit voordat u deze pagina afsluit. Na het afsluiten van deze pagina zijn de gegevens die u heeft opgegeven niet meer beschikbaar. Onder het onderstaande meldingsnummer is de melding bekend bij de Autoriteit Persoonsgegevens. U heeft het meldingsnummer nodig om de melding aan te kunnen passen of in te kunnen trekken. Vermeld het meldingsnummer bij eventuele correspondentie met de Autoriteit Persoonsgegevens over de melding.

Tijdstip ontvangst	24-04-2021 19:43:22

0. Over deze melding

Gaat het om een nieuwe of bestaande melding?	Een ingediende melding aanpassen
Wat is het meldingsnummer van de oorspronkelijke melding?	5.1.2.e
Op grond van welke wettelijke bepaling doet u deze melding?	Algemene verordening gegevensbescherming (AVG)

1. Contactgegevens en overige algemene informatie

1.1 Contactgegevens

Over welke organisatie of welk bedrijf gaat het?

Registratienummer bij de Kamer van Koophandel	09215846
Naam van het bedrijf of de organisatie	Wageningen University

Adres	Droevendaalsesteeg 4
Postcode	6708PB
Plaats	Wageningen
In welke sector is de organisatie of het bedrijf actief?	Onderwijs - Tertiair onderwijs

Wie meldt het datalek?

Naam	5.1.2.e
Functie	Corporate Privacy Officer
E-mailadres	privacy@wur.nl
Telefoonnummer	0317 5.1.2.e

Met wie kan de Autoriteit Persoonsgegevens contact opnemen voor nadere informatie over de melding?

De melder is contactpersoon	Nee
Naam contactpersoon	5.1.2.e
Functie contactpersoon	Functionaris voor de Gegevensbescherming
E-mailadres contactpersoon	dpo@wur.nl
Telefoonnummer contactpersoon	0317 5.1.2.e

1.2 Betrokkenheid andere organisatie

Was er een andere organisatie betrokken bij de inbreuk?	Nee

2. Tijdlijn

Exacte datum waarop de inbreuk was, indien bekend	16-04-2021
Startdatum van de periode waarbinnen de inbreuk was	01-01-2019
Einddatum van de periode waarbinnen de inbreuk was	16-04-2021
Duurt de inbreuk op dit moment nog voort?	Nee
Wanneer werd de inbreuk ontdekt?	16-04-2021

3. Gegevens over het datalek

3.1 Aard van de inbreuk

Inbreuk op de vertrouwelijkheid van de gegevens	Ja
Inbreuk op de integriteit van de gegevens	Nee
Inbreuk op de beschikbaarheid van de gegevens	Nee

3.2 Aard van het incident

Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest?	Persoonsgegevens per ongeluk gepubliceerd

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest

Op 16 april jl. is een kwetsbaarheid gesignaleerd binnen het online bookingsysteem voor Shared Research Facilities van WUR. Effectief kon iedereen via een SQL-injectie toegang krijgen tot een database met bestanden van 200 lokale accounts (medewerkers, studenten en externen). In die database stonden de volgende persoonsgegevens: username/password, naam, e-mail, telefoon en afdeling. Er is geen sluitende legging beschikbaar rond de toegang tot deze gegevens. De kwetsbaarheid is inmiddels dichtgezet en het actuele wachtwoordbeleid is toegepast.

4. Persoonsgegevens die betrokken zijn bij het datalek

4.1 Persoonsgegevens in het algemeen

Naam	Ja
Geslacht, geboortedatum en/of leeftijd	Nee
Burgerservicenummer (BSN)	Nee
Contactgegevens	Ja
Toegangs- of identificatiegegevens	Ja

Financiële gegevens	Nee
(Kopieën van) paspoorten of andere legitimatiebewijzen	Nee
Locatiegegevens	Nee
Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen	Nee

4.2 Bijzondere categorieën van persoonsgegevens

Persoonsgegevens waaruit iemands ras of etnische afkomst blijkt	Nee
Persoonsgegevens waaruit iemands politieke opvattingen blijken	Nee
Persoonsgegevens waaruit iemands religieuze of levensbeschouwelijke overtuigingen blijken	Nee
Persoonsgegevens waaruit iemands lidmaatschap van een vakbond blijkt	Nee
Gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid	Nee
Gegevens over iemands gezondheid	Nee
Genetische gegevens	Nee
Biometrische gegevens	Nee

4.3 Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords ("gegevensregisters") zijn getroffen door de inbreuk	200

5. De groep mensen van wie persoonsgegevens betrokken zijn bij het datalek

Werknemers	Ja

Klanten (huidig en potentieel)	Ja
Leerlingen of studenten	Ja
Patiënten	Nee
Minderjarigen	Nee
Personen uit kwetsbare groepen	Nee

Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk.

Medewerkers, studenten en externen die gebruik hebben gemaakt van het bookingsysteem.

Van minimaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?	200
Van maximaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?	200

6. Maatregelen die zijn getroffen voordat het datalek plaatsvond

Waren de persoonsgegevens op het moment dat de inbreuk zich voordeed versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk voor onbevoegden?	Nee

7. Gevolgen van het datalek

7.1 Gevolgen van de inbreuk op de vertrouwelijkheid, de integriteit en/of de beschikbaarheid van de gegevens.

Onbevoegden hebben kennis kunnen nemen van de gegevens	Ja
De gegevens kunnen op een onbehoorlijke of onrechtmatige manier worden misbruikt	Ja
Er worden binnen uw eigen organisatie	Nee

mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens gebruikt	
Er worden mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens hergebruikt voor andere doeleinden of doorgegeven aan andere organisaties	Nee
Een essentiële dienst kan tijdelijk niet meer worden verleend aan de betrokkenen	Nee
Een essentiële dienst kan permanent niet meer worden verleend aan de betrokkenen	Nee

7.2 Lichamelijke, materiële en immateriële schade voor de betrokkenen

Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkenen?

Discriminatie	Nee
Identiteitsdiefstal of -fraude	Ja
Financiële verliezen	Nee
Reputatieschade	Nee
Verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens	Nee
Ongeoorloofde ongedaanmaking van pseudonimisering	Nee
Betrokkenen kunnen hun rechten en vrijheden niet uitoefenen	Nee
Betrokkenen worden verhinderd controle over hun persoonsgegevens uit te oefenen	Nee
Geef een inschatting van de ernst van de mogelijke gevolgen voor de	2. Beperkt

betrokkenen

8. Vervolgacties naar aanleiding van het datalek

8.1 Informeren van de betrokkenen

Heeft u het datalek gemeld aan de betrokkenen of bent u van plan dat te gaan doen?	Ja
Wanneer heeft u het datalek gemeld aan de betrokkenen?	20-04-2021

Wat is de inhoud van de melding aan de betrokkenen?

Dear Booking user, The following applies to local accounts, not to SurfConext accounts: You are account holder for a local account in Booking. A vulnerability in Booking has been identified and communicated today by our Wageningen University & Research Computer Emergency Response Team (WUR-CERT). Booking could have been entered by SQL injection. I expect no negative consequences, but I cannot exclude that the databases have been read. The combination of local user name and password, your email address and phone number might have been leaked. Today, the vulnerability was solved by our programmer and confirmed by WUR-CERT. Our programmer will come up with a Booking password strategy for your local account conform the WUR-guidelines and security requirements, which means that you will have to change your password every 90 days. Please, change your password for your local account a.s.a.p., and in case for a shared group account inform the users of this account on this change. Sorry for any inconvenience this may cause. Best regards, [medewerker]

Hoeveel betrokkenen heeft u geïnformeerd of gaat u informeren?	200
Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken om de betrokkenen te informeren?	E-mail

8.2 Maatregelen om de inbreuk aan te pakken

Welke technische en organisatorische maatregelen heeft uw organisatie getroffen

om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?
De kwetsbaarheid is inmiddels dichtgezet. Voor lokale accounts is een aanpassing doorgevoerd volgens de WUR-password richtlijnen. Het password moet daarbij elke 90 dagen worden gewijzigd.

8.3 Internationale aspecten

Heeft de inbreuk zich voorgedaan in een grensoverschrijdende gegevensverwerking, en is de AP voor deze verwerking de leidende toezichthouder?	Nee
Heeft uw organisatie of bedrijf, het datalek gemeld bij privacytoezichthouders in een of meer andere EU-landen, of gaat u dat nog doen?	Nee
Heeft uw organisatie of bedrijf, het datalek gemeld bij Europese toezichthouders op andere meldplichten, of gaat u dat nog doen?	Nee

9. Overig

Is naar uw mening deze melding compleet?	Ja, de vereiste informatie is verstrekt en er is geen vervolgmelding nodig

5.1.2.e

Van: Privacy
Verzonden: vrijdag 28 mei 2021 14:07
Aan: Privacy; 5.1.2.e
Onderwerp: Nieuwe datalekmelding | 5/28/2021 12:06:48 PM - 5.1.2.e @wur.nl

Urgentie: Hoog

Beste collega,

Zojuist is er een nieuw datalek gemeld via het digitale meldformulier:

* * *

1. Geef een zo gedetailleerd mogelijke omschrijving van het incident
De pagina's achter de adminsectie staan open voor de buitenwereld zonder te hoeven in te loggen en zijn te vinden via Google. De volledige website lijkt hiermee aanpasbaar en er zijn van 1000'en personen gegevens inzichtelijk (en aanpasbaar).

2. Wat is de aard van het incident?
documenten zijn inzichtelijk en ook gegevens van gebruikers.

3. Hoelang heeft het incident geduurd?
Meer dan één dag

4a. Gedurende welke periode heeft het incident plaatsgevonden?
1 november 2018

4b. Op welke datum heeft het incident plaatsgevonden?

5. Van welke categorie personen zijn persoonsgegevens gelekt?
["het betreft een externe webisite. Hierop staan gegevens van Agro economen die lid zijn van de EAAE die inzichtelijk zijn."]

6. Van hoeveel personen zijn mogelijk persoonsgegevens gelekt?
Er staan 3807 gebruikers in.

7. Op welke datum/tijdstip is het incident ontdekt?
28-05-2021: 13.26

8. Wat voor soort persoonsgegevens zijn betrokken in het incident?
["NAW-gegevens","email adres"]

9. Welke acties zijn ondernomen naar aanleiding van het incident?
lek gedicht oude gegevens verwijderd. waar het lek zat. Beheerders van de site op de hoogte gebracht en zij gaan contact opnemen met de leden van EAAE.

* * *

Met vriendelijke groet,
5.1.2.e

5.1.2.e
Corporate Privacy Officer 5.1.2.e

Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e, Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317-5.1.2.e

Privacy

Van: WUR-CERT
Verzonden: vrijdag 28 mei 2021 13:15
Aan: 5.1.2.e
CC: Privacy
Onderwerp: Ernstig 'lek' website "The European Association of Agricultural Economists"
Bijlagen: WUL Access.mp4

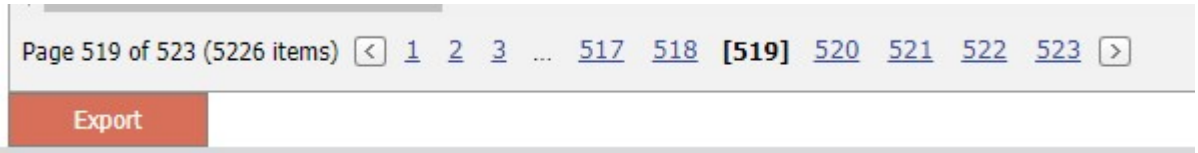
Urgentie: Hoog

Beste 5.1.2.e & 5.1.2.e

Wij hebben onderstaande responsible disclosure melding binnengekregen omtrent de webapplicatie van “The European Association of Agricultural Economists” . Na het nodige onderzoek wat de melder nu precies bedoelde ben ik erachter gekomen dat de adminsectie van de applicatie wel een slot op de voordeur heeft maar alle achterliggende pagina’s te benaderen zijn zonder in te loggen en vindbaar zijn via Google. Dit maakt het mogelijk de volledige site aan te passen zonder in te loggen, maar ook zijn er veel NAW gegevens beschikbaar.

Via onderstaande link is het mogelijk deze gegevens van **duizenden** personen in te zien. Let wel, hier zitten dubbelingen in, personen moeten zich vermoedelijk ieder jaar opgeven waardoor er een extra regel toegevoegd wordt.
Met de (on)handige export functionaliteit heb ik kunnen ontdubbelen op basis van gebruikersnaam en kom ik nog op enkele duizenden uit. Daarnaast zie ik dat de eerste inschrijvingen in 2015 gedaan zijn, mogelijk bestaat het lek dus al zo lang. Deels een slag om de arm bij deze uitspraken omdat ik natuurlijk inhoudelijk de applicatie niet ken.

https://www.wecr.wur.nl/eaae_membersite/admin/MembersOVerview.aspx.

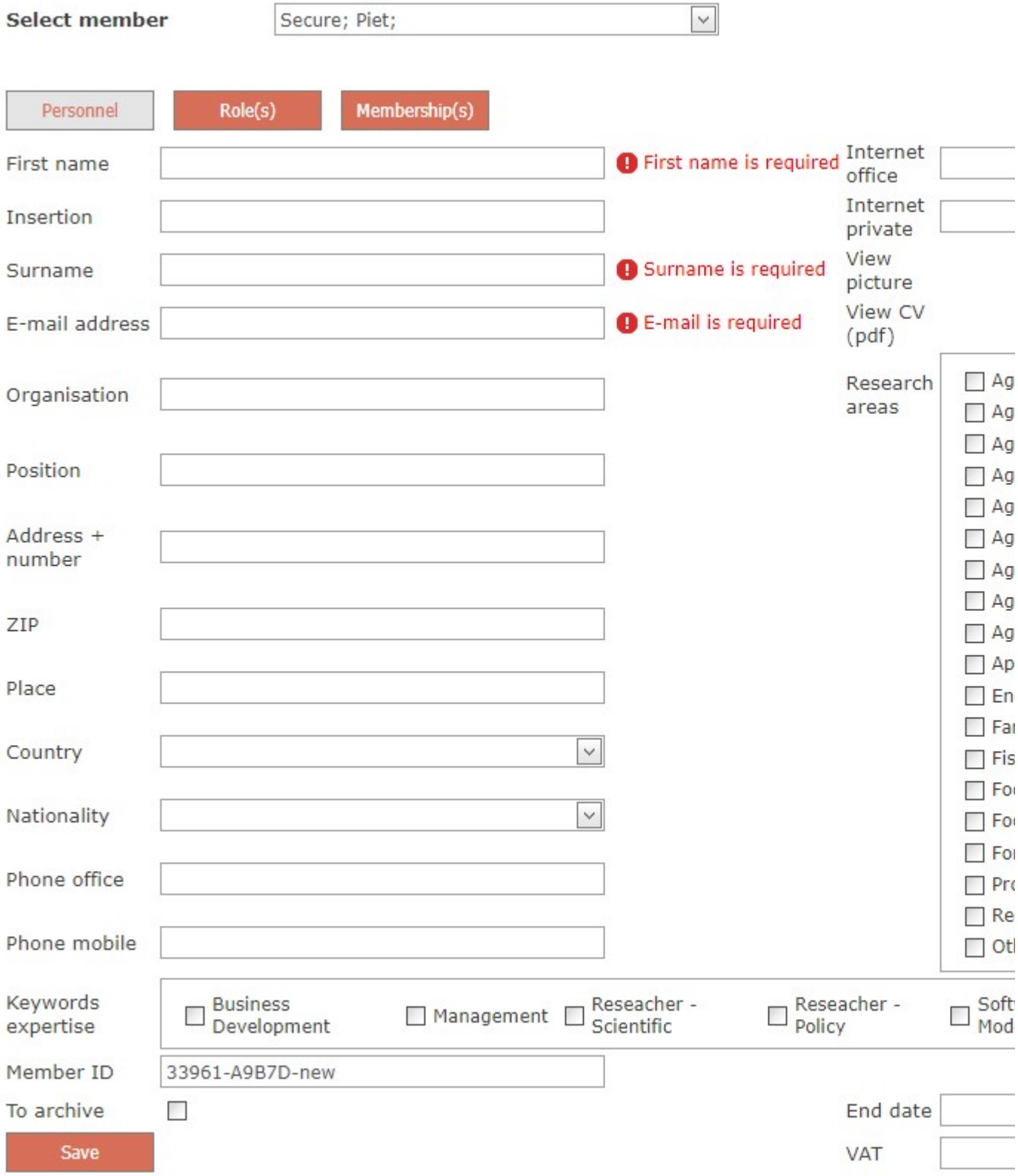


De contactpersoon van de machine waarop deze applicatie draait is 5.1.2.e en wordt afgenomen door eenheid SSG LEI.

Ik zal contact opnemen met de beheerder van de dienst/server en hem vragen:

- direct deze adminsectie offline te halen
- direct een officiele datalek melding te maken via jullie formulier (hij heeft hopelijk de kennis van de applicaties en hoeft geen aannames te doen)
- Voor toekomstige openstelling van deze applicatie eerst te laten testen op kwetsbaarheiden (bij voorkeur een pentest gezien het aantal NAW gegevens en mogelijke (imago)schade kijkende naar het doel/samenwerkingsverband).
  Ook omdat ik enigszins huiverig ben omdat het ook mogelijk is via bijvoorbeeld paypal je ‘lidmaatschap’ te betalen via deze site. Ik kan alleen de gekozen betaalmethode en invoice nummer terugzien, gelukkig geen IBAN’s. Hij zal daar zelf vast meer inzicht in hebben.

Onderstaand de gegevens welke je als nieuwe gebruiker gevraagd worden om in te vullen en o.a. terecht komen in de webapplicatie:



Bij verdere vragen hoor ik het graag.

Met vriendelijke groet,

5.1.2.e
Scrummaster Datamanagement & Hosting Services
Security coördinator

Facilitair Bedrijf, onderdeel van Wageningen University & Research

Afdeling Informatie Technologie
Postbus 59, 6700 AB, Wageningen
Gebouw 116, Akkermaalsbos 12, 6708 WB, Wageningen
5.1.2.e @wur.nl
www.wur.nl
www.disclaimer-nl.wur.nl

Van: 5.1.2.e @gmail.com>
Verzonden: woensdag 26 mei 2021 01:16
Aan: WUR-CERT <cert@wur.nl>
Onderwerp: Vulnerability Report #01

Greetings From Delhi, India
I am 5.1.2.e , a Security Researcher
https://www.linkedin.com/in/5.1.2.e

I have found some vulnerability on the website:- https://www.wecr.wur.nl

==========

Vulnerability Name: **Authentication Bypass**

Hello Team,
When I go to the url https://www/wecr/wur.nl it shows me 403 Forbidden Access is denied but when i use google dork and to be able to access admin access page. Here i try some default password for login but i am not able to access https://www.wecr.wur.nl/eaae_membersite/Default.aspx

Here I try some Dork and am able to gain access to the Admin Page of this site where I am able to control website content and many more.

Authentication system is not validated properly.

IMPACT:- An attacker can control whole website they can control website content with admin privilege

POC: Attach On Attachments.
Since it's a point of concern for the security & integrity of the website, so I would like to extend further support as well, if needed.
I hope to get a positive response on this & expect a token of appreciation for my efforts.

Thank you

Regards
5.1.2.e

Privacy

Van: Privacy
Verzonden: maandag 31 mei 2021 09:41
Aan: 5.1.2.e
Onderwerp: FW: Ernstig 'lek' website "The European Association of Agricultural Economists"

Ha 5.1.2.e, wat ik nu van 5.1.2.e begrijp is dat de European Association of Agricultural Economists een zelfstandige organisatie is waarbij wij weliswaar de website hosten, maar niet verantwoordelijk zijn voor de inhoud. Dat zou betekenen dat de meldplicht ook niet bij ons ligt. Ik heb om 11 uur een vervolgafspraak om dit nog verder door te nemen.
Groet, 5.1.2.e

5.1.2.e
Corporate Privacy Officer | Corporate Governance & Legal Services
Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317-5.1.2.e
www.wur.nl/disclaimer

Van: 5.1.2.e @wur.nl>
Verzonden: maandag 31 mei 2021 09:34
Aan: WUR-CERT <cert@wur.nl>; 5.1.2.e @wur.nl>; Privacy <privacy@wur.nl>; 5.1.2.e @wur.nl>
Onderwerp: RE: Ernstig 'lek' website "The European Association of Agricultural Economists"

Ha beide, ja het datalekformulier is in goede orde ontvangen (maar erg summier, vandaar mijn aanvullende vragen). Ik zal contact zoeken met Hans voor verdere input.
Groet, 5.1.2.e

5.1.2.e
5.1.2.e | Corporate Governance & Legal Services
Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317-5.1.2.e
www.wur.nl/disclaimer

Van: WUR-CERT <cert@wur.nl>
Verzonden: maandag 31 mei 2021 09:31
Aan: 5.1.2.e @wur.nl>; Privacy <privacy@wur.nl>; 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
Onderwerp: RE: Ernstig 'lek' website "The European Association of Agricultural Economists"

Hoi 5.1.2.e
Het datalek formulier zou ingevuld en verstuurd moeten zijn door 5.1.2.e. Hij heeft dit samen ingevuld met de ontwikkelaar 5.1.2.e
Wat is weet is dat de logging beperkt lijkt te zijn en het systeem op zijn huidige server is geïnstalleerd in 2018 maar kijkende naar de data al minstens sinds 2015 in de lucht is.
De communicatie voor de members heb ik nog niet voorbij zien komen.
Ik heb aan 5.1.2.e vrijdagmiddag aangegeven dat iemand van Privacy contact met hem zou opnemen dus hij staat vast klaar om alle vragen te beatwoorden.
Even kort en bondig, spring NU weer mijn volgende overleg in, hopelijk kan je hier mee vooruit.
Groet,
5.1.2.e

Van: 5.1.2.e @wur.nl>
Verzonden: maandag 31 mei 2021 09:25
Aan: Privacy <privacy@wur.nl>; 5.1.2.e @wur.nl>; WUR-CERT <cert@wur.nl>; 5.1.2.e @wur.nl>
Onderwerp: RE: Ernstig 'lek' website "The European Association of Agricultural Economists"

Hoi 5.1.2.e
Ik heb niet meegekregen om wie het ging. Is het datalek formulier niet bij jullie aangekomen?

Groeten, 5.1.2.e
-------- Oorspronkelijk bericht --------
Van: Privacy <privacy@wur.nl>
Datum: 31-05-2021 09:09 (GMT+01:00)
Aan: 5.1.2.e @wur.nl>, WUR-CERT <cert@wur.nl>, 5.1.2.e @wur.nl>, 5.1.2.e @wur.nl>
Onderwerp: RE: Ernstig 'lek' website "The European Association of Agricultural Economists"

Ha 5.1.2.e

Dat kan zeker, maar ik had vanmorgen nog een aantal vragen uitgezet die nodig zijn voor de eventuele melding (zie onderstaand). Ik zou daar graag nog een terugkoppeling op krijgen om een complete melding te kunnen doen.

* * *

Ha 5.1.2.e ,

Ik weet niet of 5.1.2.e nog gereageerd heeft, maar hebben jullie voor mij de laatste stand van zaken?

1. Kunnen wij inmiddels aan de hand van de logging uitsluiten dat onbevoegden toegang hebben gehad en aanpassingen hebben doorgevoerd in de NAW-gegevens van de 3807 personen? (betreft dat alleen (zakelijke) NAW en e-mailadressen?)
2. Wie is de maker van de website en wat is de relatie tussen ons en de maker (zijn wij volledig eigenaar of doen wij dat samen met de maker?)
3. Hebben jullie voor mij ook de tekst van het bericht dat de maker aan de members zal willen sturen?

* * *

Groet, 5.1.2.e
5.1.2.e
Corporate Privacy Officer | Corporate Governance & Legal Services
Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317 5.1.2.e
www.wur.nl/disclaimer

Van: 5.1.2.e @wur.nl>
Verzonden: maandag 31 mei 2021 09:08
Aan: WUR-CERT <cert@wur.nl>; 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
CC: Privacy <privacy@wur.nl>
Onderwerp: RE: Ernstig 'lek' website "The European Association of Agricultural Economists"

Ha 5.1.2.e

Krijg jij het voor elkaar dit lek alvast te melden bij de AP?

Groet,
5.1.2.e

5.1.2.e

Van: Privacy
Verzonden: maandag 31 mei 2021 11:35
Aan: 5.1.2.e WUR-CERT; 5.1.2.e
Onderwerp: RE: Ernstig 'lek' website "The European Association of Agricultural Economists"

Dag 5.1.2.e

Naar ik nu begrijp gaat het om een website die wij hosten (en waarbij wij uiteraard verantwoordelijk zijn voor adequate beveiliging). Maar wij zijn niet de verwerkingsverantwoordelijke voor de op de website aanwezige persoonsgegevens; dat is de vereniging zelf.

De verantwoordelijkheid voor het melden van het incident bij de AP ligt daarom bij de EAAE en specifiek 5.1.2.e als 5.1.2.e van de vereniging. Ik zal hem dat berichten.

Groet, 5.1.2.e

5.1.2.e
Corporate Privacy Officer | Corporate Governance & Legal Services

Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e, Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317 5.1.2.e
www.wur.nl/disclaimer

5.1.2.e

Van: Privacy
Verzonden: maandag 31 mei 2021 12:11
Aan: 5.1.2.e
CC: 'WUR-CERT'; Functionarisgegevensbescherming; 5.1.2.e
Onderwerp: Beveiligingsincident website EAAE

Urgentie: Hoog

Beste 5.1.2.e

Afgelopen vrijdag ontvingen wij een melding dat zich een beveiligingsincident heeft voorgedaan voor de website van de European Association of Agricultural Economists (EAAE). Dit incident houdt in dat de pagina's achter de adminsectie zonder login toegankelijk waren voor onbevoegden. Het beveiligingslek is inmiddels gedicht en de beheerders van de site zijn naar wij begrijpen op de hoogte gebracht.

Na enig onderzoek hebben wij vastgesteld dat persoonsgegevens (t.w.: zakelijke NAW-gegevens en e-mailadressen) van 3807 betrokkenen mogelijk inzichtelijk zijn geweest voor onbevoegden. Wij kunnen niet uitsluiten dat deze persoonsgegevens onrechtmatig zijn verwerkt. Vanwege het aantal gegevens dient dit incident gemeld te worden bij de privacytoezichthouder, de Autoriteit Persoonsgegevens (AP).

Omdat niet WUR, maar de EAAE zelf verantwoordelijk is voor deze gegevens, ligt de wettelijke plicht om actie te ondernemen ook bij de EAAE zelf. Ik begrijp dat jij op dit moment 5.1.2.e bent van de vereniging. Om die reden zou ik jou hierbij willen vragen het ertoe te leiden dat het datalek zo spoedig mogelijk door de EAAE wordt gemeld via de website van de AP (https://autoriteitpersoonsgegevens.nl/). Dit moet binnen 72 uur na ontdekking. Omdat het datalekkenformulier van de AP op dit moment bijgewerkt wordt, zal dat morgen gedaan moeten worden. Als je hier hulp bij nodig hebt zijn wij graag beschikbaar.

Wij ontvangen graag morgen een afschrift van de uiteindelijke melding zodat wij ons interne onderzoek ook kunnen sluiten.

Vriendelijke groet,
5.1.2.e

5.1.2.e
Corporate Privacy Officer | 5.1.2.e
Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e | Droevendaalsesteeg 4
6708 PB Wageningen
Tel. +31 317 5.1.2.e

FORMULIER MELDING DATALEKKEN

In geval van een beveiligingsincident waarbij persoonsgegevens betrokken zijn (ook als je dat niet zeker weet) gebruik je het datalekformulier om een melding te doen.

Het is van belang dit formulier zo volledig en nauwkeurig mogelijk in te vullen. Op basis van dit formulier maakt de functionaris voor de gegevensbescherming (F-G) een afweging of het incident gemeld moet worden aan de Autoriteit Persoonsgegevens en/of betrokken personen.

Alle communicatie over dit incident met betrokkenen of toezichthouders dient vooraf afgestemd te worden met de F-G via 0317 of privacy@wur.nl.

FORMULIER

Contactgegevens melder			
Naam	5.1.2.e		
Functie	Product Owner Integration Services, Product Owner Security		
E-mailadres	5.1.2.e @wur.nl		
Telefoonnummer	5.1.2.e		
Gegevens over het incident (omschrijving van het incident)	Op onze 5.1.2.h omgeving is het mogelijk om 5.1.2.h op te starten met verhoogde rechten, hiermee is het mogelijk om de 5.1.2.h met 5.1.2.h rechten te komen. Hierdoor zou je toegang kunnen krijgen om logging en storage van andere gehoste 5.1.2.h op dat 5.1.2.h waar je normaal geen rechten toe zou hebben. Om dit uit te kunnen voeren moet je een WUR account hebben (dus alleen interne mensen), ingelogd via VPN of op de campus zijn en rechten hebben binnen het 5.1.2.h (dit zijn op dit moment 30 personen). Deze omgeving draait nu ongeveer 6 maanden. Tot nog toe is er geen aanleiding om aan te nemen dat er misbruik heeft plaatsgevonden.		
Samenvatting van het incident	Er is privileged escalation mogelijk door een configuratiefout welke alleen intern (binnen eigen netwerk en beperkt tot 30 gebruikers) te misbruiken is, dit hebben wij zelf ontdekt.		
Toelichting	*[wat is er gebeurd (diefstal of verlies van gegevens, malware/hack/DDoS, gegevens per ongeluk gepubliceerd, etc.), op welke manier (bijv. via internet, e-mail, aanval van buitenaf, etc.) en hoe is het incident ontdekt]*		
Aard van het incident	Mogelijke inzage in logfiles en databases die persoonsgegevens bevatten.		
Toelichting	*[bijv. inzage door onbevoegden, gegevens gekopieerd/gedownload, wijzigingen aangebracht, gegevens verwijderd of vernietigd, diefstal van gegevens of nog niet bekend]*		
Datum en tijdstip van het incident	07-05-2021 15:32		
Toelichting	*[op welk moment of gedurende welke periode vond het incident plaats]*		
Datum en tijdstip van ontdekking	07-05-2021 15:00		
Toelichting	*[wanneer is het incident ontdekt]*		
Betrokkenen	Alle WUR studenten, medewerkers en PHDers		
Toelichting	*[van welke personen (medewerkers, studenten, proefpersonen etc) zijn gegevens betrokken bij het incident]*		
Aantal betrokkenen	circa 20.000 gebruikers		
Toelichting	*[eventueel een schatting van minimaal/maximaal aantal personen]*		
		Ja	Nee
	naam, adres, woonplaats (zakelijk en/of privé):	X	

Welke soorten persoonsgegevens (aankruisen)	contactgegevens (telefoonnummer, e-mailadres, etc.):	X	
	geboortedatum en -plaats	X	
	nationaliteit	X	
	geslacht	X	
	identificatiegegevens (login, wachtwoord):		X
	financiële- of HRM-gegevens	X	
	persoonsgebonden nummers (BSN, onderwijsnummer, etc.)	X	
	strafrechtelijke gegevens (veroordelingen, berispingen, etc.)		X
	kopie paspoort		X
	kopie rijbewijs		X
	foto	X	
	medische gegevens		X
	godsdienst, politieke voorkeur, vakbondslidmaatschap		X
	anders, namelijk:		
Mogelijke gevolgen (aankruisen)		Ja	Nee
	stigmatisering of uitsluiting		X
	schade aan de gezondheid		X
	blootstelling aan (identiteits)fraude	X	
	blootstelling aan spam of phishing	X	
	anders, namelijk:		
Welke acties zijn genomen	Alle logging wordt doorgespit om aan te tonen of er wel of geen misbruik is gemaakt. Er is tot op heden geen misbruik bekend.		
Toelichting	*[beschrijving welke acties zijn getroffen om het incident te adresseren en om verdere incidenten te voorkomen]*		
Welke maatregelen zijn getroffen	Huidige stand van zaken gecontroleerd en geen misbruik gevonden. Externe beheerpartij benaderd op het oplossen van dit lek op korte termijn te verwezenlijken.		
Toelichting	*[beschrijving en toelichting welke beveiligingsmaatregelen van toepassing zijn op de betrokken persoonsgegevens; zijn die bijv. versleuteld, gehasht, gepseudonimiseerd of anderszins ontoegankelijk gemaakt]*		
Internationale aspecten	Ja, de WUR is een internationale organisatie		
Toelichting	*[heeft het incident betrekking op personen in andere EER-landen [Europese Unie, Liechtenstein, Noorwegen of IJsland]:*		

Stuur dit formulier zo snel mogelijk na het constateren van een datalek naar **servicedesk.it@wur.nl**.

5.1.2.e

Van: 5.1.2.e
Verzonden: maandag 10 mei 2021 10:49
Aan: Privacy; 5.1.2.e
CC: 5.1.2.e
Onderwerp: Vulnerability: root access op Kubernetes nodes mogelijk voor niet geautoriseerde gebruikers
Bijlagen: Formulier datalekken 10052021_5.1.2.e.docx

Goedemorgen 5.1.2.e

Via deze weg doe ik namens mijzelf en de heren in de CC bijgevoegde melding. In het document is de aard van het incident en de getroffen maatregelen beschreven.

Als jullie hier vervolgacties aan willen verbinden of als zaken nog opgehelderd moeten worden hoor ik het graag.

Groet,

5.1.2.e
5.1.2.e IT Workplace Services Wageningen University & Research

WAGENINGEN
UNIVERSITY & RESEARCH

tel: (0317-5.1.2.e Workdays 08:00am - 05:30pm
Forum, building 102
Droevendaalsesteeg 2
6708 PB
Wageningen

see intranet.wur.nl -> Services -> ICT for news, FAQ's and manuals.

Privacy

Van: 5.1.2.e
Verzonden: vrijdag 7 mei 2021 17:18
Aan: 5.1.2.e ; Servicedesk IT
CC: Privacy; 5.1.2.e
Onderwerp: Re: Vulnerability: 5.1.2.h access op 5.1.2.h mogelijk voor niet geautoriseerde gebruikers
Bijlagen: Formulier datalekken.docx

Opvolgingsvlag: Opvolgen
Vlagstatus: Voltooid

Categorieën: 5.1.2.e

Hoi Allen,

Inmiddels zijn we wat verder qua kennis. We weten dat op dit moment alleen de 5.1.2.h met privilege aan staan op de 5.1.2.h omgeving.
De groep die de omgeving heeft opgebouwd (5.1.2.h) geven aan logging te hebben van de deployments en stateful sets van elk half uur vanaf het begin van de omgeving.
Hierin zou te achterhalen moeten zijn of er in die tijd andere 5.1.2.h gedraaid hebben met verhoogde rechten.

5.1.2.e en ik hebben vast een eerste draft opgezet van het datalek formulier. Die is te vinden in de bijlage.
Dit wil zeggen dat we tot maandag 15:00 hebben om bij de AP de melding te doen.
Ik was niet in staat om 5.1.2.e is out of office) te bereiken zojuist, en denk dat dit maandag afgerond moet worden.
Komende week ben ik vrij en ik zal 5.1.2.e nog even bijpraten voor het vervolg.

Gr 5.1.2.e

5.1.2.e
Sent: Friday, May 07, 2021 16:04
To: 5.1.2.e ; Servicedesk IT
Cc: Privacy; 5.1.2.e
Subject: RE: Vulnerability: 5.1.2.h op 5.1.2.h mogelijk voor niet geautoriseerde gebruikers

Dank. Ik heb nog even een inschatting gemaakt van het risico:
Uit het verhaal van 5.1.2.e begrijp ik dat de 5.1.2.h data in het systeem zit. Ik heb het even nagezocht, deze is geclassificeerd als 'ernstig'. Mocht er data in zitten van de categorie 'ontwrichtend' dan hoor ik het graag.
Gebaseerd op wat 5.1.2.e zei over het aanvallen zitten we in de categorie 'reeel' qua kans op misbruik.
In de 'vulnerability handling standard' hebben we afgesproken dat er voor deze categorie 30 dagen staat om de kwetsbaarheid te mitigeren. Als dit binnen deze tijd wordt opgelost hoeft het niet naar hoger management geëscaleerd te worden.

Vanuit privacy is er aanvullend de verplichting om te onderzoeken of dit incident geleid kan hebben tot ongeautoriseerde toegang tot persoonsgegevens.

Groeten, 5.1.2.e

From: 5.1.2.e @wur.nl>
Sent: Friday, May 07, 2021 15:33
To: Servicedesk IT <servicedesk.it@wur.nl>
Cc: 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
Subject: Vulnerability: 5.1.2.h op 5.1.2.h nodes mogelijk voor niet geautoriseerde gebruikers

Op advies van 5.1.2.e meld ik dit via de servicedesk: ik heb als niet geautoriseerde gebruiker 5.1.2.h rechten op 5.1.2.h van het 5.1.2.h . Details kunnen via mij worden opgehaald. 5.1.2.e en 5.1.2.e weten ervan, stappen worden gezet met beheer.

Privacy

Van: Privacy
Verzonden: dinsdag 21 september 2021 10:16
Aan: Privacy; 5.1.2.e
Onderwerp: Nieuwe datalekmelding | 9/21/2021 8:15:45 AM | 5.1.2.e @wur.nl

Urgentie: Hoog

Beste collega,

Zojuist is er een nieuw datalek gemeld via het digitale meldformulier:

* * *

1. Geef een zo gedetailleerd mogelijke omschrijving van het incident
per abuis is een excelbestand met 2 en 6 studentnummers en namen en opleiding van non-EU studenten verstuurd per mail aan een groep waar ook studenten in zette (100 en 800 emailadressen). De inhoud van de mail gaat over onvoldoende studievoortgang

2. Wat is de aard van het incident?
bestand per ongeluk doorgestuurd.

3. Hoelang heeft het incident geduurd?
Eén dag

4a. Gedurende welke periode heeft het incident plaatsgevonden?

4b. Op welke datum heeft het incident plaatsgevonden?
2021-09-20

5. Van welke categorie personen zijn persoonsgegevens gelekt?
["Studenten"]

6. Van hoeveel personen zijn mogelijk persoonsgegevens gelekt?
8

7. Op welke datum/tijdstip is het incident ontdekt?
20 september 2021 - 17.00 uur

8. Wat voor soort persoonsgegevens zijn betrokken in het incident?
["Persoonsgebondennummers (BSN, paspoortnummer, studentnummer)"]

9. Welke acties zijn ondernomen naar aanleiding van het incident?
informeren opleiding, data-officer en beantwoorden vragen per mail, overleg binnen SSC

* * *

Met vriendelijke groet,
5.1.2.e

5.1.2.e
Corporate Privacy Officer | 5.1.2.e

Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e, Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317 5.1.2.e

5.1.2.e

Van: Functionarisgegevensbescherming
Verzonden: maandag 20 september 2021 18:00
Aan: Privacy SSG
CC: Privacy
Onderwerp: FW: Datalek via mail Food Sciences

Urgentie: Hoog

Beste collega's,

Onderstaande mail kwam zojuist binnen in mijn mailbox. Ondernemen jullie actie! Thanks.

Met vriendelijke groet,

5.1.2.e

WAGENINGEN
UNIVERSITY & RESEARCH

5.1.2.e | Functionaris Gegevensbescherming | Wageningen University & Research | Postbus 9101, 6700 HB Wageningen | +31 (0)317 5.1.2.e | www.wur.nl

---

From: 5.1.2.e @wur.nl>
Sent: Monday, September 20, 2021 5:41 PM
To: SSC <ssc@wur.nl>; OWI Food Science <food.science@wur.nl>; Functionarisgegevensbescherming <functionarisgegevensbescherming@wur.nl>; Servicedesk IT <servicedesk.it@wur.nl>; 5.1.2.e @wur.nl>; Studyadvice Food <studyadvice.food@wur.nl>; 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
Subject: Datalek via mail Food Sciences
Importance: High

Beste lezer,

Onderstaande mail is aan alle studenten gestuurd van de opleiding MFT. De mail was eigenlijk gericht aan opleidingsdirecteuren, studieadviseurs, en studentbegeleiders, en bevat een bijlage met de naam van alle niet-EU studenten van de opleiding MFT die minder dan 15 ECTS hebben behaald. Het lijkt mij dat dit niet de bedoeling is, en dat ervoor gezorgd dient te worden dat, indien mogelijk, de mail z.s.m. wordt verwijderd uit mailboxen.

Met vriendelijke groeten,

5.1.2.e
MSc Student Food Technology | Wageningen University & Research | LinkedIn | 5.1.2.e | ☎ Tel. 06 5.1.2.e

---

From: SSC <ssc@wur.nl>
Sent: 20 September 2021 16:46

To: MFT.foodsciences <MFT.foodsciences@wur.nl>
Subject: SPM MFT

Dear programme directors, study advisors, student counselors,

Enclosed you find the list.

We have started the study progress monitoring for the academic year 2020 -2021 for non-EU students with a residence permit for "study". This means that new students who started in September 2020 must have obtained a minimum of 30 ects and students who started in February 2021 must have obtained a minimum of 15 ects in order to retain this residence permit. Second-year students must have obtained at least 30 ects.
As usual, student counselors can give students who do not meet this requirement an "excusable reason". For example due to circumstances such as illness or an accident, they were unable to meet this requirement. Covid-19 can also be used as an excusable reason this year. The MOMI act (Modern Migration Policy) also states that you may not use the same excusable reason for a student for two years in a row. If a student has an excusable reason, he/ she will not be deregistered from the IND.

The procedure is as follows:

1. *Student Immigration Office (5.1.2.e and 5.1.2.e) exports lists from Osiris of non-EU students who do not meet the ects requirement (20 September).*
2. *They send these files to the study advisors, who indicate which students are still making sufficient study progress, for example because of major courses (thesis en internship) that are not yet visible in the credits in Osiris (return to Student Immigration Office by 4 October at the latest).*
3. *The returned lists are send to the student counselors by 5.1.2.e and 5.1.2.e, who can give the students known to them an excusable reason (return to Student Immigration Office by 18 October at the latest).*
4. *5.1.2.e and 5.1.2.e inform the remaining students without an excusable reason or with insufficient (unregistered) study progress that they do not meet the ects requirement and deregister them from the IND (no later than 30 October).*

If you have any questions, don't hesitate to mail me.

Met vriendelijke groet,

5.1.2.e

Met vriendelijke groet,

5.1.2.e
Student Immigration Office
Student Service Centre

WAGENINGEN
UNIVERSITY & RESEARCH

Bezoekadres
Forum (Building 102) | Droevendaalsesteeg 2 | 6708 PB Wageningen | Nederland
Postadres
Wageningen University | Student Service Centre | Postbus 414 | 6700 AK Wageningen | Nederland

5.1.2.e

Van: Privacy ESA
Verzonden: dinsdag 21 september 2021 10:35
Aan: Privacy; Functionarisgegevensbescherming
Onderwerp: FW: Melding datalek

Urgentie: Hoog

Goedemorgen 5.1.2.e

Zie onderstaande. Ik zal een eventuele melding straks met 5.1.2.e afstemmen.

Mvg,

5.1.2.e

Van: 5.1.2.e @wur.nl>
Verzonden: dinsdag 21 september 2021 10:09
Aan: Privacy ESA <privacy.esa@wur.nl>; 5.1.2.e @wur.nl>
CC: 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
Onderwerp: Re: Melding datalek
Urgentie: Hoog

Dag 5.1.2.e

Hieronder wat antwoorden, bel me even als je tijd hebt.

Kind regards,

5.1.2.e
Manager International Office
Wageningen University & Research
+31 (0)6 5.1.2.e

Van: Privacy ESA <privacy.esa@wur.nl>
Datum: dinsdag, 21 september 2021 om 09:25
Aan: 5.1.2.e @wur.nl>
CC: 5.1.2.e @wur.nl>, 5.1.2.e @wur.nl>, 5.1.2.e @wur.nl>
Onderwerp: RE: Melding datalek

Goedemorgen 5.1.2.e

Goed dat je dit meldt. Dank je wel daarvoor. Voor we een mail aan betrokkenen gaan sturen zou ik graag wat meer informatie van je krijgen. Ik zou graag antwoord krijgen met betrekking tot de volgende vragen:

- Is er naast naam en de melding 'onvoldoende credits' sprake van meer informatie? Bijvoorbeeld contactgegevens, opleiding, studentnummers?

. opleiding en studentnummer (MFS: 2 studenten, MFT: 6 studenten) in een excel bijlage bij de mail

- Is er een poging gedaan om de mail terug te trekken?

. de mail is verstuurd via FAQtory en in overleg met de opleiding is besloten om niet terug te trekken om niet teveel aandacht te geven. En een mail terugtrekken via FAQtory kan niet eenvoudig.

- Om hoeveel studenten gaat het?

. de gegevens van 8 studenten zijn verstuurd

- Is er sprake van andere geadresseerden die per ongeluk meegenomen zijn?

. deze mail is verstuurd naar ongeveer 900 emailadressen

- Welke actie is genomen om te voorkomen dat dit nogmaals gebeurd?

. het proces wordt jaarlijks uitgevoerd en stond al in de planning om dit geheel via Osiris te laten verlopen, zonder lijsten te versturen.

- Waarom is de lijst niet via een link in de mail verstuurd (bijv via netwerklocatie of interne OneDrive)? Dit is beter stuurbaar en voorkomt – met de juiste autorisaties - dat er alsnog data zichtbaar is.

. staat op de planning

Om dit verder in goede banen te leiden is het nodig om het datalekformulier zo snel mogelijk in te vullen. Op basis van bovenstaande kunnen we verdere vervolgstappen bepalen. Gezien de creditstatus van studenten moeten we dit mogelijk melden bij de Autoriteit Persoonsgegevens. Hiermee hangt de eventuele melding met studenten samen.

Met vriendelijke groet,

5.1.2.e
Privacy Officer
Wageningen University & Research
Education & Student Affairs (ESA)
PO Box 9100, 6700 HA Wageningen
Wageningen Campus, Atlas Building, Droevendaalsesteeg 4, 6708 PB Wageningen
0317 – 5.1.2.e
disclaimer

WUR is serious about Data

DATADANGERS, de WUR-film over het belang van onze data-schatkamer en hoe deze goed te beschermen.
Vragen? Mail, bel of maak een afspraak.

Van: 5.1.2.e @wur.nl>
Verzonden: maandag 20 september 2021 18:12
Aan: Functionarisgegevensbescherming <functionarisgegevensbescherming@wur.nl>; 5.1.2.e @wur.nl>; Privacy ESA <privacy.esa@wur.nl>
CC: 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
Onderwerp: Melding datalek

Beste 5.1.2.e en 5.1.2.e,

Er is helaas vanmiddag iets fout gegaan bij het versturen van een mail met persoonlijke informatie door SSC.
De mail had gestuurd moeten worden naar team van opleidingsdirecteur en studieadviseur, maar is per ongeluk verstuurd naar mailinglijst van de opleiding met alle studenten.

De mailinglijst waren: mft.msc@wur.nl en mfs.msc@wur.nl

Wat er is verstuurd is een excelllijst van studenten (naam) die niet voldoende credits hebben gehaald volgens de wet MoMi. De hoeveelheid credits wordt niet genoemd.
Maar wel is dus helder nu voor alle studenten van deze opleiding dat deze studenten niet voldoende credits hebben gehaald.

De opleidingsdirecteur en studieadviseur hebben dit ontdekt en mij op de hoogte gesteld. Ik heb direct onderzocht wat er is gebeurd.

Wat zijn verdere stappen die nu het beste gezet kunnen worden?

- Wel/niet email sturen naar alle studenten met de vraag om de mail te verwijderen (met als risico dat studenten juist wel gaan lezen en aandacht aan geven)
- Standaard antwoord maken voor studenten die reactie sturen (we hebben al paar reacties ontvangen)
- Voorkomen dat dat het volgende keer weer gebeurd --> hier is direct actie op ondernomen
- ?

Met hartelijke groet,
5.1.2.e

5.1.2.e
5.1.2.eStudent Service Centre Wageningen University
Education and Student Affairs (ESA)
Forum, kamer 5.1.2.e
Monday – Thursday
Tel. 0317-5.1.2.e
Email: 5.1.2.e @wur.nl

5.1.2.e

Van: 5.1.2.e
Verzonden: dinsdag 21 september 2021 12:15
Aan: Functionarisgegevensbescherming
Onderwerp: FW: Melding datalek

Ha 5.1.2.e, ter info:

Zojuist besproken in het PSIRT. We gaan het melden aan de 8 studenten; niet aan de 900. Ik zal de AP informeren. 5.1.2.e neemt het voortouw in melden aan de studenten. Gaat vanuit SSC plaatsvinden.

Groet, 5.1.2.e

5.1.2.e
5.1.2.e Corporate Governance & Legal Services

Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317 5.1.2.e
www.wur.nl/disclaimer

Van: 5.1.2.e @wur.nl>
Verzonden: dinsdag 21 september 2021 11:38
Aan: Privacy ESA <privacy.esa@wur.nl>; 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
CC: 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
Onderwerp: RE: Melding datalek
Urgentie: Hoog

Hoi 5.1.2.e
Wil je even contact opnemen met 5.1.2.e Want die heeft net email gestuurd naar heel andere personen en een meeting verzoek gedaan.
Gaat wel over hetzelfde. Meeting lijkt mij niet echt nodig met deze brede groep (o.a. woordvoerder).
Hartelijke groet,
5.1.2.e

5.1.2.e
5.1.2.e Student Service Centre Wageningen University
Education and Student Affairs (ESA)
Forum, kamer 5.1.2.e
Monday – Thursday
Tel. 0317 5.1.2.e
Email: 5.1.2.e @wur.nl

From: Privacy ESA <privacy.esa@wur.nl>
Sent: dinsdag 21 september 2021 10:50
To: 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
Cc: 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
Subject: RE: Melding datalek

Top. Dank je wel.

Ik zit nu in overleg. Bel je zodra ik kan. Ondertussen nog wat punten aan het afstemmen en uitzoeken. Kan ik je daar gelijk over bijpraten.

Mvg,

5.1.2.e

Van: 5.1.2.e @wur.nl>
Verzonden: dinsdag 21 september 2021 10:47
Aan: Privacy ESA <privacy.esa@wur.nl>; 5.1.2.e @wur.nl>
CC: 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
Onderwerp: Re: Melding datalek

Ha 5.1.2.e, misschien even bellen?

Ik heb het formulier ingevuld

Van: Privacy ESA <privacy.esa@wur.nl>
Datum: dinsdag, 21 september 2021 om 10:38
Aan: 5.1.2.e @wur.nl>, 5.1.2.e @wur.nl>
CC: 5.1.2.e @wur.nl>, 5.1.2.e @wur.nl>
Onderwerp: RE: Melding datalek

Dank je wel voor de snelle antwoorden 5.1.2.e. Ik ga hiermee aan de slag en kom hier snel op terug. Mag ik jou aanspreken voor verdere vragen?

Is het datalekformulier ook ingevuld?

Mvg,

5.1.2.e

5.1.2.e

Onderwerp: PSIRT - datalek SSC
Locatie: Microsoft Teams-vergadering

Begin: di 21-9-2021 12:00
Einde: di 21-9-2021 12:30
Tijd weergeven als: Voorlopig

Terugkeerpatroon: (geen)

Vergaderingsstatus: Nog niet gereageerd

Organisator: 5.1.2.e
Verplichte deelnemers: 5.1.2.e

Optionele deelnemers: Privacy ESA; 5.1.2.e

Beste 5.1.2.e

Vandaag ontvingen wij een datalekmelding. Een collega binnen SSC heeft per ongeluk een Excelfile met persoonsgegevens over 8 studenten (naam, studentennummer, studievoortgang) gestuurd naar 900 studenten.

Wij zullen dit incident melden bij de toezichthouder (de AP), maar vanwege de aard van het incident en gevoeligheid van informatie moeten wij het ook aan alle 900 ontvangers melden.

Conform ons privacy- en incident response-beleid (bijgaand) en vanwege de met de melding gepaard gaande (reputationele) risico's nodig ik hierbij 5.1.2.e (woordvoerder), 5.1.2.e (situationeel eigenaar), 5.1.2.e (CISO), 5.1.2.e (ISO) en 5.1.2.e (F-G) uit voor een korte bespreking zodadelijk.

Groet, 5.1.2.e

Microsoft Teams-vergadering

Deelnemen op uw computer of via de mobiele app
Klik hier om deel te nemen aan de vergadering

Deelnemen met een apparaat voor videovergaderingen
wur@m.webex.com
Videovergaderings-id: 125 501 388 2
Alternatieve VTC-instructies

This is a Microsoft Teams meeting.

Meer informatie | Opties voor vergadering

5.1.2.e

Van: 5.1.2.e
Verzonden: dinsdag 21 september 2021 11:41
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: RE: PSIRT - datalek SSC

Ha 5.1.2.e

Dank je. Ik heb dit al met 5.1.2.e besproken.

Dit is de melding die ik kreeg:

> per abuis is een excelbestand met 2 en 6 studentnummers en namen en opleiding van non-EU studenten verstuurd per mail aan een groep waar ook studenten in zette (100 en 800 emailadressen). De inhoud van de mail gaat over onvoldoende studievoortgang

Dat zijn gevoeligheden die mogelijk nadelige gevolgen kunnen hebben voor de betrokkenen; de AVG verplicht ons dit te melden. In het PSIRT kunnen we bespreken/vaststellen aan wie we dit melden en hoe.

Groet, 5.1.2.e

5.1.2.e
5.1.2.e Corporate Governance & Legal Services

Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317-5.1.2.e
www.wur.nl/disclaimer

Van: 5.1.2.e
Verzonden: dinsdag 21 september 2021 11:37
Aan: 5.1.2.e
CC: 5.1.2.e @wur.nl>
Onderwerp: RE: PSIRT - datalek SSC
Urgentie: Hoog

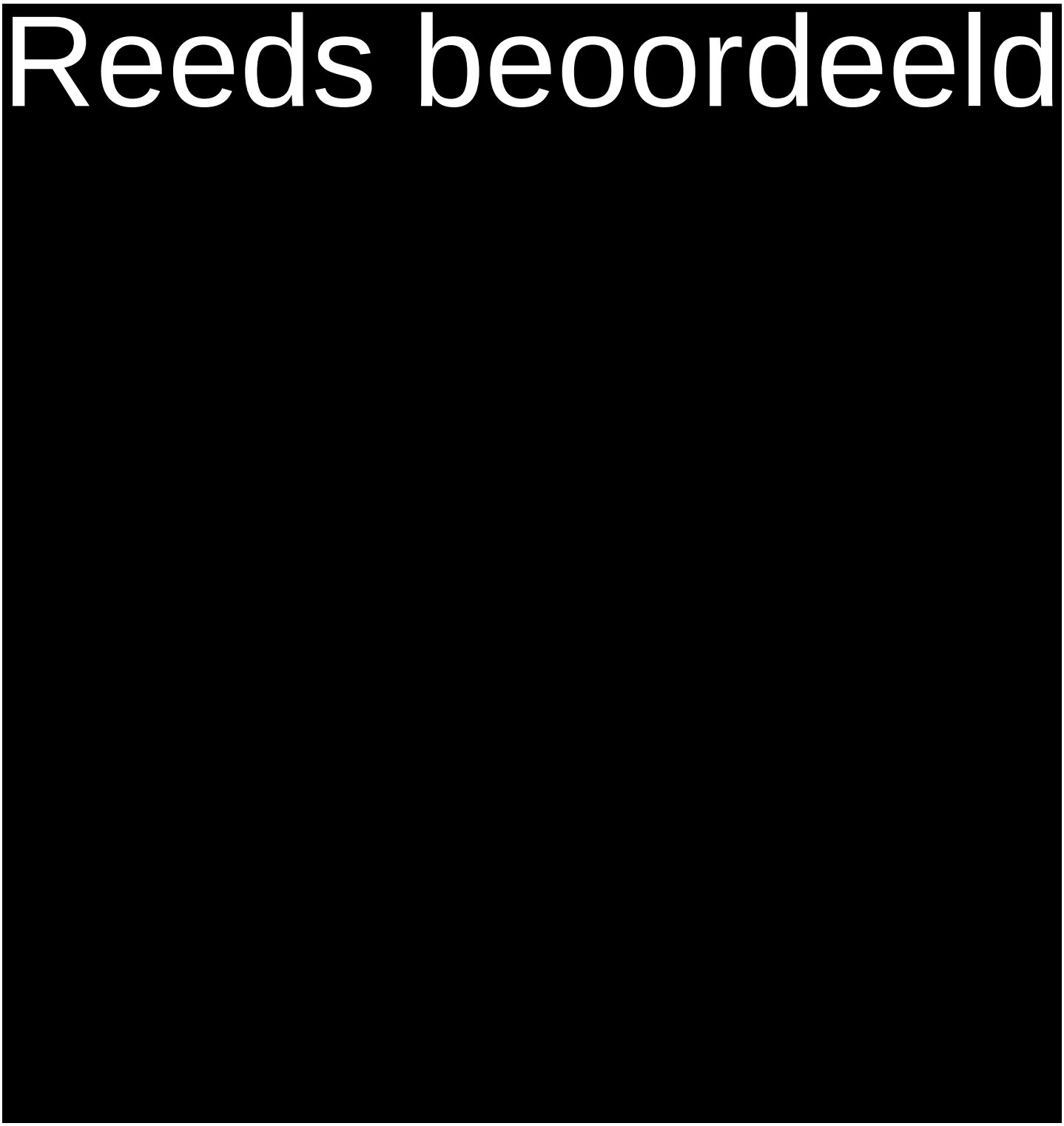
Beste 5.1.2.e

Dit is al opgepakt en ligt bij 5.1.2.e Check dit dus even met hem.
Ik denk dus dat deze meeting niet nodig is en dat dit nu wel erg hoog wordt opgenomen (naar mijn mening is het niet zo'n ingewikkeld incident).
Ik heb gister ook al uitgebreid met de opleidingsdirecteur gesproken en die is juist van mening om het niet te melden bij de studenten (zijn er ook geen 900!), omdat dat juist meer aandacht geeft. We hebben verder ook maar enkele vragen van studenten gehad en die zijn beantwoordt.

Hartelijke groet,
5.1.2.e

5.1.2.e
5.1.2.e Student Service Centre Wageningen University
Education and Student Affairs (ESA)
Forum, kamer 5.1.2.e
Monday – Thursday

Tel. 0317[redacted]
Email: [redacted]@wur.nl



AUTORITEIT
PERSOONSGEGEVENS

Ontvangstbevestiging van melding inbreuk

Dit is de kopie van uw melding van een inbreuk aan de Autoriteit Persoonsgegevens ten behoeve van uw eigen administratie.

Bewaar deze kopie goed. Bij twijfel kunt u met deze kopie achteraf aantonen dat u een melding van een inbreuk heeft gedaan bij de AP.

Meldingsnummer: 5.1.2.e

Melddatum: 21 september 2021

Meldtijdstip: 12:32

1 Introductie

1.1 De melding van een inbreuk

Wat wilt u doen?	Een nieuwe melding doen van een inbreuk
Wat voor soort datalekmelding wilt u doen?	Ik wil één inbreuk melden (reguliere melding)

1.2 Meldplicht AVG, Tw, Wjsg of Wpg

Op grond van welke wettelijke bepaling doet u deze melding?	Algemene verordening gegevensbescherming (AVG)

1.3 Andere toezichthouders

Heeft uw organisatie of bedrijf de inbreuk gemeld bij toezichthouders op andere meldplichten? Of gaat u dat nog doen?	Nee

2 Internationale aspecten

2.1 Grensoverschrijdende inbreuk

Heeft de inbreuk gevolgen voor personen in meerdere landen?	Nee

3 De verwerkingsverantwoordelijke

3.1 Gegevens verwerkingsverantwoordelijke

AUTORITEIT PERSOONSGEGEVENS

KvK-nummer	09215846
Naam van het bedrijf of de organisatie	Wageningen University
Adres	Droevendaalsesteeg 4
Postcode	6708 PB
Plaats	Wageningen

In welke sector is de organisatie of het bedrijf actief?

[✓] Onderwijs

[✓] Tertiair onderwijs

3.2 Gegevens melder en contactpersoon

Wie meldt de inbreuk?

Naam	5.1.2.e
Functie	corporate privacy officer
E-mailadres	privacy@wur.nl
Telefoonnummer	0317 5.1.2.e
Is de melder de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen voor nadere informatie over de melding?	Nee
Naam contactpersoon	5.1.2.e
Functie contactpersoon	F-G
E-mailadres contactpersoon	dpo@wur.nl
Telefoonnummer contactpersoon	0317 5.1.2.e

AUTORITEIT PERSOONSGEGEVENS

3.3 Andere organisaties

Waren er andere organisaties betrokken bij de inbreuk?	Nee

4 Tijdlijn

4.1 Duurt de inbreuk op dit moment nog voort?	Nee
(Mogelijke) startdatum van de inbreuk	20-9-2021
(Mogelijke) einddatum van de inbreuk	20-9-2021
4.2 Wanneer is het incident ontdekt?	20-9-2021
4.3 Geef (kort) aan hoe u de inbreuk heeft ontdekt	Een collega heeft per ongeluk een Excelfile met persoonsgegevens verzonden aan onbevoegde ontvangers. Dit werd direct na verzending ontdekt en intern gemeld.
4.4 Is dit het moment waarop u het incident heeft bestempeld als inbreuk (“datalek”) en dus kennis heeft gekregen van de inbreuk?	Ja

5 Gegevens over de inbreuk

5.1 Aard van de inbreuk

[✓] Persoonsgegevens (mogelijk) ingezien door onbevoegden

5.2 Aard van het incident

Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest?

[✓] E-mail met persoonsgegevens verstuurd aan verkeerde ontvanger(s)

Heeft de verkeerde ontvanger bevestigd de e-mail te hebben verwijderd?	Nee

5.3 Beschrijving van het incident

AUTORITEIT PERSOONSGEGEVENS

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest	Een collega binnen het Student Service Center van Wageningen University heeft per ongeluk een Excelfile met persoonsgegevens over 6 resp. 2 internationale studenten (naam, studentennummer, studievoortgang) gestuurd naar 800 resp. 100 studenten.

5.4 Optioneel: upload hier relevante ondersteunende documentatie bij uw melding.

6 Welke persoonsgegevens

6.1 Persoonsgegevens in het algemeen

[✓] Naam

[✓] Contactgegevens

[✓] E-mailadres

[✓] Anders

Namelijk:	studievoortgang

6.2 Bijzondere categorieën van persoonsgegevens

Meerdere opties zijn mogelijk.

6.3 Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords ("**-gegevensregisters**") zijn getroffen door het datalek	2
Geef een toelichting op bovengenoemd aantal:	Het betreft twee Excelfiles met gegevens over 2 resp. 6 studenten

7 Getroffen personen

7.1 Welke groep(en) betrokkenen is (zijn) getroffen door de inbreuk?

Meerdere opties zijn mogelijk.

[✓] Leerlingen of studenten

AUTORITEIT PERSOONSGEGEVENS

7.2 Geef een nadere omschrijving van de groep(en) betrokkenen.	Internationale studenten van Wageningen University
7.3 Is het exacte aantal betrokkenen bekend?	Ja
Het exacte aantal is:	8

8 Maatregelen vooraf

8.1 Waren de persoonsgegevens voordat de inbreuk zich voordeed versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden?

[✓] Nee

9 Gevolgen

9.1 (Mogelijke) gevolgen voor de verwerkingsverantwoordelijke en de persoonsgegevens.

Meerdere opties zijn mogelijk.

[✓] Onbevoegden hebben kennis kunnen nemen van de gegevens

9.2 (Mogelijke) gevolgen voor de betrokkene(n)

Meerdere opties zijn mogelijk.

[✓] Discriminatie of uitsluiting

9.3 Inschatting risico

Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkene(n)	Verwaarloosbaar
Licht uw keuze toe:	De meest in het oog springende categorie betreft persoonsgegevens over studievoortgang. Dit kan mogelijk risico's hebben voor de betreffende studenten in de zin dat zij hierop aangesproken kunnen worden, maar voor andere studenten is dit geen relevante / misbruikbare informatie.

AUTORITEIT PERSOONSGEGEVENS

10 Vervolgacties naar aanleiding van de inbreuk

10.1 Informeren van de betrokkene(n)

Heeft u de inbreuk reeds gemeld aan de betrokkene(n)?	Nee
Gaat u de inbreuk nog melden aan de betrokkene(n)?	Ja
Aan hoeveel personen wilt u de inbreuk gaan melden?	8
Wanneer gaat u (naar verwachting) de inbreuk melden aan de betrokkene(n)?	22-9-2021
Wat is de inhoud van de melding aan degene van wie gegevens zijn gelekt?	[nog niet precies vastgesteld]

Optioneel: upload hier een kopie van de tekst van deze kennisgeving.

Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken om de betrokkene(n) te informeren?

Meerdere opties zijn mogelijk.

[✓] Per e-mail

10.3 Maatregelen om de inbreuk aan te pakken

Heeft uw organisatie maatregelen getroffen om de inbreuk aan te pakken?	Nee, want:
Toelichting:	Het verzenden van de Excelfiles kan niet achteraf gerepareerd worden. Het actief benaderen van de 900 ontvangers met het verzoek de e-mail te verwijderen staat niet in verhouding tot de aard van het incident en de gegevens. Dit zou naar onze inschatting juist de nadruk leggen op het bestand. Bovendien is er voor de 900 ontvangers geen materieel vervolgrisico (zoals bij phishing).
Heeft uw organisatie maatregelen getroffen om nieuwe soortgelijke inbreuken te voorkomen?	Ja, namelijk:
Toelichting:	

Verzending zal in de toekomst geautomatiseerd	verlopen via een systeem en niet meer via

11 Verzenden

Is dit een voorlopige of een definitieve melding?	Nee, de melding is voorlopig. Er komt later een vervolgmelding met aanvullende informatie over de inbreuk
Geef aan wanneer u (uiterlijk) een vervolgmelding doet	24-9-2021

[✓] Door dit vakje aan te vinken verklaart u dit formulier naar waarheid in te vullen

[✓] Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen namens uw organisatie.

Privacyverklaring

[✓] Ik ben op de hoogte van de inhoud van de Privacyverklaring van de AP

AUTORITEIT PERSOONSGEGEVENS

Ontvangstbevestiging van melding inbreuk

Dit is de kopie van uw melding van een inbreuk aan de Autoriteit Persoonsgegevens ten behoeve van uw eigen administratie.

Bewaar deze kopie goed. Bij twijfel kunt u met deze kopie achteraf aantonen dat u een melding van een inbreuk heeft gedaan bij de AP.

Meldingsnummer: 5.1.2.e

Melddatum: 23 september 2021

Meldtijdstip: 08:41

1 Introductie

1.1 De melding van een inbreuk

Wat wilt u doen?	Een bestaande melding aanvullen of aanpassen
Beschikt u over het meldingsnummer van de oorspronkelijke melding?	Ja
Dit is het meldingsnummer:	5.1.2.e

2 Aanvulling op eerdere samenvatting

2.1 Wie dient de aanvulling in?

Naam	5.1.2.e
Functie	corporate privacy officer
E-mailadres	privacy@wur.nl
Telefoonnnummer	0317 5.1.2.e
2.2 Is de indiener de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen voor nadere informatie over de melding en aanvulling	Nee
Naam contactpersoon	5.1.2.e

AUTORITEIT PERSOONSGEGEVENS

Functie contactpersoon	F-G
E-mailadres contactpersoon	dpo@wur.nl
Telefoonnummer contactpersoon	031 5.1.2.e

3 Welke vragen

3.1 Welke vragen wilt u wijzigen of aanvullen?

[✓] 10. Vervolgacties

[✓] Informeren van de betrokkene(n) (de getroffen persoon of personen)?

10 Vervolgacties naar aanleiding van de inbreuk

10.1 Informeren van de betrokkene(n)

Heeft u de inbreuk reeds gemeld aan de betrokkene(n)?	Ja
Aan hoeveel personen heeft u de inbreuk gemeld?	8
Wanneer heeft u de inbreuk gemeld aan de betrokkene(n)?	21-9-2021
Wat is de inhoud van de melding aan degene van wie gegevens zijn gelekt?	Dear <name student>, On Tuesday 20 September, we have been given notice that a data breach incident has occurred. Unfortunately, your data and that of 7 other students (specific: student number, study progress) has been disclosed, for which we apologize. The information, meant for teaching staff, has been sent out to a larger group WUR students. We are taking the following steps in line with GDPR regulations to limit the consequences and prevent a future event. • The data breach is reported to the Autoriteit Persoonsgegevens • For future communication on this subject, WUR will use direct communication through Osiris This e-mail is in line with GDPR official communication procedures. If you have any

AUTORITEIT PERSOONSGEGEVENS

questions regarding the information above, please contact us, we'd be glad to answer. On behalf of:	5.1.2.e 5.1.2.eStudent Service Centre Wageningen University Education and Student Affairs (ESA)

Optioneel: upload hier een kopie van de tekst van deze kennisgeving.

Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken om de betrokkene(n) te informeren?

Meerdere opties zijn mogelijk.

[✓] Per e-mail

11 Verzenden

Is dit een voorlopige of een definitieve melding?	Ja, de melding is definitief. Ik heb de vereiste informatie verstrekt en er is geen vervolgmelding nodig

[✓] Door dit vakje aan te vinken verklaart u dit formulier naar waarheid in te vullen

[✓] Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen namens uw organisatie.

Privacyverklaring

[✓] Ik ben op de hoogte van de inhoud van de Privacyverklaring van de AP

5.1.2.e

Van: 5.1.2.e
Verzonden: vrijdag 21 mei 2021 09:02
Aan: 5.1.2.e
Onderwerp: Datalek

Ha 5.1.2.e

Allereerst: gefeliciteerd met de 60e verjaardag van je man!

Dan, minder belangrijk, maar heb jij toevallig nog een update rond het incident met Formdesk? Is er een risico dat er iets gelekt is van onze persoonsgegevens? Zo ja, kun jij mij dan van de achtergrondinformatie voorzien?

Groet, 5.1.2.e

5.1.2.e
5.1.2.e | Corporate Governance & Legal Services

WAGENINGEN UNIVERSITY & RESEARCH

Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e | Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. +31 317 5.1.2.e

Privacy

Van: Privacy
Verzonden: vrijdag 21 mei 2021 12:39
Aan: 5.1.2.e
CC: 5.1.2.e ; Privacy ESG; 5.1.2.e
Onderwerp: RE: Update vermeend datalek Formdesk

Dag 5.1.2.e

Helder verhaal en dat lijken mij prima vervolgacties. Ik denk dat het belangrijk is om prioriteit te zetten om te onderzoeken - aan de hand van de logging - hoe de bestanden begin mei kunnen zijn verwijderd zodat wij met zekerheid kunnen uitsluiten dat sprake is van een incident, maar ik deel vooralsnog je conclusie dat niet direct sprake lijkt te zijn van een (meldplichtig) datalek.

Bedankt voor de acties en goed weekend alvast.

Groet, 5.1.2.e

5.1.2.e
Corporate Privacy Officer | Corporate Governance & Legal Services

Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317 5.1.2.e
www.wur.nl/disclaimer

Van: 5.1.2.e @wur.nl>
Verzonden: vrijdag 21 mei 2021 12:27
Aan: 5.1.2.e g@wur.nl>; 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>; 5.1.2.e wur.nl>
CC: 5.1.2.e @wur.nl>; Privacy ESG <privacy.esg@wur.nl>
Onderwerp: Update vermeend datalek Formdesk

Collega's,

Ik heb vanmorgen contact gehad met 5.1.2.e van Formdesk naar aanleiding van mijn melding bij hen over het vermoeden van een datalek
Aanleiding: op 19 mei is een mogelijk datalek bij mij gemeld door 5.1.2.e en op 20 mei is dit door mij besproken met 5.1.2.e en 5.1.2.e .
Ik heb op 20 mei tevens ruggenspraak gehouden met 5.1.2.e en 5.1.2.e en heb vervolgens bij Formdesk een melding gedaan met het verzoek contact op te nemen. Dat heeft op de 21e plaatsgevonden.

Wat we nu weten:
Er is geen hack bekend bij of gesignaleerd door Formdesk.
Blijkbaar loggen jullie allen in via het account van 5.1.2.e , die hiervoor zijn accountgegevens met 5.1.2.e , en anderen heeft gedeeld.
Het account staat op naam van 5.1.2.e en ene 5.1.2.e . De laatste kan ik niet vinden op ons intranet. Kan 5.1.2.e of 5.1.2.e daar wellicht duidelijkheid in geven?
Zichtbaar is dat er op 4 mei bestanden zijn verwijderd en dat op 12 mei een nieuw wachtwoord is aangemaakt door 5.1.2.e , zoals 5.1.2.e aangaf in zijn mail.

Vervolg:
Volgende week ontvang ik de logfiles van 1 april t/m 12 mei. Zichtbaar wordt dan wanneer er is ingelogd en of er bestanden zijn gedownload.
Aan degenen die gebruik maken van het account van 5.1.2.e dan de vraag om vervolgens te checken of er niet herleidbare inlog- en downloadacties hebben plaatsgevonden.

5.1.2.e Gezien de bevindingen op dit moment lijkt het niet waarschijnlijk dat er een datalek heeft plaatsgevonden en hoeft er mogelijk nog geen melding gedaan te worden?

Advies:
Ik adviseer om het account van 5.1.2.e uit te breiden met meer gebruikers die hun eigen inlog krijgen. Dat maakt het gebruiken van het Formdesk account in ieder geval overzichtelijker en veiliger.
Als er geen verwerkersovereenkomst is met Formdesk dan adviseer ik om deze alsnog af te sluiten.

Tot zover de update. Alvast een goed weekend gewenst.
Groet, 5.1.2.e

5.1.2.e
Privacy Officer Social Sciences Group (SSG) / Environmental Sciences Group (ESG) / Agrotechnology & Food Sciences Group (AFSG)
Wageningen University & Research
+31 3175.1.2.e continues to mobile
5.1.2.e n@wur.nl

DATADANGERS, bekijk de WUR-film over het belang van onze data-schatkamer en hoe deze goed te beschermen.
Vragen? Mail, bel of maak een afspraak.

I am available on Monday, Tuesday, Wednesday, Thursday and Friday morning.
Meer privacy informatie vind je hier

5.1.2.e

Van: 5.1.2.e
Verzonden: dinsdag 25 mei 2021 17:29
Aan: 5.1.2.e
CC: 5.1.2.e Privacy ESG; 5.1.2.e
Onderwerp: RE: Update vermeend datalek Formdesk

Allen,

In aansluiting op onderstaande mail van 5.1.2.e nog het volgende.
Via 5.1.2.e heb ik de logs ontvangen, zie hieronder. Het is een korte lijst gelukkig. Ik heb 5.1.2.e al gevraagd of hij wil aangeven op welke data hij (zeer waarschijnlijk) heeft ingelogd.

Aan 5.1.2.e en eventueel andere gebruikers de vraag hetzelfde te doen en mij die informatie te sturen. Indien mogelijk deze week.
Op deze manier kunnen we als het goed is uitsluiten dat er een ongewenste bezoeker is geweest.

Dan hebben we nog de acties whitelistprocedure en het afsluiten van een verwerkersovereenkomst open staan.
Tevens raadzaam is om oud collega 5.1.2.e als gebruiker te verwijderen omdat zij inmiddels gepensioneerd is en er geen gebruik meer van maakt.
Eerder heb ik al geadviseerd om het account uit te breiden, zodat elke gebruiker een eigen wachtwoord heeft. Uit het oogpunt van security is dit een betere optie dan het delen van inloggegevens.

Als we dit alles hebben afgerond kunnen we:
naar alle waarschijnlijkheid concluderen dat er geen datalalek is geweest en
kan er, na afronding van de whitelistprocedure en het afsluiten van een verwerkersovereenkomst met een gerust hart en AVG-proof verder worden samengewerkt met Formdesk.

Bij dit alles wil ik jullie uiteraard behulpzaam zijn.

Fijne avond. Groet, 5.1.2.e

Date	Van	Tot	User	Remoteaddr
31-03-2021	13:52:46	13:53:24	supervisor	45.155.157.68
01-04-2021	09:21:58	09:27:41	supervisor	45.155.157.68
06-04-2021	07:54:24	08:08:04	supervisor	80.100.167.207
08-04-2021	11:17:28	11:22:18	supervisor	45.155.157.68
13-04-2021	10:25:58	10:28:03	supervisor	137.224.252.13
13-04-2021	15:51:01	16:42:49	supervisor	80.100.167.207
14-04-2021	07:08:29	07:11:20	supervisor	80.100.167.207
19-04-2021	07:24:19	14:48:10	supervisor	80.100.167.207
26-04-2021	14:08:49	14:20:04	supervisor	45.155.157.68
26-04-2021	09:31:33	09:37:06	supervisor	80.100.167.207
26-04-2021	13:27:03	13:27:05	supervisor	84.80.219.160
29-04-2021	08:05:40	08:13:18	supervisor	80.100.167.207
03-05-2021	18:29:11	18:29:57	supervisor	45.155.157.68
03-05-2021	11:13:52	15:05:25	supervisor	92.108.42.60
04-05-2021	09:14:18	15:35:29	supervisor	92.108.42.60
06-05-2021	11:45:19	11:59:52	supervisor	92.108.42.60
07-05-2021	08:29:26	08:29:26	supervisor	92.108.42.60
11-05-2021	09:56:06	09:59:05	supervisor	45.155.157.68
11-05-2021	14:14:53	14:35:24	supervisor	80.100.167.207
11-05-2021	12:15:51	12:18:46	supervisor	92.108.42.60
12-05-2021	12:52:59	12:53:01	supervisor	137.224.252.29
12-05-2021	09:11:50	09:12:28	supervisor	45.155.157.68
12-05-2021	09:35:13	09:55:55	supervisor	80.100.167.207

5.1.2.e
Privacy Officer Social Sciences Group (SSG) / Environmental Sciences Group (ESG) / Agrotechnology & Food Sciences Group (AFSG)
Wageningen University & Research
+31 317 5.1.2.e continues to mobile
5.1.2.e @wur.nl

DATADANGERS, bekijk de WUR-film over het belang van onze data-schatkamer en hoe deze goed te beschermen.
Vragen? Mail, bel of maak een afspraak.

I am available on Monday, Tuesday, Wednesday, Thursday and Friday morning.
Meer privacy informatie vind je hier

From: 5.1.2.e @wur.nl>
Sent: vrijdag 21 mei 2021 17:30
To: 5.1.2.e @wur.nl>; 5.1.2.e wur.nl>; 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
Cc: 5.1.2.e @wur.nl>; Privacy ESG <privacy.esg@wur.nl>
Subject: RE: Update vermeend datalek Formdesk

Dag allen,

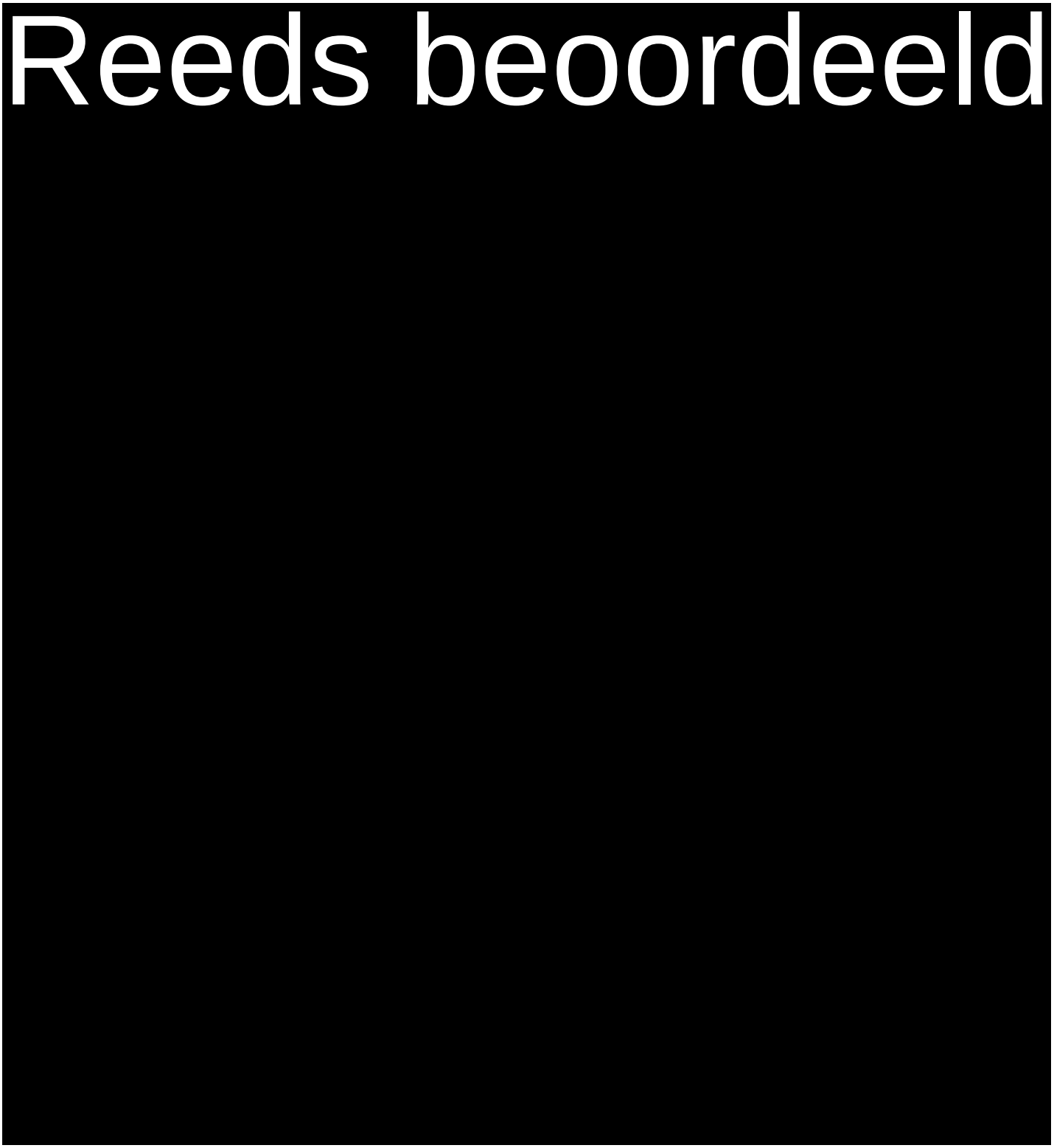
Ik werk nu meer dan 10 jaar met de applicatie Formdesk. Vooral in de eerste 5 jaar heb ik veel gebruik gemaakt van deze tool om vooral formulieren aan te bieden voor klimaatprogramma's. Mijn oud collega 5.1.2.e maakte hier ook vaak gebruik van, onder meer voor internationale conferenties. 5.1.2.e is een aantal jaren geleden met pensioen gegaan. In de afgelopen jaren heb ik nauwelijks meer gebruik gemaakt van Formdesk. Ik heb destijds WIMEK/SENSE geadviseerd gebruik te maken van deze handige tool.

In de afgelopen jaren heb ik zo nu en dan een nieuwsbrief/notificatie ontvangen wanneer er zich een verstoring had voorgedaan. Van de vermeende datalek heb ik geen bericht ontvangen van Formdesk. Mogelijk heeft de Google melding ons op het verkeerde been gezet of was er iets anders aan de hand.

Nav de Google melding heb ik nog es gekeken in Formdesk en heb ik op 4 mei oude materialen verwijderd, maar welke weet ik niet meer, en kan ik niet meer nagaan omdat de inlogprocedure is aangepast (ik kan momenteel niet inloggen, maar dat komt wel weer als ik met 5.1.2.e heb afgestemd).

De logfiles heb ik vanmiddag van Formdesk ontvangen en doorgestuurd naar 5.1.2.e.

Groet, 5.1.2.e



5.1.2.e

Van: Privacy
Verzonden: dinsdag 7 september 2021 10:35
Aan: 5.1.2.e
Onderwerp: Nieuwe datalekmelding | 9/7/2021 8:35:16 AM | 5.1.2.e @wur.nl

Urgentie: Hoog

Beste collega,

Zojuist is er een nieuw datalek gemeld via het digitale meldformulier:

* * *

1. Geef een zo gedetailleerd mogelijke omschrijving van het incident
Er is een overzicht met openstaande verzuimgevallen gestuurd naar 2 leidinggevenden en 2 controllers van WLR met gegevens die vanuit heel ASG zijn en niet alleen WLR.

2. Wat is de aard van het incident?
Een overzicht met openstaande ziekmeldingen (naam en geboorte datum) voor WLR, bevatte de ziekmeldingen van ASG. Terwijl ik geen rechten heb voor heel ASG, alleen WLR.

3. Hoelang heeft het incident geduurd?
Eén dag

4a. Gedurende welke periode heeft het incident plaatsgevonden?

4b. Op welke datum heeft het incident plaatsgevonden?
2021-09-06

5. Van welke categorie personen zijn persoonsgegevens gelekt?
["Medewerkers"]

6. Van hoeveel personen zijn mogelijk persoonsgegevens gelekt?
51 (waarvan een gedeelte de medewerkers van WLR waar de betreffende personen wel de gegevens van mogen zien)

7. Op welke datum/tijdstip is het incident ontdekt?
Op de 6e september, paar uur na het versturen van de mail.

8. Wat voor soort persoonsgegevens zijn betrokken in het incident?
["naam en geboortedatum "]

9. Welke acties zijn ondernomen naar aanleiding van het incident?
Alle betrokkenen hebben direct een mail ontvangen met het verzoek het document te verwijderen uit hun mail en verwijderde items.

* * *

Met vriendelijke groet,
5.1.2.e

5.1.2.e
Corporate Privacy Officer | 5.1.2.e

Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317-5.1.2.e

Privacy

Van: Privacy
Verzonden: dinsdag 7 september 2021 12:15
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: Datalekmelding

Beste 5.1.2.e

Bedankt voor je datalekmelding. Hoewel formeel sprake is van een 'datalek' (namelijk: onbevoegden hebben inzage gekregen in gevoelige gegevens van medewerkers van heel ASG in plaats van alleen WLR), is met de acties die jullie hebben genomen naar onze inschatting geen sprake van een kans op nadelige gevolgen voor de betrokken medewerkers. Daarvan uitgaande hoeven wij dit incident niet te melden bij de toezichthouder.

Nog één vraagje: hebben de vier ontvangers van de e-mail inmiddels ook bevestigd de e-mail te hebben verwijderd? Zo nee, dan is dat wellicht iets om nog even opvolging op te geven zodat vastligt dat geen sprake is van een risico in dat verband.

Vriendelijke groet,
5.1.2.e

5.1.2.e
Corporate Privacy Officer | 5.1.2.e
Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e | Droevendaalsesteeg 4
6708 PB Wageningen
Tel. +31 317 5.1.2.e

Privacy

Van: Privacy ESA
Verzonden: woensdag 7 juli 2021 15:16
Aan: 5.1.2.e
CC: privay@wur.nl
Onderwerp: RE: e-mail adressen

Ook voor jullie administratie

Dank 5.1.2.e Het is geen ernstig datalek. Gelukkig. Het wordt al iets anders als er dus minderjarigen betrokken zijn. BCC is het uitgangspunt, maar inderdaad zou een event organiseren via TEAMS (of ZOOM) een mogelijkheid zijn om van daaruit een specifieke uitnodiging te sturen. Al ben ik niet bekend met hoe dit praktisch is in geregeld binnen WUR. Daar zou het team van 5.1.2.e je waarschijnlijk meer over kunnen vertellen. Zij beheren voor zover ik weet ZOOM en andere onderwijsondersteunende applicaties.

Mocht je willen, dan kan ik altijd meekijken bij de organisatie van studentgerichte activiteiten privacygericht zijn ingeregeld. Mocht je dat op prijs stellen, dan kunnen we er altijd over van gedachten wisselen met een virtuele kop koffie.

Gr,

5.1.2.e

Van: 5.1.2.e @wur.nl>
Verzonden: woensdag 7 juli 2021 13:04
Aan: 5.1.2.e @wur.nl>
Onderwerp: FW: e-mail adressen
Urgentie: Hoog

Hallo 5.1.2.e

Het formulier is opgestuurd. Er zitten geen minderjarige bij. Veel van de aankomende studenten hebben zelf al een bevestiging gestuurd, Ik verwacht dat bijna iedereen hem dus al gelezen heeft, dus terugtrekken is volgens mij niet meer nuttig/mogelijk.

Heb jij een idee hoe we dit volgend jaar beter kunnen aanpakken. Is het mogelijk om een online meeting aan te maken voor onze aankomende studenten waar zij niet elkaars e-mail adressen zouden zien? Zou een meeting met Zoom dan een optie zijn?

Mocht er nog actie van mij nodig zijn hoor ik het wel.
Groeten
5.1.2.e

Van: Privacy ESA <privacy.esa@wur.nl>
Verzonden: Wednesday, July 7, 2021 11:27 AM
Aan: 5.1.2.e @wur.nl>
Onderwerp: RE: e-mail adressen
Urgentie: Hoog

Goedemorgen 5.1.2.e

Goed dat je het meldt. Dat valt onder een datalek. Gelukkig niet ernstig. Heb je een mogelijkheid om de mail in te trekken en opnieuw uit te sturen? Of om op een andere manier te repareren? Zitten hier minderjarigen bij?

Wil je het volgende formulier invullen? Mocht je daar hulp bij nodig hebben, dan ben ik beschikbaar om je te ondersteunen.

https://forms.office.com/Pages/ResponsePage.aspx?id=5TfRJx92wU2viNJkMKuxj8w45Nmm-ZdEk8XzZ0GPbGRUN043UlITMkwxS1dWOFZVN0RXODUxOFgzNy4u

Met vriendelijke groet,

5.1.2.e
Privacy Officer
Wageningen University & Research
Education & Student Affairs (ESA), Social Sciences Group (SSG),
Environmental Sciences Group (ESG) & Agrotechnology & Food Sciences Group (AFSG)
PO Box 9100, 6700 HA Wageningen
Wageningen Campus, Atlas Building, Droevendaalsesteeg 4, 6708 PB Wageningen
0317 – 5.1.2.e
disclaimer

WUR is serious about Data

DATADANGERS, de WUR-film over het belang van onze data-schatkamer en hoe deze goed te beschermen.
Vragen? Mail, bel of maak een afspraak.

Van: 5.1.2.e @wur.nl>
Verzonden: woensdag 7 juli 2021 11:13
Aan: Privacy ESA <privacy.esa@wur.nl>
Onderwerp: e-mail adressen

Hoi 5.1.2.e,

Bij het sturen van een uitnodiging voor een teams meeting aan aankomend studenten zijn de e-mail adressen per ongeluk niet in de bcc gezet en sowieso zodra mensen geaccepteerd hebben zien ze elkaars e-mail adressen blijkt (de tweede badge hadden we door en wel in bcc gedaan). Moeten we hier iets mee doen?

Groeten,
5.1.2.e

5.1.2.e
5.1.2.e
Wageningen University
Wageningen Campus; Radix; room 5.1.2.e
+31 (0)317 5.1.2.e
+31 (0)317 5.1.2.e
5.1.2.e @wur.nl
www.wur.nl/bbi
www.wur.nl/mbi
www.disclaimer-nl.wur.nl

Privacy

Van: Privacy ESA
Verzonden: donderdag 5 augustus 2021 15:50
Aan: Privacy
Onderwerp: FW: Onverwacht mensen in BCC tijdens mail

Ter info.

Van: Privacy ESA
Verzonden: donderdag 5 augustus 2021 15:49
Aan: Office, Biologie <office.biologie@wur.nl>
CC: 5.1.2.e @wur.nl>
Onderwerp: RE: Onverwacht mensen in BCC tijdens mail

Goedemiddag 5.1.2.e

Goed dat je dit incident meldt en vooral vervelend voor de betrokken student. De eerste stap die je hebt gezet naar IT is prima. Daarmee kunnen zij kijken wat het probleem met de BCC veroorzaakt en dit voor je oplossen. Ik ben erg benieuwd. Wil jij mij daarvan op de hoogte houden?

Het incident valt onder de noemer datalek en is vervelend, maar wordt doorgaans als niet ernstig beoordeeld. Het wordt ernstiger als we medische gegevens of andere bijzondere gegevens delen of gegevens over grotere groepen studenten per ongeluk verkeerd adresseren. Is daar naar jouw beoordeling sprake van? Uit jouw tekst haal ik niet direct dat dit het geval is. Het is vooral belangrijk dat we de student nu goed begeleiden en mocht het nodig zijn, dan help ik zowel jou als de student natuurlijk verder.

Het datalek moet in het WUR datalek register gemeld worden. Wil je dit doen door dit formulier in te vullen? Het melden van betrokkenen heb je voortvarend opgepakt. Dat is mooi werk van je. Toch is het handiger om dit vooraf even af te stemmen. Dan help ik je daar graag bij. Als we betrokken personen namelijk benaderen na een (potentieel) datalek moeten we bepaalde informatie delen om volledig te zijn. Ik snap dat dit nu niet gebeurd is en je hoeft voor nu op dit vlak zeker geen vervolgstap te zetten.

Nogmaals dank voor je melding en mocht ik je verder kunnen ondersteunen dan kan dat altijd. Bij voorkeur kunnen we daar morgenochtend over schakelen, daarna ben ik op vakantie. Mijn collega's van privacy@wur.nl kunnen je tijdens mijn verlof ondersteunen.

Met vriendelijke groet,

5.1.2.e
Privacy Officer
Wageningen University & Research
Education & Student Affairs (ESA), Social Sciences Group (SSG),
Environmental Sciences Group (ESG) & Agrotechnology & Food Sciences Group (AFSG)
PO Box 9100, 6700 HA Wageningen
Wageningen Campus, Atlas Building, Droevendaalsesteeg 4, 6708 PB Wageningen
0317 – 5.1.2.e

WUR is serious about Data

DATADANGERS, de WUR-film over het belang van onze data-schatkamer en hoe deze goed te beschermen.
Vragen? Mail, bel of maak een afspraak.

Van: Office, Biologie <office.biologie@wur.nl>
Verzonden: donderdag 5 augustus 2021 13:34
Aan: Privacy ESA <privacy.esa@wur.nl>
CC: 5.1.2.e @wur.nl>
Onderwerp: Onverwacht mensen in BCC tijdens mail
Urgentie: Hoog

Beste 5.1.2.e

Vanochtend heb ik vanuit de Office mailbox van Biologie gereageerd op een mail van een student. Even later bleek dat er in die mail meer dan 100(!) mensen in de BCC stonden. Ik heb IT direct gebeld om de mail terug te vragen, maar ook veel hadden al gereageerd dat deze mail waarschijnlijk niet voor hen bedoelt was. Daarna heb ik een mail gestuurd naar alle mensen in de BCC met excuses en of ze de eerder gekregen mail willen verwijderen.
In de mail van de student geeft hij aan dat hij het afgelopen jaar door corona moeite heeft gehad met studeren, en dat hij bang is dat hij zijn hertentamens niet heeft gehaald en daardoor zijn BSA niet haalt met de vraag of wij nog advies hebben. Als u wil kan ik uiteraard de mail conversatie aan u doorsturen.
Ik heb even gekeken in de lijst met emailadressen in de BCC. Het gaat om mensen die al meer dan 5 jaar zijn afgestudeerd. Ik weet 100% zeker dat ik hen niet heb toegevoegd aan de BCC. Ik heb IT ook nog een mail gestuurd hoe dit heeft kunnen gebeuren.

Nu is mijn vraag, wat kan ik verder nog doen en moet ik de betreffende student op de hoogte stellen?

Ik hoor heel graag van u.

Met vriendelijke groet,
Kindest regards,

5.1.2.e
Studyadvisor
Master Aquaculture & Marine Resource Management
Bachelor Biology
Bachelor & Master Nutrition and Health

Wageningen University & Research
Wageningen campus, Radix building 107
Room 5.1.2.e
T: +31 (0)317-5.1.2.e
E: 5.1.2.e @wur.nl

5.1.2.e

Van: Privacy
Verzonden: woensdag 7 juli 2021 13:01
Aan: Privacy; 5.1.2.e
Onderwerp: Nieuwe datalekmelding | 7/7/2021 11:01:01 AM | 5.1.2.e

Urgentie: Hoog

Beste collega,

Zojuist is er een nieuw datalek gemeld via het digitale meldformulier:

* * *

1. Geef een zo gedetailleerd mogelijke omschrijving van het incident
Er is een uitnodiging verstuurd voor een Team vergadering voor de studenten die in September gaan beginnen aan de master biologie (Totaal 80 aankomende studenten). Hiervoor zijn de studielink e-mail adressen gebruikt. Alle deelnemers waren als Optional deelnemer gezet. Bij de bevestiging van aanwezigheid van de studenten bedacht de studieadviseur dat de aankomende studenten elkaars studielink e-mail adres konden zien. De uitnodigingen zijn verstuurt en ongeveer de helft van de studenten heeft al gereageerd. Het is dus mogelijk voor de studenten om de studielink e-mail adressen van de andere studenten te zien.

2. Wat is de aard van het incident?
Studielink e-mail adressen van aankomende studenten zichtbaar voor andere studenten die aan dezelfde master gaan beginnen.

3. Hoelang heeft het incident geduurd?
Meer dan één dag

4a. Gedurende welke periode heeft het incident plaatsgevonden?
De uitnodiging is op maandag 5 jul in de ochtend verstuurd. De studenten hebben de mail al ontvangen en op gereageerd, dus ongedaan maken is niet meer mogelijk.

4b. Op welke datum heeft het incident plaatsgevonden?

5. Van welke categorie personen zijn persoonsgegevens gelekt?
["Aankomende studenten"]

6. Van hoeveel personen zijn mogelijk persoonsgegevens gelekt?
80

7. Op welke datum/tijdstip is het incident ontdekt?
6 Juli

8. Wat voor soort persoonsgegevens zijn betrokken in het incident?
["e-mail adressen"]

9. Welke acties zijn ondernomen naar aanleiding van het incident?
Gemeld bij leidinggevende

* * *

Met vriendelijke groet,

5.1.2.e

Corporate Privacy Officer | 5.1.2.e

Wageningen University & Research

Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e, Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317-5.1.2.e

Privacy

Van: Privacy
Verzonden: dinsdag 11 mei 2021 08:55
Aan: 5.1.2.e
Onderwerp: FW: Nieuwe datalekmelding | 4/30/2021 12:36:59 PM 5.1.2.e @wur.nl

Urgentie: Hoog

Ha 5.1.2.e, kunnen wij hier even contact over hebben?

Groet, 5.1.2.e
5.1.2.e
Corporate Privacy Officer | Corporate Governance & Legal Services
Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e, Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317-5.1.2.e
www.wur.nl/disclaimer

Van: Privacy <privacy@wur.nl>
Verzonden: vrijdag 30 april 2021 14:37
Aan: Privacy <privacy@wur.nl>; 5.1.2.e @wur.nl>
Onderwerp: Nieuwe datalekmelding | 4/30/2021 12:36:59 PM | 5.1.2.e @wur.nl
Urgentie: Hoog

Beste collega,

Zojuist is er een nieuw datalek gemeld via het digitale meldformulier:

* * *

1. Geef een zo gedetailleerd mogelijke omschrijving van het incident
We waren om 10:00 gestart met een pilot van het zaakproces stage/thesis/research practice. De coordinator van een stage/thesis/research practice had inzage in de zaken + onderliggende documenten van de studenten. Daar kwamen we rond 14:00 achter, toen zijn alle zaken op inactief gezet en de zeer gevoelige documenten (daar was er één van, een conficentiele thesis) zijn volledig uit Osiris verwijderd. Door het inactief maken van de zaak zijn de overige documenten ook niet meer te zien voor de thesis/stage/research practice coordinatoren.

2. Wat is de aard van het incident?
In theorie kunnen thesis/research practice/ internship coordinatoen inzage gekregen hebben in contracten en learning agreements (+ voor één, student want er was maar één zaak volledig afgerond ook beoordelingsformulieren en confidentiele thesis) van studenten die niet bij hun leerstoelgroep een stage/thesis/research practice deden.

3. Hoelang heeft het incident geduurd?
Eén dag

4a. Gedurende welke periode heeft het incident plaatsgevonden?

4b. Op welke datum heeft het incident plaatsgevonden?
2021-04-16

5. Van welke categorie personen zijn persoonsgegevens gelekt?
["Studenten"]

6. Van hoeveel personen zijn mogelijk persoonsgegevens gelekt?
25

7. Op welke datum/tijdstip is het incident ontdekt?
4/16/2021

8. Wat voor soort persoonsgegevens zijn betrokken in het incident?
["thesis/internship/research practice learning agreement, contract, verslag, beoordelingsformulier."]

9. Welke acties zijn ondernomen naar aanleiding van het incident?
De functionaliteit is onmiddelijk uitgezet. In de contracten staan o.a. naw gegevens en studentnummer van studenten, maar daar konden thesis/intenship/research practice coordinatoren al bij vanwege de rechten die zij nodig hebben voor hun werk, daarom heb ik dit niet als datalek aangevinkt.

* * *

Met vriendelijke groet,
5.1.2.e

5.1.2.e
Corporate Privacy Officer | 5.1.2.e

Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e, Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317-5.1.2.e

Privacy

Van: Privacy ESA
Verzonden: donderdag 29 april 2021 15:58
Aan: 5.1.2.e
CC: Privacy
Onderwerp: Melding datalek

Urgentie: Hoog

Goedemiddag 5.1.2.e

Vandaag sprak ik met 5.1.2.e Hij gaf aan dat er een issue was met OSIRIS autorisaties, waardoor collega's onbedoeld te veel inzage konden hebben bij gegevens van studenten. Dat zou betekenen dat dit een incident is, waartoe dit gemeld moet worden in het datalekregister. Deze melding moet zo snel mogelijk gedaan worden, omdat het altijd mogelijk is dat we formeel melding moeten doen bij de AP. Dit moet binnen 72 uur na constatering, vandaar de hoge prioriteit. Overigens verwacht ik dat dit – met de informatie van 5.1.2.e en de genomen maatregelen – een beperkt risico is. Hoe sta jij hierin?

Meldingsformulier:
https://forms.office.com/Pages/ResponsePage.aspx?id=5TfRJx92wU2viNJkMKuxj8w45Nmm-ZdEk8XzZ0GPbGRUN043UllTMkwxS1dWOFZVN0RXODUxOFgzNy4u

Met vriendelijke groet,

5.1.2.e
Privacy Officer
Wageningen University & Research
Education & Student Affairs (ESA), Social Sciences Group (SSG),
Environmental Sciences Group (ESG) & Agrotechnology & Food Sciences Group (AFSG)
PO Box 9100, 6700 HA Wageningen
Wageningen Campus, Atlas Building, Droevendaalsesteeg 4, 6708 PB Wageningen
0317 – 5.1.2.e
disclaimer

WUR is serious about Data

DATADANGERS, de WUR-film over het belang van onze data-schatkamer en hoe deze goed te beschermen.
Vragen? Mail, bel of maak een afspraak.

5.1.2.e

Van: Privacy
Verzonden: maandag 18 oktober 2021 13:21
Aan: Privacy; 5.1.2.e
Onderwerp: Nieuwe datalekmelding | 10/18/2021 11:21:22 AM | 5.1.2.e @wur.nl

Urgentie: Hoog

Beste collega,

Zojuist is er een nieuw datalek gemeld via het digitale meldformulier:

* * *

1. Geef een zo gedetailleerd mogelijke omschrijving van het incident
Van het weekend mijn werktelefoon verloren in de Efteling. Er zaten ongeveer 10 minuten tussen het verliezen en het ontdekken (18:45 - 18:55 op 17-10-2021). Ik heb via mijn google account "secure device" onmiddelijk aangezet. De telefoon is inmiddels nog niet terug, de batterij is wel leeg aangezien het nummer niet meer over gaat.

2. Wat is de aard van het incident?
per ongeluk verloren

3. Hoelang heeft het incident geduurd?
Eén dag

4a. Gedurende welke periode heeft het incident plaatsgevonden?

4b. Op welke datum heeft het incident plaatsgevonden?
2021-10-17

5. Van welke categorie personen zijn persoonsgegevens gelekt?
["Medewerkers","Mijn telefoon had toegang tot mijn contacten/werk e-mail en mijn auteniticator app. Echter zat er een 4 cijferige wachtwoord beveiliging op. Ook heb ik heel snel de google secure device aangezet."]

6. Van hoeveel personen zijn mogelijk persoonsgegevens gelekt?
weet ik niet

7. Op welke datum/tijdstip is het incident ontdekt?
18:55

8. Wat voor soort persoonsgegevens zijn betrokken in het incident?
["Mogelijk e-mails, maar kans is denk ik zeer klein."]

9. Welke acties zijn ondernomen naar aanleiding van het incident?
via google secure account aangezet.

* * *

Met vriendelijke groet,
5.1.2.e

5.1.2.e
Corporate Privacy Officer | 5.1.2.e

Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317-5.1.2.e

5.1.2.e

Van: Privacy
Verzonden: maandag 18 oktober 2021 19:15
Aan: 5.1.2.e
Onderwerp: Datalekmelding

Beste 5.1.2.e,

Bedankt voor de datalekmelding die ik vanmiddag van jou ontving. Vervelend dat je je WUR-telefoon bent kwijtgeraakt; ik hoop niet dat het te veel een domper heeft gegeven op de dag. In dit geval is waarschijnlijk geen sprake van een incident waarvoor verdere opvolging nodig is vanuit privacyoogpunt. WUR-telefoons zijn normaal gesproken versleuteld zodat de kans dat iemand toegang krijgt tot de bestanden op de telefoon zonder kennis van username/wachtwoord en WUR passcode is uitgesloten. Het incident is door jouw melding goed geregistreerd en kan daarom wat mij betreft hierbij afgesloten worden.

Voor zover je het verlies nog niet bij de Servicedesk IT hebt gemeld adviseer ik je dat alsnog te doen. De Servicedesk IT kan je helpen bij het remote wipen (waar mogelijk) en bij het aanvragen van een nieuwe WUR-telefoon.

Ik wens je verder succes en sterkte met de afwikkeling van het incident. Mocht je nog vragen hebben dan kun je mij altijd bereiken.

Vriendelijke groet,
5.1.2.e

5.1.2.e
Corporate Privacy Officer | 5.1.2.e
Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e | Droevendaalsesteeg 4
6708 PB Wageningen
Tel. +31 317 5.1.2.e

Privacy

Van: Privacy
Verzonden: donderdag 9 september 2021 21:11
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: Datalekmelding

Beste 5.1.2.e

Bedankt voor je datalekmelding. Ik begreep al dat jij hierover contact hebt gehad met 5.1.2.e. Hoewel formeel sprake is van een 'datalek' (namelijk: onbevoegden hebben inzage gekregen in (zakelijke) persoonsgegevens waartoe zij niet geautoriseerd waren), is gezien de aard van de betrokken gegevens en de acties die jullie hebben genomen, naar onze inschatting geen sprake van een kans op nadelige gevolgen voor de betrokken personen. Daarvan uitgaande hoeven wij dit incident niet te melden bij de toezichthouder.

Jouw melding helpt ons om ons datalekkenregister compleet te houden. Daarom bedankt voor je melding. Mocht je nog willen overleggen dan zijn wij daarvoor graag beschikbaar.

Vriendelijke groet,
5.1.2.e

5.1.2.e
Corporate Privacy Officer | 5.1.2.e
Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e | Droevendaalsesteeg 4
6708 PB Wageningen
Tel. +31 317 5.1.2.e

5.1.2.e

Van: Privacy
Verzonden: donderdag 9 september 2021 14:53
Aan: Privacy; 5.1.2.e
Onderwerp: Nieuwe datalekmelding | 9/9/2021 12:52:59 PM | 5.1.2.e @wur.nl

Urgentie: Hoog

Beste collega,

Zojuist is er een nieuw datalek gemeld via het digitale meldformulier:

* * *

1. Geef een zo gedetailleerd mogelijke omschrijving van het incident
Er was een Teams groep aangemaakt. Deze was abusievelijk op " Openbaar " gezet

2. Wat is de aard van het incident?
De Teamsgroep was zichtbaar voor de gehele WUR organisatie

3. Hoelang heeft het incident geduurd?
Meer dan één dag

4a. Gedurende welke periode heeft het incident plaatsgevonden?
Enkele maanden

4b. Op welke datum heeft het incident plaatsgevonden?

5. Van welke categorie personen zijn persoonsgegevens gelekt?
["Medewerkers"]

6. Van hoeveel personen zijn mogelijk persoonsgegevens gelekt?
24

7. Op welke datum/tijdstip is het incident ontdekt?
21 juli 2021

8. Wat voor soort persoonsgegevens zijn betrokken in het incident?
["Werklocatie gegevens. Gebouw en kamernummer"]

9. Welke acties zijn ondernomen naar aanleiding van het incident?
Groep is op " besloten" gezet

* * *

Met vriendelijke groet,
5.1.2.e

5.1.2.e
Corporate Privacy Officer | 5.1.2.e

Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317-5.1.2.e

5.1.2.e

Van: 5.1.2.e
Verzonden: vrijdag 5 maart 2021 11:37
Aan: 5.1.2.e
Onderwerp: Datalek

Opvolgingsvlag: Opvolgen
Vlagstatus: Voltooid

Hoi 5.1.2.e

Zou jij mij willen terugbellen in verband met een mogelijke datalek?

Het betreft de verkiezingen van PhD-kandidaten voor de GV. Het kiesregister is per abuis verstrekt aan een PhD-kandidaat. De schade lijkt wat minder groot dan we gisteren in eerste instantie dachten.

Groet, 5.1.2.e

5.1.2.e
Beleidsmedewerker Corporate Governance
Wageningen University & Research, Corporate Staff
Postbus 9101, 6700 HB Wageningen
Wageningen Campus, Gebouw 104, Droevendaalsesteeg 4, 6708 PB Wageningen
Tel: 0317 -5.1.2.e
Mobiel: 06 -5.1.2.e
Mail: 5.1.2.e @wur.nl
www.wur.nl
www.disclaimer-nl.wur.nl

5.1.2.e

Van: Privacy
Verzonden: dinsdag 6 april 2021 13:45
Aan: Privacy; 5.1.2.e
Onderwerp: Nieuwe datalekmelding | 4/6/2021 11:44:47 AM | 5.1.2.e @wur.nl

Urgentie: Hoog

Beste collega,

Zojuist is er een nieuw datalek gemeld via het digitale meldformulier:

* * *

1. Geef een zo gedetailleerd mogelijke omschrijving van het incident
Vanuit Teams is een opname gemaakt in Stream. Deze opname is per ongeluk breder beschikbaar gesteld dan de default beperkte zichtbaarheid. Hierin waren de gegevens van twee studenten zichtbaar, waaronder cijferadministratiedeel Osiris. Het filmpje is 7 keer intern bekeken. Extern bekijken (zonder WUR id) is niet mogelijk.

2. Wat is de aard van het incident?
Foutieve autorisatie ten aanzien van gevoelige data (te breed beschikbaar)

3. Hoelang heeft het incident geduurd?
Meer dan één dag

4a. Gedurende welke periode heeft het incident plaatsgevonden?
Minimaal 1 maand. Momenteel onbekend hoe lang dit zo heeft open gestaan.

4b. Op welke datum heeft het incident plaatsgevonden?

5. Van welke categorie personen zijn persoonsgegevens gelekt?
["Studenten"]

6. Van hoeveel personen zijn mogelijk persoonsgegevens gelekt?
2

7. Op welke datum/tijdstip is het incident ontdekt?
9 maart 2021

8. Wat voor soort persoonsgegevens zijn betrokken in het incident?
["NAW-gegevens","Foto's of video's","Geboortedatum/-plaats, geslacht, nationaliteit","Persoonsgebondennummers (BSN, paspoortnummer, studentnummer)","Gender, e-mailcorrespondentie met student (Faqtory), studiegegevens zoals afstudeergegevens, cijfers, titel, studievoortgangsoverzicht"]

9. Welke acties zijn ondernomen naar aanleiding van het incident?
De autorisaties van het filmpje zijn ingetrokken, melding aangemaakt bij IT servicedesk en datalekformulier, melding aan manager met incident en bovendien verzoek tot awareness sessie.

* * *

Met vriendelijke groet,
5.1.2.e

5.1.2.e
Corporate Privacy Officer | 5.1.2.e

Wageningen University & Research

Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e, Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317-5.1.2.e

5.1.2.e

Van: Privacy
Verzonden: dinsdag 2 maart 2021 16:16
Aan: Privacy; 5.1.2.e
Onderwerp: Nieuwe datalekmelding | 3/2/2021 3:15:40 PM 5.1.2.e @wur.nl

Urgentie: Hoog

Beste collega,

Zojuist is er een nieuw datalek gemeld via het digitale meldformulier:

* * *

1. Geef een zo gedetailleerd mogelijke omschrijving van het incident
Een tijd geleden heb ik via het emailadres smaaklessen@wur.nl 75 doorzichtige leskisten bij Manutan besteld. Deze heb ik op factuur besteld. Nu kreeg ik onderstaande een mail: De cyberaanval die de Manutan Group heeft getroffen heeft geleid tot een datalek. Zoals wij je in onze vorige communicatie hebben laten weten, is de Manutan-groep het slachtoffer geworden van een cyberaanval door ransomware*, die heeft geresulteerd in een inbraak in onze IT-systemen. Ondanks de robuustheid van onze bestaande beveiligingsmaatregelen en het reactievermogen van onze teams om verspreiding van de aanval te voorkomen, hebben de onderzoeken van de cybersecurity-experts bevestigd dat de hackers erin geslaagd zijn om bepaalde bedrijfsgegevens te stelen. Hoewel de onderzoeken nog lopende zijn, willen we je zo snel mogelijk informeren zodat je op deze situatie kunt reageren met gepaste waakzaamheid en de nodige beschermingsmaatregelen kunt nemen. Ondanks de uiterst complexe aard van deze aanvallen, hebben onze experts vastgesteld dat de volgende gegevens hierbij zijn betrokken, zonder in dit stadium te kunnen bevestigen dat de lijst compleet is: - Achternaam, voornaam, adres - Functie of rol binnen het bedrijf - Factuurinformatie - IBAN Naar de mening van onze cybersecurity-experts is de kans extreem laag dat deze gegevens al door de aanvallers kunnen zijn misbruikt om fraude te plegen. Niettemin, bewust van de vele kwaadwillende manieren waarop deze gegevens kunnen worden gebruikt, raden wij je aan zeer waakzaam te blijven, in het bijzonder bij het uitvoeren van financiële of boekhoudkundige handelingen waarbij je adres-, bank- of andere gegevens zou moeten wijzigen. Zoals je weet hebben veiligheid in het algemeen en jouw veiligheid in het bijzonder onze hoogste prioriteit. Onze operaties zullen de komende dagen geleidelijk opstarten met versterkte beveiliging en controles aangepast aan de situatie. We staan tot je beschikking voor alle verdere informatie of specifieke vragen die je wellicht hebt. Wij danken je zeer voor je steun en begrip hierin. Gegevens die ik gedeeld heb (factuur- en aflevergegevens) zijn bij Manutan dus bekend. Ik neem aan ook enkele financiele gegevens (zoals het bankrekeningnummer van Wecr? aangezien het via een factuur betaald is).

2. Wat is de aard van het incident?
Nog niet bekend volgens mij

3. Hoelang heeft het incident geduurd?
Eén dag

4a. Gedurende welke periode heeft het incident plaatsgevonden?

4b. Op welke datum heeft het incident plaatsgevonden?
2021-02-21

5. Van welke categorie personen zijn persoonsgegevens gelekt?
["Factuuradres (en bankrekeningnummer?) Wecr"]

6. Van hoeveel personen zijn mogelijk persoonsgegevens gelekt?
2

7. Op welke datum/tijdstip is het incident ontdekt?
Geen idee

8. Wat voor soort persoonsgegevens zijn betrokken in het incident?
["NAW-gegevens","Financiële gegevens (salaris, tarieven)"]

9. Welke acties zijn ondernomen naar aanleiding van het incident?
De informatiesystemen zijn gesloten en ik heb deze mail gekregen.

* * *

Met vriendelijke groet,
5.1.2.e

5.1.2.e
Corporate Privacy Officer | 5.1.2.e

Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e, Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317-5.1.2.e

Privacy

Van: Privacy
Verzonden: dinsdag 9 maart 2021 09:59
Aan: Privacy ESA
Onderwerp: RE: Manutan Cyber Attack: bericht van de Group General Management

Ha[redacted]

Ter info. Ik heb hierover nog even contact gehad met inkoop (wij kregen deze melding ook rechtstreeks van een aantal mensen). Ik heb onderstaand bericht uitgestuurd aan de melders.

* * *

Beste,

Op 2 maart jl. heb jij bij het meldpunt datalekken een melding gemaakt van een datalek. Kort samengevat gaat het over een incident dat bij Manutan B.V., een leverancier van (kantoor)artikelen, heeft plaatsgevonden en waarbij ook persoonsgegevens van WUR gecompromitteerd zijn.

Wij hebben gekeken of in dit geval actie vanuit de kant van WUR vereist is, bijvoorbeeld in de vorm van een nader onderzoek bij Manutan of een melding bij de toezichthouder. In dit geval komen wij tot de conclusie dat dit aanvullende onderzoek niet nodig is.

Tussen WUR en Manutan bestaat geen structurele doorgifte van persoonsgegevens. Iedere doorgifte is gekoppeld aan een concrete bestelling en vindt plaats ten behoeve van de uitlevering van de bestelde artikelen, onder zelfstandige verantwoordelijkheid van Manutan. De persoonsgegevens die worden uitgewisseld betreffen naam, (zakelijke) contactgegevens en zakelijke financiële gegevens. Op basis van deze omstandigheden concluderen wij dat geen sprake is van een meldplichtig incident voor WUR.

Voor de volledigheid is binnen ProQme en via de intranetgroep een melding uitgegaan van het incident en dat extra alertheid geboden is.

Bedankt voor je melding. Mocht je nog vragen hebben over het voorgaande dan kun je altijd contact opnemen.

Vriendelijke groet,
[redacted]

[redacted]
Corporate Privacy Officer | [redacted]

Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | [redacted] Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317[redacted]
www.wur.nl/disclaimer

Van: Privacy ESA <privacy.esa@wur.nl>
Verzonden: woensdag 3 maart 2021 15:52
Aan: Privacy <privacy@wur.nl>
Onderwerp: FW: Manutan Cyber Attack: bericht van de Group General Management

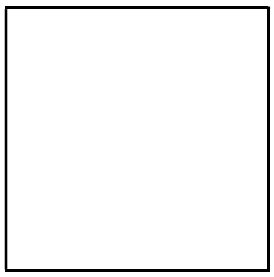
Ter info. Volgens mij hoeven wij hier niets mee te doen.

Van: [redacted] @wur.nl>
Verzonden: dinsdag 2 maart 2021 09:25

Aan: Privacy ESA <privacy.esa@wur.nl>
Onderwerp: FW: Manutan Cyber Attack: bericht van de Group General Management

---

From: Manutan <nl@manutaninternational.emsecure.net>
Sent: 01 March 2021 21:37
To: 5.1.2.e [redacted] @wur.nl>
Subject: Manutan Cyber Attack: bericht van de Group General Management



Online versie | Afmelden

Magazijn & werkplaats | Veiligheid | Gereedschap | Verpakking | Hygiëne | Terrein | Kantoor | Horeca

Beste 5.1.2.e [redacted]

De cyberaanval die de Manutan Group heeft getroffen heeft geleid tot een datalek.
Zoals wij je in onze vorige communicatie hebben laten weten, is de Manutan-groep het slachtoffer geworden van een cyberaanval door ransomware*, die heeft geresulteerd in een inbraak in onze IT-systemen. Ondanks de robuustheid van onze bestaande beveiligingsmaatregelen en het reactievermogen van onze teams om verspreiding van de aanval te voorkomen, hebben de onderzoeken van de cybersecurity-experts bevestigd dat de hackers erin geslaagd zijn om bepaalde bedrijfsgegevens te stelen.
Hoewel de onderzoeken nog lopende zijn, willen we je zo snel mogelijk informeren zodat je op deze situatie kunt reageren met gepaste waakzaamheid en de nodige beschermingsmaatregelen kunt nemen. Ondanks de uiterst complexe aard van deze aanvallen, hebben onze experts vastgesteld dat de volgende gegevens hierbij zijn betrokken, zonder in dit stadium te kunnen bevestigen dat de lijst compleet is:
- Achternaam, voornaam, adres
- Functie of rol binnen het bedrijf
- Factuurinformatie
- IBAN

Naar de mening van onze cybersecurity-experts is de kans extreem laag dat deze gegevens al door de aanvallers kunnen zijn misbruikt om fraude te plegen. Niettemin, bewust van de vele kwaadwillende manieren waarop deze gegevens kunnen worden gebruikt, raden wij je aan zeer waakzaam te blijven, in het bijzonder bij het uitvoeren van financiële of boekhoudkundige handelingen waarbij je adres-, bank- of andere gegevens zou moeten wijzigen. Zoals je weet hebben veiligheid in het algemeen en jouw veiligheid in het bijzonder onze hoogste prioriteit. Onze operaties zullen de komende dagen geleidelijk opstarten met

versterkte beveiliging en controles aangepast aan de situatie.
We staan tot je beschikking voor alle verdere informatie of specifieke vragen die je wellicht hebt. Wij danken je zeer voor je steun en begrip hierin.

Met vriendelijke groeten,

5.1.2.e – Group Chief Executive Officer
5.1.2.e – Group Deputy Chief Executive Officer
5.1.2.e – Group Deputy Chief Executive Officer

Technical contact: cyberinfo@manutan.nl
Commercieel / Sales contact: 030 - 229 61 11 (toets 3)
Media contact: communication@manutan.fr

* Ransomware Ransomware is een type malware dat gegevens versleutelt en vraagt om betaling als losgeld in ruil waarvoor een wachtwoord wordt verstrekt om de gegevens vrij te geven.

Manutan B.V.
Postbus 2, 3734 ZG Den Dolder
Telefoon: 030 - 229 61 11
E-mail: advies@manutan.nl

Volg ons via

Uitstekend

Privacy

Van: Privacy
Verzonden: maandag 8 maart 2021 10:12
Aan: 5.1.2.e
Onderwerp: Terugkoppeling melding datalek

Beste 5.1.2.e,
Op 2 maart jl. heb jij bij het meldpunt datalekken een melding gemaakt van een datalek. Kort samengevat gaat het over een incident dat bij Manutan B.V., een leverancier van (kantoor)artikelen, heeft plaatsgevonden en waarbij ook persoonsgegevens van WUR gecompromitteerd zijn.
Wij hebben gekeken of in dit geval actie vanuit de kant van WUR vereist is, bijvoorbeeld in de vorm van een nader onderzoek bij Manutan of een melding bij de toezichthouder. In dit geval komen wij tot de conclusie dat dit aanvullende onderzoek niet nodig is.
Tussen WUR en Manutan bestaat geen structurele doorgifte van persoonsgegevens. Iedere doorgifte is gekoppeld aan een concrete bestelling en vindt plaats ten behoeve van de uitlevering van de bestelde artikelen, onder zelfstandige (verwerkings)verantwoordelijkheid van Manutan. De persoonsgegevens die worden uitgewisseld betreffen naam, (zakelijke) contactgegevens en zakelijke financiële gegevens.
Op basis van deze omstandigheden concluderen wij dat geen sprake is van een meldplichtig incident voor WUR.
Voor de volledigheid is binnen ProQme en via de intranetgroep een melding uitgegaan van het incident en dat extra alertheid geboden is.
Voor nu bedankt voor je melding. Mocht je nog vragen hebben over het voorgaande dan kun je altijd contact opnemen.
Vriendelijke groet,

5.1.2.e
5.1.2.e
Corporate Privacy Officer | 5.1.2.e
Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) 5.1.2.e | Droevendaalsesteeg 4
6708 PB Wageningen
Tel. +31 317 5.1.2.e

5.1.2.e

Van: Privacy
Verzonden: dinsdag 2 maart 2021 11:02
Aan: Privacy; 5.1.2.e
Onderwerp: Nieuwe datalekmelding | 3/2/2021 10:01:26 AM 5.1.2.e @wur.nl

Urgentie: Hoog

Beste collega,

Zojuist is er een nieuw datalek gemeld via het digitale meldformulier:

* * *

1. Geef een zo gedetailleerd mogelijke omschrijving van het incident
De afdeling inkoop heeft een melding gekregen van toeleveringsbedrijf Manutan dat zij getroffen zijn door een ransomware aanval op 21 februari 2021. Hier zijn ook gegevens van WUR-bestellers mee gemoeid. Hun experts hebben vastgesteld dat de volgende gegevens hierbij zijn betrokken, zonder in dit stadium te kunnen bevestigen dat de lijst compleet is: - Achternaam, voornaam, adres - Functie of rol binnen het bedrijf - Factuurinformatie - IBAN Het incident loopt nog en de gevolgen zijn dat hun gegevens in handen van derden zijn gekomen.

2. Wat is de aard van het incident?
Ransomware attack

3. Hoelang heeft het incident geduurd?
Meer dan één dag

4a. Gedurende welke periode heeft het incident plaatsgevonden?
21 februari 2021

4b. Op welke datum heeft het incident plaatsgevonden?

5. Van welke categorie personen zijn persoonsgegevens gelekt?
["Medewerkers"]

6. Van hoeveel personen zijn mogelijk persoonsgegevens gelekt?
Bestellers bij Manutan

7. Op welke datum/tijdstip is het incident ontdekt?
21 feb 2021

8. Wat voor soort persoonsgegevens zijn betrokken in het incident?
["NAW-gegevens","bestellingen die gedaan zijn"]

9. Welke acties zijn ondernomen naar aanleiding van het incident?
Dit loopt nog. Zie www.manutan.nl en contactadres: cyberinfo@manutan.nl. Melding uit afdeling Inkoop via 5.1.2.e

* * *

Met vriendelijke groet,
5.1.2.e

5.1.2.e
Corporate Privacy Officer 5.1.2.e

Wageningen University & Research
Postbus 9101, 6700 HB Wageningen

B:104 (Atlas) | 5.1.2.e Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317 5.1.2.e

5.1.2.e

Van: Privacy
Verzonden: donderdag 5 augustus 2021 16:08
Aan: Privacy; 5.1.2.e
Onderwerp: Nieuwe datalekmelding | 8/5/2021 2:07:41 PM | 5.1.2.e @wur.nl

Urgentie: Hoog

Beste collega,

Zojuist is er een nieuw datalek gemeld via het digitale meldformulier:

* * *

1. Geef een zo gedetailleerd mogelijke omschrijving van het incident
Vanuit de mailbox Office Biologie heb ik gereageerd op een mail van een student. De student schrijft dat hij door corona minder motivatie had om te studeren, de motivatie nu weer gevonden heeft, maar bang is dat hij de herkansingen niet haalt en daardoor zijn BSA niet haalt. Ik heb daarop gereageerd met een bericht dat als het door bijzondere omstandigheden komt, hij het beste even contact op kan nemen met de decaan. Nadat ik de mail verstuurd had, kwamen er een aantal mailtjes binnen van andere personen, dat dit bericht niet voor hen is bedoelt en of het wel goed is gegaan. Ik heb de mail geopend en zag tot mijn schrik dat er meer dan 100 emailadressen in de BCC waren opgenomen. Ik heb direct IT gebeld om de mail terug te vragen, maar helaas hebben een aantal mensen de mail wel gezien. Ik heb de mensen uit de BCC een mail gestuurd met mijn excuses en of ze de mail direct willen verwijderen. Ik heb de emailadressen even nagekeken, en kwam erachter dat het gaat om oud biologie studenten die al meer dan 5 jaar zijn afgestudeerd. Ik weet 100% zeker dat ik hen niet heb toegevoegd in de BCC. Ik heb IT hierover ook gemaild, hoe dit mogelijk is.

2. Wat is de aard van het incident?
Datalek. Mensen hebben een mail ingezien die niet voor hen bedoelt was.

3. Hoelang heeft het incident geduurd?
Eén dag

4a. Gedurende welke periode heeft het incident plaatsgevonden?

4b. Op welke datum heeft het incident plaatsgevonden?
2021-08-05

5. Van welke categorie personen zijn persoonsgegevens gelekt?
["Studenten"]

6. Van hoeveel personen zijn mogelijk persoonsgegevens gelekt?
1

7. Op welke datum/tijdstip is het incident ontdekt?
5 augustus 2021 10:28

8. Wat voor soort persoonsgegevens zijn betrokken in het incident?
["naam, emailadres en bericht student"]

9. Welke acties zijn ondernomen naar aanleiding van het incident?
Ik heb IT direct gebeld of zij de mail konden terug halen en heb alle mensen in de BCC een bericht gestuurd met het dringende verzoek om de eerder gezonden mail te verwijderen. Daarna heb ik een mail gestuurd naar IT met de vraag hoe dit heeft kunnen gebeuren en heb ik contact opgenomen met 5.1.2.e

* * *

Met vriendelijke groet,
5.1.2.e

5.1.2.e
Corporate Privacy Officer | 5.1.2.e

Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e, Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317 5.1.2.e

Privacy

Van: Functionarisgegevensbescherming
Verzonden: vrijdag 2 juli 2021 17:14
Aan: 5.1.2.e
CC: Privacy; 5.1.2.e
Onderwerp: FW: Datalek / securityincident SURFsharekit
Bijlagen: Incident SURFsharekit.pdf; Untitled attachment 00009.htm

Beste 5.1.2.e

Gisteravond ontving ik onderstaande mail met bijlage van de Functionaris voor gegevensbescherming van SURF. Het blijkt dat de SURFsharekit vanaf januari 2021 tot 1 juli heeft open gestaan. Ik begrijp dat deze applicatie voornamelijk gebruikt wordt voor afstudeerpublicaties, afstudeerwerk en leermaterialen. Zojuist met 5.1.2.e gebeld en die gaf aan dat het vooral ten behoeve van Groen Kennisnet gebruikt wordt. Ik acht de kans klein dat er persoonsgegevens in staan opgenomen. Graag zie ik dat dit maandag gecontroleerd wordt door de bibliotheek.

Omdat de verwachting is dat er nauwelijks persoonsgegevens in zullen zijn opgenomen gaat WU vooralsnog niet melden bij de Autoriteit Persoonsgegevens. Wel zullen we intern het datalek registreren.

Mocht maandag uit het onderzoek blijken dat de veronderstelling ten aanzien van de persoonsgegevens anders is, dan zal ik opnieuw een afweging maken om dit datalek te melden bij de AP.

Graag maandag even contact.

Met vriendelijke groet,

5.1.2.e

WAGENINGEN
UNIVERSITY & RESEARCH

5.1.2.e | Functionaris Gegevensbescherming | Wageningen University & Research | Postbus 9101, 6700 HB Wageningen | +31 (0)317 5.1.2.e | www.wur.nl

---

From: 5.1.2.e @surf.nl>
Sent: Thursday, July 01, 2021 7:16 PM
To: 5.1.2.e @wur.nl>
Subject: Datalek / securityincident SURFsharekit

Beste 5.1.2.e ,

SURF heeft een datalek geconstateerd in SURFSharekit, een dienst waarvan uw instelling gebruik maakt. Bij gebruik van deze dienst is SURF verwerker in de zin van de AVG, uw instelling is verwerkingsverantwoordelijke. Ik informeer u hierbij over het incident, zodat u kunt bepalen of melding aan betrokkenen en/of AP nodig is, en of nog andere stappen genomen moeten worden.

Wat is SURFsharekit
SURFsharekit is de online opslagplaats voor het hoger onderwijs. Onderzoekspublicaties, afstudeerproducten en open leermaterialen kunnen worden opgeslagen en via verschillende platformen digitaal toegankelijk gemaakt worden.

Nadere toelichting
Op 1 juli is geconstateerd dat het in sommige gevallen mogelijk is om ongeoorloofde toegang te krijgen tot gegevens (waaronder persoonsgegevens en auteursrechtelijk beschermd materiaal) binnen de dienst SURFsharekit. Een functionaliteit waarmee materiaal gedeeld kan worden met personen binnen de eigen instelling, schermde toegang voor andere gebruikers van SURFsharekit (buiten de eigen onderwijsinstelling) niet af. Daardoor is het mogelijk dat SURFsharekit gebruikers buiten jullie instelling toegang gehad hebben tot stukken die alleen bedoeld waren voor publicatie binnen de instelling.

Helaas kan niet worden vastgesteld of en in welke mate er misbruik is gemaakt van dit beveiligingslek. Dit beveiligingslek is ontstaan op 3 januari 2021 en tot vandaag onontdekt gebleven. Het probleem in de software is inmiddels opgelost.

In de bijlage een beschrijving van het incident in iets meer detail. Neem voor vragen gerust contact met mij op.

Hartelijke groet,

SURF

5.1.2.e
Functionaris Gegevensbescherming
06 - 5.1.2.e

Datalek / beveiligingsincident SURFsharekit

Vandaag is geconstateerd dat gebruikers van SURFsharekit ongeoorloofd toegang hebben kunnen hebben tot bepaalde bestanden. Via deze weg informeren wij jullie over wat er gebeurd is.

Wat is SURFsharekit
SURFsharekit wordt voor het overgrote deel gebruikt om onderzoekspublicaties, afstudeerwerk en leermaterialen open beschikbaar te maken. Het is echter ook mogelijk om materialen voor een specifieke groep beschikbaar te maken, bijvoorbeeld voor medewerkers en studenten van 1 hogeschool.

Wat is er gebeurd?
In de ochtend van 1 juli heeft SURF bericht ontvangen van een hogeschool dat het voor een gebruiker van een andere hogeschool mogelijk was om materialen in te zien. Na onderzoek blijkt dat bij het benaderen van een bestand via een directe link, het systeem alleen controleert of je toegang hebt tot SURFsharekit, maar niet of je toegang mag hebben tot dit specifieke materiaal. Dit is vanaf 3 januari 2021 het geval. Directe links kunnen op een aantal manieren worden verkregen.

- Via OAI/SRU/JSON-API koppeling met 'niet publieke' kanalen.
- Kopiëren van de link uit SURFsharekit.

Wie konden bestanden inzien?
Bestanden zijn niet publiek toegankelijk geweest. Wel was het mogelijk dat medewerkers en studenten van andere instellingen die SURFsharekit afnemen, materialen hebben kunnen inzien die alleen bedoeld waren voor publicatie binnen jullie eigen instelling. 30 hogescholen en universiteiten maken gebruik van SURFsharekit.

Hoe groot is de impact?
Er wordt niet veel gebruik gemaakt van de mogelijkheid om semi-open materiaal te delen. Voor de onderwijsinstellingen die deze optie gebruiken, is er een beperkt risico dat er ongeoorloofde toegang heeft plaatsgevonden. Als er binnen de instelling gebruik wordt gemaakt van deze functionaliteit, dan vragen wij je om zo snel mogelijk contact met ons op te nemen via fg@surf.nl. Graag adviseren wij je dan over het vervolg.
De software is inmiddels aangepast, waardoor dit beveiligingslek is gedicht.

AVG
Voor de dienst SURFsharekit is SURF verwerker in de zin van de AVG. De onderwijsinstelling is de verwerkingsverantwoordelijke. Dit betekent dat de onderwijsinstellingen zelf moeten beoordelen of hier sprake is van een datalek en of dit incident gemeld moet worden aan de Autoriteit Persoonsgegevens en/of betrokkenen.

SURF zal de beveiliging van de dienst SURFsharekit in de komende periode verder onder de loep nemen.

Voor vragen over dit incident aan SURF kun je terecht bij fg@surf.nl.

Privacy

Van: Functionarisgegevensbescherming
Verzonden: maandag 5 juli 2021 18:12
Aan: 5.1.2.e
CC: Privacy
Onderwerp: RE: Datalek / securityincident SURFsharekit

Hallo 5.1.2.e en 5.1.2.e

Veel dank voor het naar boven halen van de informatie.

We kunnen nu wel met 100% zekerheid concluderen dat er geen sprake is van een datalek bij WUR op basis van het tijdelijk opengestaan hebben van de applicatie SURFsharekit bij SURF.

Met vriendelijke groet,

5.1.2.e

WAGENINGEN
UNIVERSITY & RESEARCH

5.1.2.e Functionaris Gegevensbescherming | Wageningen University & Research | Postbus 9101, 6700 HB Wageningen | +31 (0)317 5.1.2.e www.wur.nl

---

From: 5.1.2.e @wur.nl>
Sent: Monday, July 05, 2021 10:29 AM
To: 5.1.2.e @wur.nl>; Functionarisgegevensbescherming <functionarisgegevensbescherming@wur.nl>
Cc: Privacy <privacy@wur.nl>
Subject: RE: Datalek / securityincident SURFsharekit

Hoi 5.1.2.e

Mede op basis van de onderstaande info van 5.1.2.e denk ik niet dat het datalek bij SURF Sharekit de WUR raakt. Sowieso zullen er geen persoonsgegevens in betrokken zijn anders dan de naam van de invoerders.

Groet, 5.1.2.e

Van: 5.1.2.e @wur.nl>
Verzonden: maandag 5 juli 2021 10:05
Aan: Functionarisgegevensbescherming <functionarisgegevensbescherming@wur.nl>
CC: Privacy <privacy@wur.nl>; 5.1.2.e @wur.nl>
Onderwerp: RE: Datalek / securityincident SURFsharekit

Op de vraag die ik hieronder nog benoemde heb ik het volgende antwoord gekregen:
*"Binnen het project zijn de e-modules ingevoerd in SURF Sharekit in de community IL (door een uitzendkracht). Deze heb ik inmiddels weer **niet-gepubliceerd** gemaakt omdat het de oude emodules betreft en* 5.1.2.e *ze eerst wilt metadateren in L4L."*

From: 5.1.2.e
Sent: maandag 5 juli 2021 7:38
To: Functionarisgegevensbescherming <functionarisgegevensbescherming@wur.nl>
Cc: Privacy <privacy@wur.nl>; 5.1.2.e @wur.nl>
Subject: RE: Datalek / securityincident SURFsharekit

Hallo 5.1.2.e

SURF sharekit is niet voor Groen Kennisnet gebruikt of in gebruik.
SURF sharekit is de repository voor leermiddelen van SURF en is door de Library in 2019 gebruikt in een pilot voor het invoeren van leermaterialen (ihkv Library for Learning, L4L).
Het kan zijn dat SURF sharekit nog gebruikt wordt door Library – Education support voor invoer van leermaterialen ihkv de community Information Literacy. Ik denk het niet, maar dat zou ik moeten navragen.

5.1.2.e kan je me helpen of dat er dan sprake is van opname van persoonsgegevens?
Een enkel persoon heeft in die pilot rechten gekregen om materiaal in te voeren. De ingevoerde data zijn 'digitale' bibliotheekkaartjes, behalve de invoerder geen persoonsgegevens denk ik.

Vrgr 5.1.2.e

Reeds beoordeeld

Privacy

Van: 5.1.2.e
Verzonden: dinsdag 4 mei 2021 10:03
Aan: Privacy AFSG; Privacy
Onderwerp: RE: URGENT Datalek thesis platform Food Sciences

Opvolgingsvlag: Opvolgen
Vlagstatus: Voltooid

Categorieën: 5.1.2.e

Hoi 5.1.2.e

We zijn aan het nazoeken welke soort acties überhaupt gelogd worden, om te bepalen of er meer kan zijn gebeurd op de site dan deze logging vermeldt. Maar hoe het ook zij: dit is de enige logging die we hebben dus nabellen gaat sowieso niet meer opleveren dan ik nu verstuurd heb.

Zodra ik meer weet over de criteria waarmee gelogd wordt horen jullie dat uiteraard van me.

Met vriendelijke groet,

5.1.2.e
Product Owner Datamanagement & Hosting Services en UCC

Wageningen University & Research
Facilitair Bedrijf, afdeling Informatie Technologie
Postbus 59, 6700 AB, Wageningen
Gebouw 116, Akkermaalsbos 12, 6708 WB, Wageningen
Aub geen papieren post sturen / Please do not send postal mail
Tel. 0317 5.1.2.e
[redacted]@wur.nl
www.wur.nl
http://www.wur.nl/nl/Disclaimer.htm

From: Privacy AFSG <privacy.afsg@wur.nl>
Sent: dinsdag 4 mei 2021 09:59
To: 5.1.2.e @wur.nl>; Privacy <privacy@wur.nl>
Subject: URGENT Datalek thesis platform Food Sciences
Importance: High

Hallo 5.1.2.e

Bedankt voor de snelle actie, fijn dat hier ook namen bij staan. Ik kan niet beoordelen of dit voldoende is (dat is aan 5.1.2.e om dit te beoordelen), maar het lijkt mij al heel specifiek.
Ik zie alleen de namen van 5.1.2.e en 5.1.2.e terwijl volgens mij de melder van het datalek (student met WUR-account) ook toegang heeft gehad die dag.

5.1.2.e is de eigenaar van de sharepoint en 5.1.2.e doet (samen met 5.1.2.e) het thesis platform Food Sciences.
Vanuit het overzicht lijkt het erop dat er geen andere interacties zijn geweest, maar ik vraag me dus af of dit klopt. Moet ik hier nog even achteraan bellen?

Met vriendelijke groet, 5.1.2.e

****
5.1.2.e **CIPP/E**
Privacy Officer Agrotechnology & Food Sciences Group (AFSG)
Wageningen University & Research
Tel. 0317-5.1.2.e , schakelt door naar mobiel
privacy.afsg@wur.nl

DATADANGERS, bekijk de WUR-film over het belang van onze data-schatkamer en hoe deze goed te beschermen.
Vragen? Mail, bel of maak een afspraak.

Meer privacy informatie vind je hier

Van: 5.1.2.e @wur.nl>
Verzonden: maandag 3 mei 2021 16:12
Aan: Privacy AFSG <privacy.afsg@wur.nl>; Privacy <privacy@wur.nl>
Onderwerp: RE: Datalek thesis platform Food Sciences

Hoi 5.1.2.e en 5.1.2.e

Bijgevoegd de audit log voor deze site van heel 21-04-2021. Hebben jullie hier voldoende aan?

Met vriendelijke groet,

5.1.2.e
Product Owner Datamanagement & Hosting Services en UCC

Wageningen University & Research
Facilitair Bedrijf, afdeling Informatie Technologie
Postbus 59, 6700 AB, Wageningen
Gebouw 116, Akkermaalsbos 12, 6708 WB, Wageningen
Aub geen papieren post sturen / Please do not send postal mail
Tel. 0317 5.1.2.e
5.1.2.e @wur.nl
www.wur.nl
http://www.wur.nl/nl/Disclaimer.htm

From: 5.1.2.e
Sent: maandag 3 mei 2021 14:40
To: Privacy AFSG <privacy.afsg@wur.nl>; Privacy <privacy@wur.nl>
Subject: RE: Datalek thesis platform Food Sciences

Hoi 5.1.2.e en 5.1.2.e

Ik heb 1 van mijn sharepointbeheerders gevraagd om uit te zoeken wat wij hierover kunnen vinden. Mocht het niet lukken om dit vandaag op te leveren, dan laat ik dat (inclusief verwachting wanneer dan wel) uiteraard weten.

Met vriendelijke groet,

5.1.2.e
Product Owner Datamanagement & Hosting Services en UCC

Wageningen University & Research
Facilitair Bedrijf, afdeling Informatie Technologie
Postbus 59, 6700 AB, Wageningen
Gebouw 116, Akkermaalsbos 12, 6708 WB, Wageningen
Aub geen papieren post sturen / Please do not send postal mail
Tel. 0317 5.1.2.e
5.1.2.e @wur.nl
www.wur.nl
http://www.wur.nl/nl/Disclaimer.htm

From: Privacy AFSG <privacy.afsg@wur.nl>
Sent: maandag 3 mei 2021 14:27
To: Privacy <privacy@wur.nl>; 5.1.2.e @wur.nl>
Subject: Datalek thesis platform Food Sciences
Importance: High

Hallo 5.1.2.e

Ik ben met 5.1.2.e (productmanager Office 365) bezig om te kijken of hij de logging details van het datalek boven water kan krijgen. Ik weet niet hoe ik de chat van Teams kan exporteren naar de mail, maar heb deze hieronder gekopieerd ter informatie.

5.1.2.e : ik ben tot uiterlijk 15 uur beschikbaar, zou je kunnen reageren naar alle betrokkenen in deze mail? 5.1.2.e is de Functionaris Gegevensbescherming van WUR en hij heeft die gegevens nodig om het risico van het datalek te kunnen beoordelen.

Met vriendelijke groet, 5.1.2.e

****
5.1.2.e **, CIPP/E** | Privacy Officer 5.1.2.e

T: 0317 5.1.2.e
E-mail 5.1.2.e @wur.nl ***Ik ben niet aanwezig: woensdag NM en vrijdag***
E-mail privacy: privacy.afsg@wur.nl

Input nodig m.b.t. privacy binnen WUR? Klik hier voor meer informatie en templates

5.1.2.e

- **Chat**
- Files
- Organization
- Activity

13:57
Hallo 5.1.2.e, ik ben privacy officer voor AFSG en ben ivm een datalek op een thesis platform van Food Sciences op zoek naar logging-details in de timeframe van dat datalek. Ik hoorde dat jij de productmanager bent van Office 365, weet jij bij wie ik die details op kan vragen?

5.1.2.e
14:01
Wat voor details zoek je dan precies? Want 'thesis platform van Food Sciences' zegt mij zo gauw nog niks
Is dat de naam van een website, applicatie of teamsite of iets dergelijks?

Overigens ben ik nu ook weer voor videocalls bereikbaar, ben net uit overleg

14:14
Hallo 5.1.2.e, het gaat om details als daadwerkelijk gebruikte toegang tot de sharepoint tijdens dit datalek (binnen en buiten WUR) en wat er eventueel gedaan is. Ik ben een leek op IT-gebied en weet niet welke informatie je allemaal precies naar boven kunt halen, maar het liefst zo specifiek en volledig mogelijk. Wat zijn de mogelijkheden?

5.1.2.e
14:14
Daarvoor moet ik weten om welke URL het gaat

14:15
Ik weet nu dat 5.1.2.e de eigenaar is van de sharepoint waarop dit thesis platform 2x per jaar aangeboden wordt. Als ik bij hem moet zijn, dan hoor ik dat graag. De link
is https://wageningenur4.sharepoint.com/sites/FT_ThesisTopics/SitePages/Home.aspx
De datum waarop dit datalek was is 21 april. Om 11 uur is de site aangepast en rond 13.30 uur was het probleem opgelost. Heb je hiermee voldoende informatie v.w.b. de timeframe?

5.1.2.e

Van: Privacy
Verzonden: vrijdag 8 oktober 2021 09:17
Aan: Privacy;5.1.2.e
Onderwerp: Nieuwe datalekmelding | 10/8/2021 7:16:39 AM 5.1.2.e @wur.nl

Urgentie: Hoog

Beste collega,

Zojuist is er een nieuw datalek gemeld via het digitale meldformulier:

* * *

1. Geef een zo gedetailleerd mogelijke omschrijving van het incident
Op de UBW productie-servers en acceptatieservers (5.1.2.h en 5.1.2.h) stonden een aantal shares open met gegevens die mogelijk privacy gevoelig zijn. De gegevens die meest kwalijk zijn, zijn de bijlagen bij MXP declaraties (dus alleen buitenlandse reisdeclaraties) en een aantal bankafschriften. Er kunnen individuele betalingen aan personeel tussen zitten, maar de betalingen aan personeel lopen voor 99% via HRM.

2. Wat is de aard van het incident?
Iedereen op het WUR netwerk had toegang tot de shares mits het pad naar de share bij hen bekend zou zijn

3. Hoelang heeft het incident geduurd?
Meer dan één dag

4a. Gedurende welke periode heeft het incident plaatsgevonden?
Vanaf installatie UBW

4b. Op welke datum heeft het incident plaatsgevonden?

5. Van welke categorie personen zijn persoonsgegevens gelekt?
["Medewerkers"]

6. Van hoeveel personen zijn mogelijk persoonsgegevens gelekt?
0, maar niet bekend, geen signalen dat onbevoegden de shares benaderd hebben.

7. Op welke datum/tijdstip is het incident ontdekt?
7 oktober 2021

8. Wat voor soort persoonsgegevens zijn betrokken in het incident?
["Declaraties"]

9. Welke acties zijn ondernomen naar aanleiding van het incident?
Shares zijn dicht gezet (beveiligd)

* * *

Met vriendelijke groet,
5.1.2.e

5.1.2.e
Corporate Privacy Officer | 5.1.2.e

Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) 5.1.2.e Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317 5.1.2.e

5.1.2.e

Van: 5.1.2.e
Verzonden: vrijdag 8 oktober 2021 09:24
Aan: 5.1.2.e
Onderwerp: RE: Openstaande shares UBW

Bedankt, 5.1.2.e Ik heb hem ontvangen.

Groet, 5.1.2.e

5.1.2.e
5.1.2.e Corporate Governance & Legal Services

Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317 5.1.2.e
www.wur.nl/disclaimer

Van: 5.1.2.e @wur.nl>
Verzonden: vrijdag 8 oktober 2021 09:18
Aan: 5.1.2.e @wur.nl>
Onderwerp: RE: Openstaande shares UBW

Ok 5.1.2.e
helder, ik heb de melding aangemaakt
groet, 5.1.2.e

Van: 5.1.2.e @wur.nl>
Verzonden: vrijdag 8 oktober 2021 09:01
Aan: 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
CC: 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
Onderwerp: RE: Openstaande shares UBW

Ha 5.1.2.e

Bedankt voor het navragen. Formeel was een tijdje sprake van een datalek omdat onbevoegden mogelijk inzage hebben gehad in persoonsgegevens (nl. de individuele (reis)declaraties/betalingen) die niet voor hen beschikbaar zouden moeten zijn. In dat licht zou het zeer gewaardeerd worden als je het formulier wilt (laten) invullen; dat kost meestal ergens tussen 5-10 min. Omdat de shares nu dicht staan is dit vooral een formaliteit; dit helpt om het datalekkenregister compleet te houden (onderdeel van onze complianceplicht / 33 lid 5 AVG). Gezien de kleine kans op nadelige gevolgen voor individuen is de afwikkeling na de interne melding klaar.

Als je hierover nog vragen zorgen hebt, kun je me altijd even een berichtje sturen of bellen.

Groet, 5.1.2.e

5.1.2.e
5.1.2.e Corporate Governance & Legal Services

Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317-5.1.2.e
www.wur.nl/disclaimer

Van: 5.1.2.e @wur.nl>
Verzonden: vrijdag 8 oktober 2021 08:41
Aan: 5.1.2.e wur.nl>; 5.1.2.e @wur.nl>
CC: 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>; 5.1.2.e wur.nl>; 5.1.2.e @wur.nl>
Onderwerp: RE: Openstaande shares UBW

Hoi 5.1.2.e en 5.1.2.e

Shares staan nu dicht. Volgens 5.1.2.e stonden er de volgende gegevens op die mogelijk privacy gevoelig zijn:

> De gegevens die meest kwalijk zijn, zijn de bijlagen bij MXP declaraties (dus alleen buitenlandse reisdeclaraties) en een aantal bankafschriften.
> Betalingen aan personeel loopt 99% via HRM maar er kunnen individuele betalingen aan personeel tussen zitten.

Is het nodig dat hiervoor alsnog een privacy melding wordt aangemaakt?
Hoor graag van jullie

Groeten, 5.1.2.e

Van: 5.1.2.e @wur.nl>
Verzonden: donderdag 7 oktober 2021 16:26
Aan: 5.1.2.e @wur.nl>; 5.1.2.e wur.nl>; 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
CC: 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
Onderwerp: RE: Openstaande shares UBW

Hoi,

Dank allemaal voor het aanbod om te helpen maar ik ben helemaal niet blij met de gang van zaken. Dat komt allemaal nog wel een keertje misschien.

We hebben de rechten aangepast en verwachten dat het hiermee is opgelost. Er is een kans dat een enkele gebruiker tegen problemen aan gaat lopen maar dat kunnen we relatief snel oplossen.
We hebben een communicatie gedaan op de teamsite van F&C voor het geval er toch problemen ontstaan.

Groeten,
5.1.2.e en 5.1.2.e

Van: 5.1.2.e @wur.nl>
Verzonden: 07 October 2021 16:00
Aan: 5.1.2.e wur.nl>; 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
CC: 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
Onderwerp: RE: Openstaande shares UBW

Hoi 5.1.2.e en 5.1.2.e ,

Bedankt voor jullie aanbod, maar is vooralsnog niet nodig.
5.1.2.e en 5.1.2.e hebben er nu contact over en koppelen straks terug.
Paniek is niet nodig.

5.1.2.e heb ik begin van de middag gesproken en ze begrijpt dat we het eerst willen uitzoeken.
5.1.2.e en 5.1.2.e sprak ik toevallig in een ander overleg en heb ze toen ook gelijk hiervan op de hoogte gesteld.

Groet, 5.1.2.e

Van: 5.1.2.e @wur.nl>
Verzonden: donderdag 7 oktober 2021 14:18
Aan: 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
CC: mdt_it_security_services <mdt_it_security_services@wur.nl>; 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
Onderwerp: RE: Openstaande shares UBW

Hoi 5.1.2.e

Ik wil ook helpen indien gewenst.

Gr 5.1.2.e

From: 5.1.2.e
Sent: Thursday, 7 October 2021 14:13
To: 5.1.2.e
Cc: mdt_it_security_services; 5.1.2.e
Subject: RE: Openstaande shares UBW

Hoi 5.1.2.e

Bedankt voor je reactie, de share staat inderdaad open voor alle wuraccounts. Ik had ook een iets ruimere termijn voorgesteld, maar 5.1.2.e heeft overleg gehad met legal en zij vinden het dermate kritisch dat er meer haast achter zou moeten zitten. Als ik kan helpen geef maar een gil.

Groet,

5.1.2.e

From: 5.1.2.e @wur.nl>
Sent: Thursday, 7 October 2021 12:01
To: 5.1.2.e @wur.nl>
Cc: mdt_it_security_services <mdt_it_security_services@wur.nl>; 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
Subject: RE: Openstaande shares UBW

Hoi 5.1.2.e ,

Dat shares met dergelijk gevoelige gegevens open staan zou inderdaad niet mogen.
Kan iedereen bij de WUR daar echt bij? Zo ja dan moeten we zeker direct actie ondernemen (en hiermee niet wachten op de security audit).

Helaas is 5.1.2.e vandaag vanwege privé omstandigheden niet aanwezig en ik kan de gevolgen van het dichtzetten niet overzien.
Laten we het niet zomaar dichtzetten maar dat in goed overleg oppakken. 5.1.2.e en 5.1.2.e heb ik daarom meegenomen in de cc.

Groet, 5.1.2.e

Van: 5.1.2.e @wur.nl>
Verzonden: donderdag 7 oktober 2021 10:56
Aan: 5.1.2.e @wur.nl>
CC: mdt_it_security_services <mdt_it_security_services@wur.nl>; 5.1.2.e @wur.nl>
Onderwerp: Openstaande shares UBW
Urgentie: Hoog

Hallo 5.1.2.e

Gezien onze goede sessie van gister vind ik dit lastig, maar we krijgen weinig gehoor op deze meldingen en maken ons serieus zorgen over de impact en nog meer hoe we dit soort zaken goed op jullie netvlies krijgen.

Op de UBW productie-servers en acceptatieservers (5.1.2.h en 5.1.2.h) staan een aantal shares open voor de gehele WUR met gevoelige informatie: declaraties van medewerkers, betalingen van de WUR (grote aantallen), een groot aantal rapportages met veel financiële data, logfiles waarin queries en andere zaken staan en nog meer gevoelige zaken. We hebben het open staan van deze share in juli gemeld en daarna geresumeerd:

- 23-07 Gemeld bij team
- 29-07 5.1.2.e verzoekt het team de shares dicht te zetten
- 03-08 herinnerd (5.1.2.e heeft het doorgegeven)
- 21-09 herinnerd (geen reactie)

Gisteren heeft 5.1.2.e contact gehad met 5.1.2.e geeft aan dat het inderdaad niet goed is dat de share open staat maar dat hij het lastig vindt om de zaken dicht te zetten omdat daarvan de impact moeilijk te overzien is. Dit begrijpen we, maar dit kan zo niet blijven bestaan, als deze data bij de Telegraaf of andere partijen terecht komt hebben we ook impact als WUR.

Noodzakelijke acties:

1. De shares moeten binnen 3 dagen worden dichtgezet conform de WUR vulnerability handling standard. Gezien het weekend, laten we de maandag einde van de dag als deadline pakken. Als de shares dan niet dichtgezet zijn zullen we deze melding moeten escaleren. Kunnen jullie aangeven hoe deze is dichtgezet?
2. Gezien de data die we tegenkomen (namen met IBAN-nummers erbij, reisgegevens van personen met bestemmingen, PCR-test declaraties met naam en toenaam, bijlagen van declaraties met namen/adressen) zal waarschijnlijk ook een melding lek persoonsgegevens opgestart moeten worden. Vandaar CC naar 5.1.2.e , onze local privacy officer, zij begeleidt deze processen.

Het is niet mijn favoriete optie om het op deze manier aan te pakken (en ook onze eerste keer dat we het zo aanpakken), maar ik zie geen andere optie op dit moment.

Groet,

5.1.2.e

Privacy

Van: Functionarisgegevensbescherming
Verzonden: dinsdag 25 mei 2021 17:38
Aan: Privacy
CC: 5.1.2.e
Onderwerp: RE: Nieuwe datalekmelding | 5/25/2021 12:19:28 PM | 5.1.2.e @wur.nl

Hallo 5.1.2.e,

Zoals we telefonisch reeds afgesproken hebben is melding van dit datalek bij de AP zonder meer aan de orde.

Wie de melding aan betrokkenen moet doen moeten we nog maar even bespreken. Dit zal dienen te worden voorbereid door de situationeel eigenaar i.a.m. communicatie, lijkt mij.

Goed om in voorgaande context ook Hubert ook aan te haken!

Met vriendelijke groet,

5.1.2.e

WAGENINGEN
UNIVERSITY & RESEARCH

5.1.2.e | Functionaris Gegevensbescherming | Wageningen University & Research | Postbus 9101, 6700 HB Wageningen | +31 (0)317 5.1.2.e | www.wur.nl

---

From: Privacy <privacy@wur.nl>
Sent: Tuesday, May 25, 2021 4:48 PM
To: 5.1.2.e @wur.nl>
Cc: 5.1.2.e @wur.nl>
Subject: FW: Nieuwe datalekmelding | 5/25/2021 12:19:28 PM | 5.1.2.e @wur.nl
Importance: High

Ha 5.1.2.e,

Ik heb inmiddels contact gehad met 5.1.2.e en met 5.1.2.e van de Servicedesk IT (ticket 637836.00) naar aanleiding van onderstaand datalek. 5.1.2.e heeft op een link in een e-mail geklikt om haar wachtwoord te veranderen. Waarschijnlijk was dat afgelopen vrijdag. Op maandag is in haar e-mailaccount ingebroken. Vanuit haar account zijn ca. 2200 e-mails verstuurd naar externen (vermoedelijk ook deels onbestaande accounts). Verder is een regel aangemaakt waarbij alle inkomende e-mail naar de verwijderde items werden doorgestuurd. In de inbox zelf stonden geen persoonsgegevens anders dan contactgegevens. MFA stond niet aan omdat 5.1.2.e tot een groep nieuwe medewerkers behoort waarvoor het nog niet was ingeschakeld.

Ik stel voor dit datalek te melden bij de toezichthouder en ook bij de betrokkenen c.q. de ontvangers van de phishing e-mails vanuit het account van 5.1.2.e

Dat betekent ook dat vanwege de exposure waarschijnlijk het PSIRT in actie moet komen over hoe en door wie het incident gemeld moet worden aan betrokkenen ([redacted], jij, situationeel eigenaar). Ik zal de uitnodiging sturen aan [redacted] en [redacted] werkt bij speciale collecties. Vind jij dat vanuit de library ook iemand aangehaakt moet worden? Zo ja, [redacted]?

Groet, [redacted]

[redacted]
Corporate Privacy Officer | Corporate Governance & Legal Services

Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | [redacted], Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317-[redacted]
www.wur.nl/disclaimer

Van: Privacy <privacy@wur.nl>
Verzonden: dinsdag 25 mei 2021 14:20
Aan: Privacy <privacy@wur.nl>;[redacted]@wur.nl>
Onderwerp: Nieuwe datalekmelding | 5/25/2021 12:19:28 PM |[redacted]@wur.nl
Urgentie: Hoog

Beste collega,

Zojuist is er een nieuw datalek gemeld via het digitale meldformulier:

* * *

1. Geef een zo gedetailleerd mogelijke omschrijving van het incident
Ik ben in een phising mail getrapt en er zijn uit mijn naam een heleboel mails verstuurd, niet naar WUR accounts, maar wel naar veel nadere (mogelijk niet bestaande accounts). Ik kon zelf geen mail meer versturen. Mijn mail adres werd als spam account aangemerkt

2. Wat is de aard van het incident?
Phising

3. Hoelang heeft het incident geduurd?
Meer dan één dag

4a. Gedurende welke periode heeft het incident plaatsgevonden?
in ieder geval vanaf 24 mei tot in de middag van 25 mei 2021

4b. Op welke datum heeft het incident plaatsgevonden?

5. Van welke categorie personen zijn persoonsgegevens gelekt?
["geen idee"]

6. Van hoeveel personen zijn mogelijk persoonsgegevens gelekt?
geen idee

7. Op welke datum/tijdstip is het incident ontdekt?
25 mei ongeveer 9.30

8. Wat voor soort persoonsgegevens zijn betrokken in het incident?
["Identificatiegegevens (login/wachtwoord)"]

9. Welke acties zijn ondernomen naar aanleiding van het incident?
Helpdesk gebeld, nieuw wachtwoord aangemaakt, ICT lost rest op (geen verstand van wat er precies moet gebeuren. Ook overlegd over installatie dual authenticatie op mijn account (heb ik nu niet)

* * *

Met vriendelijke groet,
5.1.2.e

[redacted]
Corporate Privacy Officer | 5.1.2.e

Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317 5.1.2.e

5.1.2.e

Van: 5.1.2.e
Verzonden: dinsdag 25 mei 2021 17:48
Aan: 5.1.2.e
Onderwerp: Datalek / melding aan betrokkenen
Bijlagen: 20191009_proces_privacy-security-breach_proces_1.0.pdf; 20210525_voorlopige_melding_5.1.2.e.pdf

Urgentie: Hoog

Beste 5.1.2.e en 5.1.2.e

Vandaag ontvingen wij een datalekmelding. Een collega binnen de WUR library heeft op een link in een e-mail geklikt om haar wachtwoord te veranderen. Waarschijnlijk was dat afgelopen vrijdag. Op maandag is in haar e-mailaccount ingebroken. Vanuit haar account zijn ca. 2200 e-mails verstuurd naar externen (vermoedelijk ook deels onbestaande accounts). Verder is een regel aangemaakt waarbij alle inkomende e-mail naar de verwijderde items werden doorgestuurd. In de inbox zelf stonden geen persoonsgegevens anders dan contactgegevens.

Ik begreep vanuit de Servicedesk IT dat MFA nog niet was ingeschakeld, omdat de medewerker half april in dienst is getreden en voor deze nieuwe medewerkers MFA niet was ingeschakeld.

Wij hebben dit incident inmiddels gemeld bij de toezichthouder (de AP), maar vanwege de aard van phishing en het beleid van de AP op dat gebied moeten wij het ook aan alle ca. 2200 ontvangers melden. Conform ons privacy- en incident response-beleid (bijgaand) en vanwege de met de melding gepaard gaande risico's nodig ik hierbij in overleg met 5.1.2.e (woordvoerder), 5.1.2.e (situationeel eigenaar), 5.1.2.e (CISO), 5.1.2.e (ISO) en 5.1.2.e (F-G) uit voor een korte bespreking morgenochtend.

Groet, 5.1.2.e

5.1.2.e | Corporate Governance & Legal Services

WAGENINGEN UNIVERSITY & RESEARCH

Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e | Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. +31 317 5.1.2.e

5.1.2.e

Van: 5.1.2.e
Verzonden: woensdag 26 mei 2021 15:14
Aan: 5.1.2.e
Onderwerp: RE: e-mail naar betrokkenen phishing versturen - jullie hulp nodig

Ha 5.1.2.e

Dank voor je bericht. Vanuit het privacyoogpunt is vastgesteld dat sprake is van een risico voor de ontvangers dat ondervangen kan worden met onverwijld actieve berichtgeving. Ik had daarover vanmorgen nog contact met de Autoriteit Persoonsgegevens die daarop aandrong naar aanleiding van het gisteren gemelde datalek. Zij gaven aan dat dit binnenkort op grond van nieuwe Europese richtsnoeren het standaardbeleid zal zijn bij iedere phishing.

Het betreft 599 ontvangers (ik heb de lijst). De tekst van het bericht is door het Privacy & Security Incident Response Team vastgesteld.

Heb jij zo voldoende informatie?

Groet, 5.1.2.e

[redacted] Corporate Governance & Legal Services

Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317 5.1.2.e
www.wur.nl/disclaimer

Van: 5.1.2.e @wur.nl>
Verzonden: woensdag 26 mei 2021 15:07
Aan: 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
Onderwerp: RE: e-mail naar betrokkenen phishing versturen - jullie hulp nodig

Hoi 5.1.2.e

doorgaans sturen we geen mails in reactie op phishing maar als we signalen binnenkrijgen (men vraagt het doorgaans direct na bij de Servicedesk IT) die actie nodig hebben laten we door mailbeheer de betreffende mail verwijderen uit de mailboxen en de erin opgenomen link(s) blokkeren en zetten we een bericht op itsupport en bijv intranetgroepen.

Ik heb er nog geen meldingen binnen zien komen: is er zicht op aan hoeveel het is verzonden en waarom voor dit bericht een tegenbericht nodig?

Met vriendelijke groet,

5.1.2.e
Servicedesk IT | Communicatieteam FB
Wageningen University & Research
Facilitair Bedrijf - Informatie Technologie

Beschikbaar: maandag t/m donderdag: 08:00 - 17:30 ; vrijdag: 08:00 – 14:00
Contact: E-mail | Microsoft Teams | Skype for Business

groetjes
5.1.2.e

From: 5.1.2.e @wur.nl>
Sent: woensdag 26 mei 2021 14:57
To: 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
Subject: e-mail naar betrokkenen phishing versturen - jullie hulp nodig
Importance: High

Hoi 5.1.2.e en 5.1.2.e,

Ik probeerde jullie al even te bellen, maar kon jullie helaas niet bereiken. Daarom dit bericht. Er is een issue geweest rondom phishing. Daarover moet een mail worden verstuurd naar de betrokkenen (die de mail ontvingen).
We hebben de tekst opgesteld en 5.1.2.e heeft de verzendinformatie. Hij begreep van 5.1.2.e dat jullie ons kunnen helpen bij de verzending.
Klopt dat?

De teksten heb ik hieronder overgenomen. In de opsomming wat handige toevoegingen over onderwerp en ondertekening.

- ondertekening Servicedesk
- onderwerp: Belangrijk: informatie over phishing e-mail

Ik ben nog niet goed bekend met dit proces én stap over een paar minuten in de auto, dus ook even wat minder goed bereikbaar zometeen. Maar ik hoop dat we dit samen kunnen regelen. Zal mijn mail in de gaten houden en ben mobiel zo ook weer bereikbaar.

Alvast bedankt voor jullie hulp.

Groeten,5.1.2.e

* * * *English below* * * *

Geachte heer, mevrouw,

U heeft een phishing e-mail ontvangen. Het onderwerp is 'Re: MAY benefit payment'. Wilt u deze direct verwijderen?
De e-mail is op 24 mei verstuurd vanuit een e-mailadres van WUR (@wur.nl). De e-mail is ondertekend door 'Help Desk'.

Verwijder de e-mail, deze is onveilig
We verzoeken u deze e-mail niet te openen. De link in de e-mail kan onbevoegden toegang geven tot uw systemen en bestanden. Klik er dus niet op.

Heeft u vragen? Neem contact op met de Servicedesk IT
Voor verdere vragen over dit bericht kunt u contact opnemen met de Servicedesk IT via servicedesk.it@wur.nl.

Met vriendelijke groet,

* * *

Dear Sir or Madam,

You have received a phishing email. The subject is 'Re: MAY benefit payment'. Please delete it immediately.

The email was sent on 24 May from a WUR email address (@wur.nl). The e-mail is signed by 'Help Desk'.

Delete the e-mail, it is unsafe
Please do not open this e-mail. The link in the e-mail may allow unauthorised access to your systems and files. Please do not click on it.

For more information, please contact the Servicedesk IT
For further questions about this message, please contact the Servicedesk IT at servicedesk.it@wur.nl.

Kind regards,

Privacy

Van: 5.1.2.e
Verzonden: woensdag 26 mei 2021 12:35
Aan: Privacy; 5.1.2.e
CC: 5.1.2.e
Onderwerp: RE: Terugkoppeling betrokkenen

Dag collega's,

Helder en zakelijk bericht. Ik heb er geen opmerkingen bij.

Groet,
5.1.2.e

From: Privacy <privacy@wur.nl>
Sent: woensdag 26 mei 2021 12:00
To: 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
Cc: 5.1.2.e @wur.nl>
Subject: Terugkoppeling betrokkenen

Dag allen,

Hieronder een zo kort mogelijk conceptberichtje, waar m.i. de vereiste informatie in staat. Zodra ik vanuit IT de e-maillijst krijg kan men (vanuit welk loket binnen FB?) dit met jullie welnemen uitsturen.

* * *

* * * *English below* * * *

Geachte heer, mevrouw,

Op 24 mei jl. heeft u vanuit een @wur.nl-mailadres een e-mail ontvangen met het onderwerp "Re: MAY benefit payment", ondertekend door 'Help Desk'.

Dit betreft een spambericht. Via de hyperlink in het bericht kunnen onbevoegden toegang krijgen tot uw systemen en bestanden. Voor zover u dit nog niet heeft gedaan verzoeken wij u het bericht direct uit uw inbox te verwijderen en niet op de link te klikken.

Voor verdere vragen over dit bericht kunt u contact opnemen met de Servicedesk IT via servicedesk.it@wur.nl.

Met vriendelijke groet,
[…]

* * *

Dear Sir, Madam,

On 24 May you received an e-mail with the subject "Re: MAY benefit payment" from an @wur.nl-address, signed by 'Help Desk'.

This is a spam message. Through the hyperlink unauthorized persons may access your systems and files. If you have not yet did so, we request you to delete the message from your inbox and avoid clicking on the link.

For further questions about this message, please contact the Servicedesk IT through servicedesk.it@wur.nl.

With kind regards,
[…]

Privacy

Van: Functionarisgegevensbescherming
Verzonden: woensdag 26 mei 2021 15:10
Aan: Privacy; 5.1.2.e
CC: 5.1.2.e
Onderwerp: RE: Terugkoppeling betrokkenen

Ook van mijn kant akkoord met de tekst.

Met vriendelijke groet,

5.1.2.e

WAGENINGEN
UNIVERSITY & RESEARCH

5.1.2.e | Functionaris Gegevensbescherming | Wageningen University & Research | Postbus 9101, 6700 HB Wageningen | +31 (0)317 5.1.2.e | www.wur.nl

---

From: Privacy <privacy@wur.nl>
Sent: Wednesday, May 26, 2021 2:30 PM
To: 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
Cc: 5.1.2.e @wur.nl>
Subject: RE: Terugkoppeling betrokkenen

Dag allen, ik weet ook niet zeker of de Servicedesk IT het aanspreekpunt moet zijn, maar dit leek mij de meest voorkomende plek en ik zou niet weten welk ander loket vanuit het FB daarvoor in aanmerking kan komen. Ik begreep van 5.1.2.e dat de Servicedesk IT in eerdere berichten als contactpunt is opgenomen.

Ik heb overigens ook nog geen lijst met ontvangers vanuit IT (ik verwacht die elk moment).

@5.1.2.e: ik begrijp dat het uitsturen van dit soort berichten normaal door communicatie wordt gedaan vanuit een no-reply-adres 5.1.2.e dacht 5.1.2.e ?). Zou jij dat eventueel kunnen nagaan?

Het bericht zelf lijkt mij prima zo.

Groet, 5.1.2.e

5.1.2.e
Corporate Privacy Officer | Corporate Governance & Legal Services

Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | C5.1.2.e, Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317-5.1.2.e
www.wur.nl/disclaimer

Van: 5.1.2.e @wur.nl>
Verzonden: woensdag 26 mei 2021 13:48
Aan: 5.1.2.e @wur.nl>;5.1.2.e @wur.nl>;5.1.2.e @wur.nl>;5.1.2.e @wur.nl>; Privacy <privacy@wur.nl>
CC: 5.1.2.e @wur.nl>
Onderwerp: RE: Terugkoppeling betrokkenen

Dag,

Is de servicedesk er van op de hoogte dat er naar hun wordt gerefereerd?
Helder bericht. Al blijven de mensen die reeds geklikt hebben mogelijk met wat vragen zitten die vervolgens bij de servicedesk uit komen.

Groeten, 5.1.2.e

From: 5.1.2.e @wur.nl>
Sent: Wednesday, May 26, 2021 13:10
To: 5.1.2.e @wur.nl>;5.1.2.e @wur.nl>;5.1.2.e @wur.nl>;5.1.2.e @wur.nl>; Privacy <privacy@wur.nl>
Cc: 5.1.2.e @wur.nl>
Subject: RE: Terugkoppeling betrokkenen

Dag allemaal,

Samen met 5.1.2.e keek ik kort naar de e-mail. Ik heb de tekst iets aangepast. De inhoud uiteraard zo min mogelijk. Kunnen jullie hiermee uit de voeten?

Volgens mij wordt de mail ook naar contacten buiten WUR gestuurd. Als het alleen binnen WUR wordt verstuurd, zou ik de aanhef nog iets veranderen, bijv. naar Beste WUR-collega's en studenten. Dan spreek je de ontvanger wat persoonlijker aan. Algemeen is Beste lezer ook een optie.

Een ander punt: als de mail ook extern wordt verstuurd, kun je aangeven dat het onze eigen servicedesk is. Voor medewerker en studenten is dit een bekend adres, voor externen kan het misschien onbetrouwbaar voelen.

Het kan bij verzending helpen om de WUR-handtekening en een duidelijke afzender (persoon/naam) te tonen. Zo zorgen we dat het een vertrouwde e-mail is.

Groeten 5.1.2.e

* * * *English below* * * *

Geachte heer, mevrouw,

U heeft een phishing e-mail ontvangen. Het onderwerp is 'Re: MAY benefit payment'. Wilt u deze direct verwijderen?
De e-mail is op 24 mei verstuurd vanuit een e-mailadres van WUR (@wur.nl). De e-mail is ondertekend door 'Help Desk'.

Verwijder de e-mail, deze is onveilig
We verzoeken u deze e-mail niet te openen. De link in de e-mail kan onbevoegden toegang geven tot uw systemen en bestanden. Klik er dus niet op.

Heeft u vragen? Neem contact op met de Servicedesk IT
Voor verdere vragen over dit bericht kunt u contact opnemen met de Servicedesk IT via servicedesk.it@wur.nl.

Met vriendelijke groet,
[…]

* * *

Dear Sir or Madam,

You have received a phishing email. The subject is 'Re: MAY benefit payment'. Please delete it immediately.
The email was sent on 24 May from a WUR email address (@wur.nl). The e-mail is signed by 'Help Desk'.

Delete the e-mail, it is unsafe
Please do not open this e-mail. The link in the e-mail may allow unauthorised access to your systems and files. Please do not click on it.

For more information, please contact the Servicedesk IT
For further questions about this message, please contact the Servicedesk IT at servicedesk.it@wur.nl.

Kind regards,

Ontvangstbevestiging

Uw verzoek tot het indienen van een melding wordt in behandeling genomen.
U kunt de melding niet online raadplegen. Maak daarom een print voor uw eigen administratie. Doe dit voordat u deze pagina afsluit. Na het afsluiten van deze pagina zijn de gegevens die u heeft opgegeven niet meer beschikbaar. Onder het onderstaande meldingsnummer is de melding bekend bij de Autoriteit Persoonsgegevens. U heeft het meldingsnummer nodig om de melding aan te kunnen passen of in te kunnen trekken. Vermeld het meldingsnummer bij eventuele correspondentie met de Autoriteit Persoonsgegevens over de melding.

Tijdstip ontvangst	25-05-2021 17:46:48
Uniek nummer	5.1.2.e

0. Over deze melding

Gaat het om een nieuwe of bestaande melding?	Een nieuwe melding indienen
Op grond van welke wettelijke bepaling doet u deze melding?	Algemene verordening gegevensbescherming (AVG)

1. Contactgegevens en overige algemene informatie

1.1 Contactgegevens

Over welke organisatie of welk bedrijf gaat het?

Registratienummer bij de Kamer van Koophandel	09215846
Naam van het bedrijf of de organisatie	Wageningen University
Adres	Droevendaalsesteeg 4
Postcode	6708PB
Plaats	Wageningen
In welke sector is de organisatie of het	Onderwijs - Tertiair onderwijs

bedrijf actief?

Wie meldt het datalek?

Naam	5.1.2.e
Functie	corporate privacy officer
E-mailadres	privacy@wur.nl
Telefoonnummer	0317 5.1.2.e

Met wie kan de Autoriteit Persoonsgegevens contact opnemen voor nadere informatie over de melding?

De melder is contactpersoon	Nee
Naam contactpersoon	5.1.2.e
Functie contactpersoon	functionaris gegevensbescherming
E-mailadres contactpersoon	dpo@wur.nl
Telefoonnummer contactpersoon	0317 5.1.2.e

1.2 Betrokkenheid andere organisatie

Was er een andere organisatie betrokken bij de inbreuk?	Nee

2. Tijdlijn

Exacte datum waarop de inbreuk was, indien bekend	24-05-2021
Duurt de inbreuk op dit moment nog voort?	Nee
Wanneer werd de inbreuk ontdekt?	25-05-2021

3. Gegevens over het datalek

3.1 Aard van de inbreuk

Inbreuk op de vertrouwelijkheid van de gegevens	Ja
Inbreuk op de integriteit van de gegevens	Nee
Inbreuk op de beschikbaarheid van de gegevens	Nee

3.2 Aard van het incident

Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest?	Hacking, malware (bijv. ransomware) en/of phishing

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest

Een collega binnen de WUR-library heeft op een link in een e-mail geklikt om haar wachtwoord te veranderen. Zeer waarschijnlijk was dat afgelopen vrijdag. Op maandag is in haar e-mailaccount ingebroken. Vanuit haar account zijn ca. 2200 e-mails verstuurd naar externen (vermoedelijk ook deels onbestaande accounts). Verder is een regel aangemaakt waarbij alle inkomende e-mail naar de verwijderde items werden doorgestuurd. In de inbox zelf stonden geen persoonsgegevens anders dan contactgegevens.

4. Persoonsgegevens die betrokken zijn bij het datalek

4.1 Persoonsgegevens in het algemeen

Naam	Ja
Geslacht, geboortedatum en/of leeftijd	Nee
Burgerservicenummer (BSN)	Nee
Contactgegevens	Ja
Toegangs- of identificatiegegevens	Ja
Financiële gegevens	Nee
(Kopieën van) paspoorten of andere legitimatiebewijzen	Nee
Locatiegegevens	Nee
Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen	Nee

4.2 Bijzondere categorieën van persoonsgegevens

Persoonsgegevens waaruit iemands ras	Nee

of etnische afkomst blijkt	
Persoonsgegevens waaruit iemands politieke opvattingen blijken	Nee
Persoonsgegevens waaruit iemands religieuze of levensbeschouwelijke overtuigingen blijken	Nee
Persoonsgegevens waaruit iemands lidmaatschap van een vakbond blijkt	Nee
Gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid	Nee
Gegevens over iemands gezondheid	Nee
Genetische gegevens	Nee
Biometrische gegevens	Nee

4.3 Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords ("gegevensregisters") zijn getroffen door de inbreuk	1

5. De groep mensen van wie persoonsgegevens betrokken zijn bij het datalek

Werknemers	Nee
Klanten (huidig en potentieel)	Ja
Leerlingen of studenten	Nee
Patiënten	Nee
Minderjarigen	Nee
Personen uit kwetsbare groepen	Nee

Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk.

Externe, onbekende e-mailadressanten

Van minimaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?	1500

Van maximaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?	2500

6. Maatregelen die zijn getroffen voordat het datalek plaatsvond

Waren de persoonsgegevens op het moment dat de inbreuk zich voordeed versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk voor onbevoegden?	Nee

7. Gevolgen van het datalek

7.1 Gevolgen van de inbreuk op de vertrouwelijkheid, de integriteit en/of de beschikbaarheid van de gegevens.

Onbevoegden hebben kennis kunnen nemen van de gegevens	Ja
De gegevens kunnen op een onbehoorlijke of onrechtmatige manier worden misbruikt	Nee
Er worden binnen uw eigen organisatie mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens gebruikt	Nee
Er worden mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens hergebruikt voor andere doeleinden of doorgegeven aan andere organisaties	Nee
Een essentiële dienst kan tijdelijk niet meer worden verleend aan de betrokkenen	Nee
Een essentiële dienst kan permanent	Nee

niet meer worden verleend aan de betrokkenen	

7.2 Lichamelijke, materiële en immateriële schade voor de betrokkenen

Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkenen?

Discriminatie	Nee
Identiteitsdiefstal of -fraude	Ja
Financiële verliezen	Nee
Reputatieschade	Nee
Verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens	Nee
Ongeoorloofde ongedaanmaking van pseudonimisering	Nee
Betrokkenen kunnen hun rechten en vrijheden niet uitoefenen	Nee
Betrokkenen worden verhinderd controle over hun persoonsgegevens uit te oefenen	Nee
Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkenen	2. Beperkt

8. Vervolgacties naar aanleiding van het datalek

8.1 Informeren van de betrokkenen

Heeft u het datalek gemeld aan de betrokkenen of bent u van plan dat te gaan doen?	Nog niet bekend

Wat is de inhoud van de melding aan de betrokkenen?

n.n.b.

Hoeveel betrokkenen heeft u geïnformeerd of gaat u informeren?	0

Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken om de betrokkenen te informeren?	e-mail

8.2 Maatregelen om de inbreuk aan te pakken

Welke technische en organisatorische maatregelen heeft uw organisatie getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?
Het wachtwoord is na ontdekking aangepast en de regel is verwijderd.

8.3 Internationale aspecten

Heeft de inbreuk zich voorgedaan in een grensoverschrijdende gegevensverwerking, en is de AP voor deze verwerking de leidende toezichthouder?	Nee
Heeft uw organisatie of bedrijf, het datalek gemeld bij privacytoezichthouders in een of meer andere EU-landen, of gaat u dat nog doen?	Nee
Heeft uw organisatie of bedrijf, het datalek gemeld bij Europese toezichthouders op andere meldplichten, of gaat u dat nog doen?	Nee

9. Overig

Is naar uw mening deze melding compleet?	Nee, er komt later een vervolgmelding met aanvullende informatie over deze inbreuk

Ontvangstbevestiging van melding inbreuk

Dit is de kopie van uw melding van een inbreuk aan de Autoriteit Persoonsgegevens ten behoeve van uw eigen administratie.

Bewaar deze kopie goed. Bij twijfel kunt u met deze kopie achteraf aantonen dat u een melding van een inbreuk heeft gedaan bij de AP.

Meldingsnummer: 5.1.2.e

Melddatum: 08 juni 2021

Meldtijdstip: 17:20

1 Introductie

1.1 De melding van een inbreuk

Wat wilt u doen?	Een bestaande melding aanvullen of aanpassen
Beschikt u over het meldingsnummer van de oorspronkelijke melding?	Ja
Dit is het meldingsnummer:	5.1.2.e

2 Aanvulling op eerdere samenvatting

2.1 Wie dient de aanvulling in?

Naam	5.1.2.e
Functie	corporate privacy officer
E-mailadres	privacy@wur.nl
Telefoonnnummer	0317 5.1.2.e
2.2 Is de indiener de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen	voor nadere informatie over de melding en aanvulling

Nee	
Naam contactpersoon	5.1.2.e
Functie contactpersoon	functionaris voor de gegevensbescherming
E-mailadres contactpersoon	dpo@wur.nl
Telefoonnummer contactpersoon	03175.1.2.e

3 Welke vragen

3.1 Welke vragen wilt u wijzigen of aanvullen?

[✓] 5. Gegevens over de inbreuk

[✓] Samenvatting van het incident

[✓] 6. Betrokken persoonsgegevens

[✓] Hoeveelheid persoonsgegevens

[✓] 7. Getroffen personen

[✓] Aantal personen die door de inbreuk zijn getroffen

[✓] 10. Vervolgacties

[✓] Informeren van de betrokkene(n) (de getroffen persoon of personen)?

5 Gegevens over datalek

5.3 Beschrijving van het incident

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest	Een collega binnen de WUR-library heeft op een link in een e-mail geklikt om haar wachtwoord te veranderen. Zeer waarschijnlijk was dat vrijdag 21 mei jl. Op maandag 24 mei jl. is in haar e-mailaccount ingebroken. Vanuit haar account zijn 599 e-mails verstuurd naar externen (grotendeels onbestaande accounts). Verder is een regel aangemaakt waarbij alle inkomende e-mail naar

de verwijderde items werden doorgestuurd. In de	inbox zelf stonden geen persoonsgegevens anders dan contactgegevens.

5.4 Optioneel: upload hier relevante ondersteunende documentatie bij uw melding.

6 Betrokken persoonsgegevens

6.3 Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords ("**-gegevensregisters**") zijn getroffen door het datalek	1
Geef een toelichting op bovengenoemd aantal:	Het betreft de mailbox van één persoon.

7 Betrokkenen

7.3 Is het exacte aantal betrokkenen bekend?	Ja
Het exacte aantal is:	599

10 Vervolgacties naar aanleiding van de inbreuk

10.1 Informeren van de betrokkene(n)

Heeft u de inbreuk reeds gemeld aan de betrokkene(n)?	Ja
Aan hoeveel personen heeft u de inbreuk gemeld?	599
Wanneer heeft u de inbreuk gemeld aan de betrokkene(n)?	26-5-2021
Wat is de inhoud van de melding aan degene van wie gegevens zijn gelekt?	Geachte heer, mevrouw, U heeft een phishing e-mail ontvangen. Het onderwerp is ‘Re: MAY benefit payment’. Wilt u deze direct verwijderen? De e-mail is op 24 mei verstuurd vanuit een e-mailadres van WUR (@wur.nl). De e-mail is ondertekend door ‘Help Desk’. Verwijder de e-mail, deze is onveilig We verzoeken u deze e-mail niet te openen. De link in de e-mail kan onbevoegden toegang

geven tot uw systemen en bestanden. Klik er dus niet op. Heeft u vragen? Neem contact op Voor verdere vragen over dit bericht kunt u	contact opnemen met privacy@wur.nl. Met vriendelijke groet, Servicedesk IT

Optioneel: upload hier een kopie van de tekst van deze kennisgeving.

Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken om de betrokkene(n) te informeren?

Meerdere opties zijn mogelijk.

[✓] Per e-mail

11 Verzenden

Is dit een voorlopige of een definitieve melding?	Ja, de melding is definitief. Ik heb de vereiste informatie verstrekt en er is geen vervolgmelding nodig

[✓] Door dit vakje aan te vinken verklaart u dit formulier naar waarheid in te vullen

[✓] Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen namens uw organisatie.

Privacyverklaring

[✓] Ik ben op de hoogte van de inhoud van de Privacyverklaring van de AP

5.1.2.e

Van: Privacy
Verzonden: woensdag 8 september 2021 09:41
Aan: Privacy; 5.1.2.e
Onderwerp: Nieuwe datalekmelding | 9/8/2021 7:41:02 AM 5.1.2.e @wur.nl

Urgentie: Hoog

Beste collega,

Zojuist is er een nieuw datalek gemeld via het digitale meldformulier:

* * *

1. Geef een zo gedetailleerd mogelijke omschrijving van het incident
Mijn 5.1.2.e account bleek gehacked.

2. Wat is de aard van het incident?
5.1.2.e account gehacked maar men kon er niet in komen aangezien 2fa aan staat.

3. Hoelang heeft het incident geduurd?
Eén dag

4a. Gedurende welke periode heeft het incident plaatsgevonden?

4b. Op welke datum heeft het incident plaatsgevonden?
2021-09-08

5. Van welke categorie personen zijn persoonsgegevens gelekt?
["Er is geen data gelekt omdat er geen info op mijn pc staat."]

6. Van hoeveel personen zijn mogelijk persoonsgegevens gelekt?
geen

7. Op welke datum/tijdstip is het incident ontdekt?
8 september.

8. Wat voor soort persoonsgegevens zijn betrokken in het incident?
["Er is niets gelekt. Geen persoonsgevens op mijn pc."]

9. Welke acties zijn ondernomen naar aanleiding van het incident?
Wachtwoord is gewijzigd.

* * *

Met vriendelijke groet,
5.1.2.e

Corporate Privacy Officer | 5.1.2.e

Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317 5.1.2.e

Privacy

Van: Privacy
Verzonden: woensdag 8 september 2021 16:02
Aan: 5.1.2.e
Onderwerp: RE: Datalekmelding

Dag 5.1.2.e

Helder. Bedankt voor je aanvullende reactie (en voor het melden).

Gezien het feit dat de 2FA zijn werk goed heeft gedaan vloeien hier voor WUR geen vervolgacties uit voort en is deze melding hierbij gesloten.

Groet, 5.1.2.e

Van: 5.1.2.e @wur.nl>
Verzonden: woensdag 8 september 2021 13:48
Aan: Privacy <privacy@wur.nl>
Onderwerp: RE: Datalekmelding

Dag 5.1.2.e

Vanochtend kreeg ik de melding terwijl we met een ander probleem bezig waren dat men met mijn account probeerde in te loggen. Ik zelf heb hier geen meldingen over gehad en omdat 2fa aan staat, kunnen ze er ook niet zomaar in.
Ik heb voor de zekerheid toch maar mijn wachtwoord gewijzigd en aan security gevraagd of ze nog wat dieper kunnen kijken.
Vandaar dat ik voor de zekerheid een melding naar jullie gemaakt.

Met vriendelijke groet,

5.1.2.e
Senior Skilled servicedesk medewerker
Servicedesk IT
Wageningen University & Research
Facilitair Bedrijf - Informatie Technologie
E Servicedesk.IT@wur.nl
T (0317-4) 88 888
W ITsupport.wur.nl

From: Privacy <privacy@wur.nl>
Sent: woensdag 8 september 2021 13:20
To: 5.1.2.e @wur.nl>
Subject: Datalekmelding

Beste 5.1.2.e

Bedankt voor je datalekmelding van vanmorgen. Je geeft hierin aan dat je account is gehackt, maar dat derden geen toegang hebben gehad tot je account. Naar aanleiding daarvan ben ik benieuwd naar de precieze aard van de hack: kun je iets preciezer omschrijven:

- hoe je account gehackt is (bijv. phishing?)
- hoe je dit ontdekt hebt
- waarom je zeker weet dat derden geen toegang hebben gehad tot bestanden in je account (dus buiten Outlook ook niet tot je OneDrive/Teams/netwerkopslag?)

Ik hoor graag nog even van je.

Groet, 5.1.2.e

[redacted]
Corporate Privacy Officer | 5.1.2.e
Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e | Droevendaalsesteeg 4
6708 PB Wageningen
Tel. +31 317 5.1.2.e

Privacy

Van: 5.1.2.e
Verzonden: donderdag 23 september 2021 09:53
Aan: Privacy
Onderwerp: RE: Nieuwe datalekmelding | 9/21/2021 1:29:39 PM | 5.1.2.e @wur.nl

Dank!

Met vriendelijke groet,

5.1.2.e

WAGENINGEN
UNIVERSITY & RESEARCH

5.1.2.e | General Counsel & Compliance officer| Corporate Governance & Legal Services | Wageningen University & Research | Postbus 9101, 6700 HB Wageningen | +31 (0)317 5.1.2.e | www.wur.nl

---

From: Privacy <privacy@wur.nl>
Sent: Wednesday, September 22, 2021 5:44 PM
To: 5.1.2.e @wur.nl>
Subject: RE: Nieuwe datalekmelding | 9/21/2021 1:29:39 PM | 5.1.2.e @wur.nl

Hierbij de datalekmelding.

Van: Privacy
Verzonden: woensdag 22 september 2021 17:18
Aan: 5.1.2.e @wur.nl>
Onderwerp: FW: Nieuwe datalekmelding | 9/21/2021 1:29:39 PM | 5.1.2.e @wur.nl
Urgentie: Hoog

Dag 5.1.2.e

Wij ontvingen gistermiddag onderstaande melding. Ik had vanmorgen nog even contact met 5.1.2.e hierover.

In Planon is een kwetsbaarheid gesignaleerd, waardoor medewerkers toegang konden krijgen tot actieve meldingen bij de Servicedesk Facilities van andere personen, door een getal te wijzigen in het eigen meldingsnummer. De inhoud van de meldingen betreft vooral huis-tuin-en-keuken-zaken, zoals kapotte toiletten en dergelijke. In sommige gevallen kan het gaan om het aanvragen van toegang voor locaties; in dat geval zouden ook WUR-card nummers betrokken kunnen zijn. Verder zijn uitsluitend de naam van de melder en inhoud van de melding kenbaar geweest.

Het betreft wel een potentieel grote groep betrokkenen (4797 meldingen sinds december 2019; dat hoeven geen unieke betrokkenen te zijn), maar het risico op misbruik is zeer klein en de verwachte gevolgen zeer beperkt (hooguit zou een medewerker inzage hebben in de melding van een andere medewerker).

De functionaliteit is inmiddels uitgezet.

Mijn advies is om het incident te melden bij de toezichthouder vanwege de grote groep betrokkenen. Ik zie echter geen waarschijnlijke negatieve gevolgen, zodat een melding aan betrokkenen mij niet nodig lijkt.

Ik hoor graag of jij het hiermee eens bent.

Groet, 5.1.2.e

Van: Privacy <privacy@wur.nl>
Verzonden: dinsdag 21 september 2021 15:30
Aan: Privacy <privacy@wur.nl>; 5.1.2.e wur.nl>
Onderwerp: Nieuwe datalekmelding | 9/21/2021 1:29:39 PM | 5.1.2.e @wur.nl
Urgentie: Hoog

Beste collega,

Zojuist is er een nieuw datalek gemeld via het digitale meldformulier:

* * *

1. Geef een zo gedetailleerd mogelijke omschrijving van het incident
Via de e-mail communiceert Planon een directe link naar tickets naar de melder en evt naar namens wie gemeld wordt. Deze link zou enkel door die twee (altijd natuurlijke) personen in gezien moeten kunnen worden. Dit blijkt niet het geval te zijn geweest, waardoor het mogelijk was deze link te delen en om getallen te gokken om inzage te verkrijgen in andermans tickets.

2. Wat is de aard van het incident?
Inzage van facilitaire meldingen door onbevoegden

3. Hoelang heeft het incident geduurd?
Meer dan één dag

4a. Gedurende welke periode heeft het incident plaatsgevonden?
december 2019 - 21-09-2021

4b. Op welke datum heeft het incident plaatsgevonden?

5. Van welke categorie personen zijn persoonsgegevens gelekt?
["Studenten","Medewerkers"]

6. Van hoeveel personen zijn mogelijk persoonsgegevens gelekt?
1000

7. Op welke datum/tijdstip is het incident ontdekt?
21-09-2021 14:00

8. Wat voor soort persoonsgegevens zijn betrokken in het incident?
["NAW-gegevens","Persoonsgebondennummers (BSN, paspoortnummer, studentnummer)"]

9. Welke acties zijn ondernomen naar aanleiding van het incident?
De directe link functionaliteit is uitgeschakeld

* * *

Met vriendelijke groet,
5.1.2.e

5.1.2.e
Corporate Privacy Officer 5.1.2.e

Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e, Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317[redacted]

AUTORITEIT
PERSOONSGEGEVENS

Ontvangstbevestiging van melding inbreuk

Dit is de kopie van uw melding van een inbreuk aan de Autoriteit Persoonsgegevens ten behoeve van uw eigen administratie.

Bewaar deze kopie goed. Bij twijfel kunt u met deze kopie achteraf aantonen dat u een melding van een inbreuk heeft gedaan bij de AP.

Meldingsnummer: 5.1.2.e

Melddatum: 22 september 2021

Meldtijdstip: 17:38

1 Introductie

1.1 De melding van een inbreuk

Wat wilt u doen?	Een nieuwe melding doen van een inbreuk
Wat voor soort datalekmelding wilt u doen?	Ik wil één inbreuk melden (reguliere melding)

1.2 Meldplicht AVG, Tw, Wjsg of Wpg

Op grond van welke wettelijke bepaling doet u deze melding?	Algemene verordening gegevensbescherming (AVG)

1.3 Andere toezichthouders

Heeft uw organisatie of bedrijf de inbreuk gemeld bij toezichthouders op andere meldplichten? Of gaat u dat nog doen?	Nee

2 Internationale aspecten

2.1 Grensoverschrijdende inbreuk

Heeft de inbreuk gevolgen voor personen in meerdere landen?	Nee

3 De verwerkingsverantwoordelijke

3.1 Gegevens verwerkingsverantwoordelijke

AUTORITEIT PERSOONSGEGEVENS

KvK-nummer	09215846
Naam van het bedrijf of de organisatie	Wageningen University
Adres	Droevendaalsesteeg 4
Postcode	6708PB
Plaats	Wageningen

In welke sector is de organisatie of het bedrijf actief?

[✓] Onderwijs

[✓] Tertiair onderwijs

3.2 Gegevens melder en contactpersoon

Wie meldt de inbreuk?

Naam	5.1.2.e
Functie	Corporate Privacy Officer
E-mailadres	privacy@wur.nl
Telefoonnummer	0317 5.1.2.e
Is de melder de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen voor nadere informatie over de melding?	Nee
Naam contactpersoon	5.1.2.e
Functie contactpersoon	F-G
E-mailadres contactpersoon	dpo@wur.nl
Telefoonnummer contactpersoon	0317 5.1.2.e

AUTORITEIT PERSOONSGEGEVENS

3.3 Andere organisaties

Waren er andere organisaties betrokken bij de inbreuk?	Nee

4 Tijdlijn

4.1 Duurt de inbreuk op dit moment nog voort?	Nee
(Mogelijke) startdatum van de inbreuk	1-12-2019
(Mogelijke) einddatum van de inbreuk	21-9-2021
4.2 Wanneer is het incident ontdekt?	21-9-2021
4.3 Geef (kort) aan hoe u de inbreuk heeft ontdekt	Een medewerker signaleerde dat hij/zij toegang had tot de inhoud van een melding (bij onze facilitaire servicedesk) van een andere medewerker en heeft dat gerapporteerd aan de Servicedesk IT.
4.4 Is dit het moment waarop u het incident heeft bestempeld als inbreuk (“datalek”) en dus kennis heeft gekregen van de inbreuk?	Ja

5 Gegevens over de inbreuk

5.1 Aard van de inbreuk

[✓] Persoonsgegevens (mogelijk) ingezien door onbevoegden

5.2 Aard van het incident

Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest?

[✓] Autorisatie(s) van medewerker(s) verkeerd ingesteld

5.3 Beschrijving van het incident

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest	In onze servicedesksoftware is een kwetsbaarheid gesignaleerd, waardoor medewerkers van WUR toegang konden krijgen tot - uitsluitend actieve -

AUTORITEIT PERSOONSGEGEVENS

meldingen bij de Servicedesk Facilities van andere medewerkers binnen WUR, door een getal te wijzigen in het eigen meldingsnummer. De inhoud van de meldingen betreft vooral huis-tuin-en-keuken-zaken, zoals kapotte toiletten en dergelijke. In sommige gevallen kan het gaan om het aanvragen van toegang voor locaties. De kans op misbruik is zeer klein.	

5.4 Optioneel: upload hier relevante ondersteunende documentatie bij uw melding.

6 Welke persoonsgegevens

6.1 Persoonsgegevens in het algemeen

[✓] Naam

[✓] Anders

Namelijk:	(zeer incidenteel) WUR-card nummers

6.2 Bijzondere categorieën van persoonsgegevens

Meerdere opties zijn mogelijk.

6.3 Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords ("-**gegevensregisters**") zijn getroffen door het datalek	1
Geef een toelichting op bovengenoemd aantal:	Het betreft één softwaresysteem

7 Getroffen personen

7.1 Welke groep(en) betrokkenen is (zijn) getroffen door de inbreuk?

Meerdere opties zijn mogelijk.

[✓] Werknemers

7.2 Geef een nadere omschrijving van de groep(en) betrokkenen.	Medewerkers van WUR
7.3 Is het exacte aantal betrokkenen bekend?	Nee
Het minimum aantal betrokkenen is:	1

AUTORITEIT PERSOONSGEGEVENS

Het maximum aantal betrokkenen is:	4,797

8 Maatregelen vooraf

8.1 Waren de persoonsgegevens voordat de inbreuk zich voordeed versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden?

[✓] Nee

9 Gevolgen

9.1 (Mogelijke) gevolgen voor de verwerkingsverantwoordelijke en de persoonsgegevens.

Meerdere opties zijn mogelijk.

[✓] Onbevoegden hebben kennis kunnen nemen van de gegevens

9.2 (Mogelijke) gevolgen voor de betrokkene(n)

Meerdere opties zijn mogelijk.

[✓] Anders

Namelijk:	Facilitaire meldingen waren mogelijk inzichtelijk voor andere medewerkers

9.3 Inschatting risico

Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkene(n)	Verwaarloosbaar
Licht uw keuze toe:	Het risico op misbruik is zeer klein. Effectief zou een medewerker het nummer in de eigen melding moeten veranderen in een ander nummer. Bovendien waren alleen actieve meldingen inzichtelijk (in de regel is de doorlooptijd enkele uren tot enkele dagen). Tot slot de verwachte gevolgen voor de privacy van de betrokkenen zeer beperkt (hooguit zou een medewerker inzage hebben in de - in de regel nogal triviale - melding van een andere medewerker).

AUTORITEIT PERSOONSGEGEVENS

10 Vervolgacties naar aanleiding van de inbreuk

10.1 Informeren van de betrokkene(n)

Heeft u de inbreuk reeds gemeld aan de betrokkene(n)?	Nee
Gaat u de inbreuk nog melden aan de betrokkene(n)?	Nee

10.2 Motivering niet (persoonlijk) informeren van de betrokkene(n)

Waarom ziet u er van af om (een deel van) de personen van wie gegevens zijn getroffen door de inbreuk te informeren over het incident?

Meerdere opties zijn mogelijk.

[✓] Het zou een onevenredige inspanning vergen om iedere betrokkene op individuele basis te informeren

Licht toe waarom het een onevenredige inspanning zou vergen om de betrokkenen op individuele basis te informeren	De kans op misbruik en het risico op nadelige gevolgen is dermate verwaarloosbaar (zie bovenstaande antwoorden) dat iedere melding aan betrokkenen onevenredig zou zijn.

10.3 Maatregelen om de inbreuk aan te pakken

Heeft uw organisatie maatregelen getroffen om de inbreuk aan te pakken?	Ja, namelijk:
Toelichting:	De functionaliteit is inmiddels uitgezet, zodat medewerkers geen misbruik meer kunnen maken van de kwetsbaarheid.
Heeft uw organisatie maatregelen getroffen om nieuwe soortgelijke inbreuken te voorkomen?	Ja, namelijk:
Toelichting:	De functionaliteit is inmiddels uitgezet, zodat medewerkers geen misbruik meer kunnen maken van de kwetsbaarheid.

11 Verzenden

Is dit een voorlopige of een definitieve melding?

AUTORITEIT
PERSOONSGEGEVENS

Ja, de melding is definitief. Ik heb de vereiste informatie verstrekt en er is geen vervolgmelding nodig

[✓] Door dit vakje aan te vinken verklaart u dit formulier naar waarheid in te vullen

[✓] Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen namens uw organisatie.

Privacyverklaring

[✓] Ik ben op de hoogte van de inhoud van de Privacyverklaring van de AP

5.1.2.e

Van: Privacy
Verzonden: donderdag 25 november 2021 12:35
Aan: Privacy; 5.1.2.e
Onderwerp: Nieuwe datalekmelding | 11/25/2021 11:34:51 AM | 5.1.2.e @wur.nl

Urgentie: Hoog

Beste collega,

Zojuist is er een nieuw datalek gemeld via het digitale meldformulier:

* * *

1. Geef een zo gedetailleerd mogelijke omschrijving van het incident
Een student meldde dat er doorgeklikt kon worden op roosterrecords waardoor uiteindelijk informatie over de deelnemers aan onderwijs gevonden konden worden. De gegevens waren lijsten van interne (nietszeggende id's). Doorklikken op de ID leverde de wuraccount (id) van de gebruiker op en naam/email adres van de gebruiker. Je kon via deze manier herleiden voor welke vakken een student ingeschreven is (of is is geweest). Dit was alleen mogelijk op een pagina voor studenten waar je via SSO op kan komen. Op de openbare pagina en de SSO pagina voor medewerkers was alles correct in orde. De oorzaak was een vinkje in de settings die dit mogelijk maakte en dat is per direct aangepast. In principe betreft het gegevens die ook via andere manieren te vinden is binnen het wur netwerk, dus de gevolgen zijn naar verwachting zeer beperkt of verwaarloosbaar.

2. Wat is de aard van het incident?
De oorzaak was een vinkje in de settings die dit mogelijk maakte en dat is per direct aangepast.

3. Hoelang heeft het incident geduurd?
Meer dan één dag

4a. Gedurende welke periode heeft het incident plaatsgevonden?
Vermoedelijk sinds april 2021 tot het moment van melden (25 nov 2021), het moment waarop voor de group tool de studenten zijn toegevoegd binnen timeedit.

4b. Op welke datum heeft het incident plaatsgevonden?

5. Van welke categorie personen zijn persoonsgegevens gelekt?
["Studenten"]

6. Van hoeveel personen zijn mogelijk persoonsgegevens gelekt?
geen idee en ook niet te achterhalen.

7. Op welke datum/tijdstip is het incident ontdekt?
25 nov 2021 is de melding binnengekomen bij het beheer van TimeEdit. De melding was al iets eerder gedaan bij de privacy officwer.

8. Wat voor soort persoonsgegevens zijn betrokken in het incident?
["NAW-gegevens","Identificatiegegevens (login/wachtwoord)"]

9. Welke acties zijn ondernomen naar aanleiding van het incident?
De setting is uitgezet en werking van de setting wordt gecommuniceerd met de beheerders zodat herhaling wordt voorkomen.

* * *

Met vriendelijke groet,
5.1.2.e

Corporate Privacy Officer 5.1.2.e

Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317 5.1.2.e

Privacy

Van: Privacy
Verzonden: donderdag 25 november 2021 13:21
Aan: Privacy ESA
Onderwerp: RE: Vraag TimeEdit

NB: ik zie dat TimeEdit al op de witte lijst staat. Ik dacht dat logging een check was in dat proces, maar kennelijk niet. Of is er wel logging, maar niet op dit proces?

5.1.2.e
Corporate Privacy Officer | Corporate Governance & Legal Services
Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317 5.1.2.e
www.wur.nl/disclaimer

Van: Privacy
Verzonden: donderdag 25 november 2021 13:06
Aan: Privacy ESA <privacy.esa@wur.nl>
Onderwerp: RE: Vraag TimeEdit

Ha 5.1.2.e, fijn – dank je voor de opvolging en terugkoppeling. Heb het formulier ontvangen. Inderdaad goed om de student even te berichten.
Qua omvang: betrof dit studentengegevens van ál onze actieve studenten die op deze manier toegankelijk waren? Verder eens met de conclusie dat het niet waarschijnlijk is dat dit incident een risico meebrengt voor de studenten en dus niet gemeld hoeft te worden. Gaat er nu wel logging opkomen (en ook witte-lijst-proces opstarten)?
Groet, 5.1.2.e

Corporate Privacy Officer | Corporate Governance & Legal Services
Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317 5.1.2.e
www.wur.nl/disclaimer

Van: Privacy ESA <privacy.esa@wur.nl>
Verzonden: donderdag 25 november 2021 12:25
Aan: Privacy <privacy@wur.nl>
Onderwerp: RE: Vraag TimeEdit

Goedemorgen 5.1.2.e,
Komt een datalekformulier jouw kant op. Stond een vinkje verkeerd, waardoor dit mogelijk was. Dit is hersteld.
Risico is mijns inziens beperkt, doordat het enkel met WUR-emailadressentoegankelijk is. Gegevens waren inzichtelijk voor studenten, niet docenten. Gaat om WUR-ID, e-mailadres, naam, vak. Overigens zat er een filter op, waardoor deze gegevens niet geheel representatief waren. Het is niet mogelijk na te gaan in hoeverre gegevens op deze wijze zijn geraadpleegd, maar gezien de semi-openbare aard van de gegevens is het risico beperkt voor studenten. Daarmee zou dit niet gemeld hoeven worden aan de AP.
Zal ik de student berichten met een korte reactie en het verzoek om te checken of het inderdaad verholpen is?
Mvg,
5.1.2.e

Van: Privacy <privacy@wur.nl>
Verzonden: dinsdag 23 november 2021 08:47
Aan: Privacy ESA <privacy.esa@wur.nl>
Onderwerp: FW: Vraag TimeEdit

Ha 5.1.2.e,
Zou jij hier snel actie op willen ondernemen en binnenkort ergens aan mij willen terugkoppelen?
Groet, 5.1.2.e

Corporate Privacy Officer | Corporate Governance & Legal Services
Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317[redacted]
www.wur.nl/disclaimer

Van: [redacted]@wur.nl>
Verzonden: vrijdag 19 november 2021 12:56
Aan: Privacy <privacy@wur.nl>
Onderwerp: Vraag TimeEdit

Beste lezer,

Vandaag was ik mijn rooster aan het opzoeken op TimeEdit en bij toeval kwam ik erachter dat je van elk vak kan zien wie dat volgen, hebben gevolgd of gaan volgen, ook al doe je dat vak zelf helemaal niet. Vervolgens kan je per persoon zien bij welke andere groepen ze horen, dus welke vakken iemand heeft gedaan of doet.

Als jenamelijk in TimeEdit een vak kiest waarvan een rooster is gepubliceerd kan je daarop klikken om een overzicht van die activiteit (college, tutorial etc. te krijgen). Bij elke activiteit staat namelijk ook een Group (A, B of iedereen), maar daar kan ik ook op klikken. Dan krijg je een lijst met nummers te zien. Ik weet niet of dit studentnummers zijn of andere nummers, maar als je die aanklinkt, krijg je van de desbetreffende persoon het wurid, naam en emailadres te zien. Maar ook van welke groepen ze lid zijn, dus eigenlijk welke vakken iemand heeft gedaan.

Ik vond dit zelf best wel gek, dus vroeg me af of andere studenten dat van mij dus ook kunnen zien.

Met vriendelijke groet,

[redacted]

Privacy

Van: Privacy
Verzonden: donderdag 25 november 2021 14:39
Aan: 5.1.2.e
CC: Privacy ESA
Onderwerp: Datalekmelding

Beste 5.1.2.e

Bedankt voor je datalekmelding van vanmiddag.

Ik heb inmiddels ook contact gehad met 5.1.2.e en begrijp dat sprake is van een autorisatie-/inrichtingsissue binnen de TimeEdit applicatie waarbij WUR-account, naam en e-mailadres van studenten inzichtelijk waren voor andere studenten.

Hier is formeel sprake van een datalek in de zin van de AVG, omdat onbevoegden inzage kregen in een bestand met (niet-gevoelige) persoonsgegevens waartoe zij normaal gesproken niet geautoriseerd zijn. Wij kunnen niet uitsluiten dat sprake is geweest van toegang en kunnen daarmee de ernst van het datalek niet volledig beoordelen. Maar in afstemming met de functionaris voor de gegevensbescherming stelden wij inmiddels vast dat hier geen sprake is van een waarschijnlijkheid op negatieve gevolgen voor de betrokkenen, zodat wij het incident niet hoeven te melden bij de Autoriteit Persoonsgegevens of bij de betrokken medewerkers.

Nogmaals dank voor je melding. Dit helpt ons om ons datalekkenregister compleet te houden en waar nodig tijdig actie te kunnen nemen. Mocht je nog vragen hebben of willen overleggen dan zijn wij daarvoor graag beschikbaar.

Vriendelijke groet,
5.1.2.e

[redacted]
Corporate Privacy Officer 5.1.2.e
Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e |
Droevendaalsesteeg 4 6708 PB
Wageningen
Tel. +31 317 5.1.2.e

Privacy

Van: Privacy
Verzonden: vrijdag 8 oktober 2021 11:19
Aan: 5.1.2.e ; Functionarisgegevensbescherming; 5.1.2.e
CC: 5.1.2.e
Onderwerp: RE: Nieuwe datalekmelding | 10/7/2021 7:15:27 AM

Dank en daar heb je natuurlijk gelijk in (maar het is uiteindelijk wel veiliger; ze kunnen de irrelevantie ook vaststellen door vervolgens naar MyHR te gaan). De herinnering zou ook iets kunnen zijn als "check of er een actie voor je klaarstaat", maar dan wordt het wel heel onbepaald.
Wij hopen dat er een gebalanceerde tussenoplossing bedacht kan worden.
Groet, 5.1.2.e

Corporate Privacy Officer | Corporate Governance & Legal Services
Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317-5.1.2.e
www.wur.nl/disclaimer

Van: 5.1.2.e @wur.nl>
Verzonden: vrijdag 8 oktober 2021 11:14
Aan: Privacy <privacy@wur.nl>; Functionarisgegevensbescherming <functionarisgegevensbescherming@wur.nl>; 5.1.2.e @wur.nl>
CC: 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
Onderwerp: RE: Nieuwe datalekmelding | 10/7/2021 7:15:27 AM
Urgentie: Hoog

Onze mails hebben elkaar gekruist: dat is in combinatie met het feit dat een aantal HR Professionals de mail kunnen negeren niet zo handig. Dat kunnen ze nl opbv de naam juist vaststellen.
5.1.2.e (PO) legt de werkgroep WvP/ HR nu voor dat we óf de mailfunctionaliteit helemaal uit kunnen zetten óf HR Professionals de mail in een aantal gevallen moeten negeren en dat kunnen ze dus aan de naam van de mdw vaststellen.
Met vriendelijke groet,
5.1.2.e

Afw op vrijdag
CC-mail gaat naar een aparte folder en lees ik onregelmatig

Van: Privacy <privacy@wur.nl>
Verzonden: Friday, October 08, 2021 10:53 AM
Aan: 5.1.2.e @wur.nl>
CC: 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>;
Functionarisgegevensbescherming <functionarisgegevensbescherming@wur.nl>
Onderwerp: RE: Nieuwe datalekmelding | 10/7/2021 7:15:27 AM

Ha 5.1.2.e ,
Bedankt voor ons gesprek. Ik heb inmiddels even met 5.1.2.e afgestemd. Ik vat het even samen:
De ontvangers hebben via DPI al toegang tot deze informatie, zodat de persoonsgegevens bij hen al bekend kunnen zijn. In die zin is er geen (verhoogd) risico binnen WUR. Tegelijkertijd is de e-mail een andere verwerking dan het raadplegen van DPI. De informatie komt met de e-mail ook op een andere plek terecht dan DPI (namelijk in Outlook/e-mailboxen van alle actieve en inactieve HR-professionals). Dit betekent dat de betrokkenen met deze functionaliteit wel een groter risico lopen (bijv. als de e-mailbox van de HR- professional gehackt wordt en de mail nog niet handmatig verwijderd is). Om die reden, maar ook omdat de taak primair bij de leidinggevende ligt (en er dus geen noodzaak is tot verwerken van de persoonsgegevens door de HR-professional) en omdat het best een aantal keer per jaar kan voorkomen, adviseren wij als tijdelijke actie om de e-mails richting de HR-professionals toch te anonimiseren naar iets als 'er staat een actie voor je klaar', hangende de (hopelijke) implementatie van het onderscheid inactieve/actieve HR-professional bij ADP.
Kunnen jullie hiermee uit de voeten?

Groet, 5.1.2.e

Corporate Privacy Officer | Corporate Governance & Legal Services
Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e, Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317 5.1.2.e
www.wur.nl/disclaimer

Van: 5.1.2.e @wur.nl>
Verzonden: donderdag 7 oktober 2021 18:27
Aan: Privacy <privacy@wur.nl>
CC: 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
Onderwerp: Re: Nieuwe datalekmelding | 10/7/2021 7:15:27 AM

Ha 5.1.2.e, sorry toch niet meer gelukt vandaag, bel je morgen!!
Outlook voor Android downloaden

From: Privacy <privacy@wur.nl>
Sent: Thursday, October 7, 2021 1:35:26 PM
To: 5.1.2.e @wur.nl>
Cc: 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
Subject: RE: Nieuwe datalekmelding | 10/7/2021 7:15:27 AM

Ha 5.1.2.e ,
Als het lukt dan inderdaad graag nog even contact. Het is natuurlijk wel een datalek, omdat onbevoegden inzage krijgen in bijzondere persoonsgegevens waarvoor zij niet geautoriseerd zijn. Dat de gevolgen waarschijnlijk niet nadelig zijn voor betrokkenen doet daar niet aan af (dat heeft alleen gevolgen voor de afweging van het privacyteam om het wel/niet te melden aan de AP).
Groet, 5.1.2.e

Corporate Privacy Officer | Corporate Governance & Legal Services
Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e, Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317-5.1.2.e
www.wur.nl/disclaimer

Van: 5.1.2.e @wur.nl>
Verzonden: donderdag 7 oktober 2021 11:50
Aan: Privacy <privacy@wur.nl>
Onderwerp: Re: Nieuwe datalekmelding | 10/7/2021 7:15:27 AM

Zit in workshop maar ga je bellen in een pauze 5.1.2.e!
En nee dit is iets anders en al contained.
Outlook voor Android downloaden

From: Privacy <privacy@wur.nl>
Sent: Thursday, October 7, 2021 11:13:53 AM
To: 5.1.2.e @wur.nl>
Subject: FW: Nieuwe datalekmelding | 10/7/2021 7:15:27 AM

Ha 5.1.2.e ,
Zou jij mij hier even over kunnen terugbellen? Betreft dit hetzelfde issue als een paar maanden geleden?
Groet, 5.1.2.e

Corporate Privacy Officer | Corporate Governance & Legal Services
Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e, Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317 5.1.2.e
www.wur.nl/disclaimer

Van: Privacy <privacy@wur.nl>
Verzonden: donderdag 7 oktober 2021 09:16
Aan: Privacy <privacy@wur.nl>; 5.1.2.e @wur.nl>
Onderwerp: Nieuwe datalekmelding | 10/7/2021 7:15:27 AM
Urgentie: Hoog

Beste collega,

Zojuist is er een nieuw datalek gemeld via het digitale meldformulier:

* * *

1. Geef een zo gedetailleerd mogelijke omschrijving van het incident
melding vanuit de wet poortwachter van medewerker, naam en afdeling worden in het bericht genoemd, die niet werkzaam is binnen mijn kenniseenheid (ik heb autorisatie voor alle meldingen binnen asg, niet buiten asg.

2. Wat is de aard van het incident?
automatisch gegenereerd bericht wat verstuurd is

3. Hoelang heeft het incident geduurd?
Eén dag

4a. Gedurende welke periode heeft het incident plaatsgevonden?

4b. Op welke datum heeft het incident plaatsgevonden?
2021-10-07

5. Van welke categorie personen zijn persoonsgegevens gelekt?
["Medewerkers"]

6. Van hoeveel personen zijn mogelijk persoonsgegevens gelekt?
ik heb bericht van 1 medewerker ontvangen. weet niet hoeveel medewerkers dit bericht hebben ontvangen

7. Op welke datum/tijdstip is het incident ontdekt?
7-10-2021

8. Wat voor soort persoonsgegevens zijn betrokken in het incident?
["NAW-gegevens","feit dat medewerker ziek is, snds wanneer en op welke afdeling werkzaam"]

9. Welke acties zijn ondernomen naar aanleiding van het incident?
Melding bij hoofd PSA 5.1.2.e

* * *

Met vriendelijke groet,
5.1.2.e

[redacted]
Corporate Privacy Officer | 5.1.2.e

Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317 5.1.2.e

Privacy

Van: 5.1.2.e
Verzonden: dinsdag 12 oktober 2021 08:29
Aan: Privacy
CC: 5.1.2.e
Onderwerp: RE: Datalekmelding 7 oktober jl.

Beste 5.1.2.e

Dank voor je uitgebreide toelichting.
Ik heb inmiddels ook binnen HR inmiddels het bericht langs zien komen dat inderdaad de email meldingen voorlopig uitstaan totdat een aanpassing is gedaan in het systeem.

Groeten,
5.1.2.e

Van: Privacy <privacy@wur.nl>
Verzonden: maandag 11 oktober 2021 10:15
Aan: 5.1.2.e @wur.nl>
CC: 5.1.2.e @wur.nl>
Onderwerp: RE: Datalekmelding 7 oktober jl.

Beste 5.1.2.e,

Hierbij gaat een verdere terugkoppeling naar aanleiding van jouw datalekmelding van 7 oktober jl. over het autorisatieissue bij de e-mailattendering over zieke medewerkers.

Wij hebben geconstateerd dat de HR-professionals die de e-mail ontvingen ook via DPI toegang hadden tot deze persoonsgegevens (NB: dit is onderdeel van een breder autorisatievraagstuk). De e-mailattendering aan de HR-professionals is echter ook een nieuwe verwerking en de informatie komt hierdoor ook in de inboxen van alle HR-professionals terecht die betrokken zijn geweest bij de interne loopbaan van de betreffende medewerkers. Dit betekent dat de betrokken medewerkers een groter risico lopen, bijv. als een onbevoegde zich toegang verschaft tot de e-mailbox van een 'inactieve' HR-professional terwijl de e-mail nog niet handmatig verwijderd is.

Wij hebben om die reden geadviseerd een tijdelijke maatregel te implementeren, hangende de verbetering van de functionaliteit door ADP. Ik begreep zojuist dat de e-mailattendering tijdelijk is uitgezet.

Vanwege het feit dat geen sprake is van een waarschijnlijkheid op negatieve gevolgen voor de betrokkenen hebben wij het incident in afstemming met de F-G niet gemeld bij de Autoriteit Persoonsgegevens of bij de betrokken medewerkers.

Tot slot wil ik je nogmaals bedanken voor jouw melding. Dit helpt ons om ons datalekkenregister compleet te houden en om tijdig actie te kunnen nemen. Mocht je nog vragen hebben of willen overleggen dan zijn wij daarvoor graag beschikbaar.

Vriendelijke groet,
5.1.2.e

[redacted]
Corporate Privacy Officer | Corporate Governance & Legal Services

Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317 5.1.2.e
www.wur.nl/disclaimer

Van: 5.1.2.e @wur.nl>
Verzonden: donderdag 7 oktober 2021 14:49
Aan: Privacy <privacy@wur.nl>
Onderwerp: RE: Datalekmelding 7 oktober jl.

Beste 5.1.2.e

Dank voor deze terugkoppeling.

Groeten,
5.1.2.e

Van: Privacy <privacy@wur.nl>
Verzonden: donderdag 7 oktober 2021 13:43
Aan: 5.1.2.e @wur.nl>
Onderwerp: Datalekmelding 7 oktober jl.

Beste 5.1.2.e

Bedankt voor je datalekmelding van vanmorgen.

Ik begrijp dat sprake is van een autorisatie-issue binnen de e-mailfunctionaliteit van ADP, waarbij e-mails rond ziekte worden verstuurd aan HR-collega's binnen WUR die ooit betrokken zijn geweest bij het dienstverband van de betreffende medewerkers.

Hier is sprake van een datalek in de zin van de AVG, omdat onbevoegden inzage krijgen in (gevoelige) persoonsgegevens waartoe zij niet geautoriseerd zijn. Dat dit veroorzaakt wordt door gebrekkige functionaliteit of een 'bug' doet daar niet aan af. Naar aanleiding van jouw melding heb ik contact gezocht met 5.1.2.e en hangende de discussie met HR-FAB kan ik je nog geen volledig uitsluitsel geven welke opvolging hieraan wordt gegeven.

Ik probeer hier op korte termijn bij je op terug te komen.

In de tussentijd nogmaals dank voor je melding.

Vriendelijke groet,
5.1.2.e

[redacted]
Corporate Privacy Officer | 5.1.2.e
Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e | Droevendaalsesteeg 4
6708 PB Wageningen
Tel. +31 317 5.1.2.e

5.1.2.e

Van: Privacy
Verzonden: maandag 29 maart 2021 14:27
Aan: Privacy; 5.1.2.e
Onderwerp: Nieuwe datalekmelding | 3/29/2021 12:26:33 PM | 5.1.2.e @wur.nl

Urgentie: Hoog

Beste collega,

Zojuist is er een nieuw datalek gemeld via het digitale meldformulier:

* * *

1. Geef een zo gedetailleerd mogelijke omschrijving van het incident
Bij de inrichting van de Optare Workflow is door een menselijke fout de inrichting van de signalen niet juist geconfigureerd. Dit heeft tot gevolg gehad dat er een e-mailsignalering is verstuurd aan een groep van ca. 495 medewerkers met een Professional Self Services (PSS)-rol. Die e-mails bevatten persoonsgegevens (naam, e-mailadres, werknemernummer, contracttype, aard van de taak (‘flexibele uitruil’)) van in totaal 5 medewerkers van WUR. Er is geen toegang tot andere informatie over de medewerker en geen sprake van verwerking van bijzondere persoonsgegevens. De ontvanger van de e-mails had ook geen toegang tot verdere informatie over de betreffende 5 medewerkers. De soort uitruil is ook niet benoemd in het mailbericht (uitsluitend: “aanvraag flexibele arbeidsvoorwaarden”). Deze signalering is verstuurd op 29 maart 2021.

2. Wat is de aard van het incident?
Inzage door onbevoegden

3. Hoelang heeft het incident geduurd?
Eén dag

4a. Gedurende welke periode heeft het incident plaatsgevonden?

4b. Op welke datum heeft het incident plaatsgevonden?
2021-03-29

5. Van welke categorie personen zijn persoonsgegevens gelekt?
["Medewerkers"]

6. Van hoeveel personen zijn mogelijk persoonsgegevens gelekt?
1

7. Op welke datum/tijdstip is het incident ontdekt?
29 maart 13:50 u

8. Wat voor soort persoonsgegevens zijn betrokken in het incident?
["NAW-gegevens"]

9. Welke acties zijn ondernomen naar aanleiding van het incident?
Analyse op aantal resterende transacties in de pijplijn waarvoor de signalering nog aan kan staan. Het automatisch versturen van de signaleringen is na de ontdekking op 18 maart voor nieuwe transacties uitgezet.

* * *

Met vriendelijke groet,
5.1.2.e

Corporate Privacy Officer | 5.1.2.e

Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e, Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317-5.1.2.e

Privacy

Van: 5.1.2.e
Verzonden: donderdag 7 oktober 2021 11:59
Aan: 5.1.2.e ; Privacy; 5.1.2.e
CC: HR functioneelbeheer; 5.1.2.e
Onderwerp: Fwd: Analyse 6 wekelijks gesprek reintegratie gesprek - data lek....

Zie hieronder, bug in ADP mailfunctionaliteit.
Werken aan oplossing.

Als de melding niet een mdw in jouw aandachtsgebied betreft mag je deze dus negeren, hij komt nl. ook bij de juiste collega.

Groet,5.1.2.e

Outlook voor Android downloaden

From: 5.1.2.e @wur.nl>
Sent: Thursday, October 7, 2021 11:51:22 AM
To: 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
Cc: HR functioneelbeheer <hr.functioneelbeheer@wur.nl>
Subject: Analyse 6 wekelijks gesprek reintegratie gesprek - data lek....

Dag allen!
5.1.2.e en ik hebben samen een en ander geanalyseerd. In ieder geval zijn wij van mening dat dit NIET als datalek gelabeld hoeft te worden!!

Wat is er aan de hand?

- In het kader van procesoptimalisatie heeft CHR FAB in overleg met het projectgroep “Verzuim en poortwachter traject” een aantal signalen ingericht/omgezet, zodat tijdig de verantwoordelijke actoren een seintje krijgen met een hele tekst en uitleg
- De inrichting is verder correct!
- 5.1.2.e en ik hebben geconcludeerd dat er toch een beperking zit in de functionaliteit van Workflow, deze zal ik verder toelichten.

Oorzaak van onterechte mail activiteit

Bij de inrichting van de Workflow kun je een aantal condities opgeven, zodat het systeem rekening kan houden dat een dergelijke workflow wel of niet gegenereerd moet worden. Tot nu toe bestond de inrichting van Workflow signalen voornamelijk uit taken, dus bepaalde rollen krijgen een taak in hun inbox.
We hebben geconstateerd dat er een verschil zit in functionaliteit van mail activiteit en bij de taak activiteit wat betreft verzuim/re-integratietraject. In tegenstelling tot een “taak activiteit” houdt Workforce geen rekening mee met de mail functie v.w.b. inactieve contracten! Bij het genereren van de signalen voor zes wekelijkse gesprek, waarbij ook een mail activiteit van toepassing is, de hele data screent op medewerkerniveau en niet o.b.v. actieve contract. Als een medewerker ooit bij een Sciencesgroup heeft gewerkt (intern of extern contract) wordt deze mail alsnog aan alle professionals (HRO/HRADV) verstuurd. Op dit moment kunnen we helaas aan de inrichting niet veel aan sleutelen, hooguit de mailfunctie uitzetten. Wij beschouwen dit als een BUG in het systeem en zullen z.s.m. dit melden bij ADP!

Wel of geen datalek?

Het FAB team is van mening dat dit NIET als een datalek moet worden beschouwd! Alle professionals (HRO/HRadviseurs) hebben sowieso in DPI toegang tot heel HR WUR data, dus ook daar zou de historie kunnen inzien. Wel zijn we het mee eens dat dit niet een handige werkwijze. Wat betreft MSS

rollen, daar hebben we geen onterechte zaken kunnen constateren. De mail is aan de juiste MSS rollen bezorgd en niet voor de inactieven!
Alle HRO en HR adviseur die deze mail niet hadden moeten ontvangen, graag negeren!
Vraag aan 5.1.2.e / EES team, moeten we de mailfunctie nu tijdelijk uitzetten? Wat we ook kunnen doen is om mail activiteit om te bouwen in taak activiteit, zodat de signalering als een taak in de Inbox komt.
Op dit moment staat de teller van het aantal gegenereerde signalen op 20 sinds 01-10-2021 (live datum van Workflow)
Groet,
5.1.2.e

Van: 5.1.2.e @wur.nl>
Verzonden: donderdag 7 oktober 2021 09:13
Aan: HR functioneelbeheer <hr.functioneelbeheer@wur.nl>
Onderwerp: Fwd: 6 wekelijks gesprek reintegratie gesprek - data lek....
Help!?
Outlook voor Android downloaden

From: 5.1.2.e @wur.nl>
Sent: Thursday, October 7, 2021 8:31:41 AM
To: 5.1.2.e @wur.nl>
Subject: FW: 6 wekelijks gesprek reintegratie gesprek - data lek....
Hee hai, binnen asg krijgen we deze melding.... is van SSG dus zou niet bij ons (en wie weet wie nog meer...) binnen mogen komen denk ik?
Groeten,
5.1.2.e

Van: noreply@adp.nl <noreply@adp.nl>
Verzonden: donderdag 7 oktober 2021 3:34
Aan: 5.1.2.e @wur.nl>
Onderwerp: 6 wekelijks gesprek reintegratie gesprek
English below

Beste Leidinggevende,

Medewerker 5.1.2.e is minimaal 12 weken (gedeeltelijk) ziek en er is reeds n.a.v. de probleemanalyse een eerste Plan van Aanpak opgesteld.

Na het opstellen van een Plan van Aanpak dient er volgens de Wet verbetering Poortwachter tenminste elke zes weken een re-integratiegesprek plaats te vinden tussen de medewerker en de leidinggevende. Hiervan moet een kort verslag worden gemaakt. Bij wijzigingen op het oorspronkelijke Plan van aanpak, moet er een evaluatie van het Plan van aanpak worden ingevuld en dit moet wederom worden toegevoegd aan het digitale re-integratiedossier (dido).

Dit periodieke gesprek blijft terugkeren tot het moment dat het re-integratietraject wordt beëindigd, hetzij wegens hervatting van werkzaamheden of wegens aanvraag van een WIA-uitkering.

Er staat een Workforcetaak met directe toegang naar het benodigde document voor je klaar in je inbox van MyHR.

Als leidinggevende kunnen de volgende stappen in de MyHR inbox worden gevolgd
· Dit bericht openen
· Document aanmaken
· Samen invullen
· Opslaan op je schijf
· Printen en beide tekenen (als dit niet fysiek kan, dan graag een akkoord mail bijvoegen van beide partijen)

Je kan dit formulier elke keer dat het van toepassing is zelf uploaden in MyHR via deze taak of je stuurt het

naar de HR-supportafdeling van jouw kenniseenheid. Het signaal kan worden afgesloten nadat het document middels de upload in deze taak aan het dossier is toegevoegd.

Loonsanctie bij onvoldoende re-integratie-inspanningen
Vanuit de Wet verbetering Poortwachter zijn we als werkgever verplicht om samen met de medewerker te zorgen dat deze zo snel mogelijk weer aan het werk kan met een goed plan van aanpak en opvolging hiervan. Is het UWV van mening dat wij onvoldoende inspanningen hebben gedaan hierin, dan kan het UWV ons verplichten om na twee verzuimjaren nog een jaar het loon van de medewerker door te betalen.

We adviseren je daarom om het re-integratiedossier altijd tijdig en goed bij te houden.

Uiteraard kun je altijd voor advies en ondersteuning contact opnemen met je HR Adviseur.

Met vriendelijke groet,
HR Servicedesk

Dear supervisor,

Employee 5.1.2.e [redacted] has been (partially) sick for at least 12 weeks and an initial Action Plan has already been drawn up based on the Problem Analysis.

After an Action Plan has been drawn up, a reintegration conversation must be had between the employee and the supervisor at least once every six weeks, according to the Wet Verbetering Poortwachter (Eligibility for Permanent Invalidity Benefit (Restrictions) Act).

A short report of this meeting must be submitted. If changes have been enacted in original Action Plan, an evaluation of the Plan must be completed and must again be added to the digital reintegration file.

This periodic conversation will continue until the reintegration process is terminated, either due to work resumption or an application for WIA benefits.

A Workforce task with direct access to the required document is waiting for you in your MyHR inbox.

As a supervisor, the following steps can be taken in the MyHR inbox
· Open this message
· Create document
· Fill in together
· Save it to your drive
· Print and sign both (if this is not possible physically, please enclose a consent e-mail from both parties)

You can upload this form in MyHR yourself via this task whenever it is applicable, or send it to the HR Support department of your knowledge unit. The reminder can be closed after the document has been added to the file by uploading it in this task.

Salary penalty for insufficient reintegration efforts
Under the Wet Verbetering Poortwachter (Eligibility for Permanent Invalidity Benefit (Restrictions) Act), we, as employers, are obliged to, together with the employee, ensure that they can return to work as soon as possible with a good Action Plan and follow-up. If the UWV is of the opinion that we have made insufficient efforts in this respect, the UWV may oblige us to continue paying the employee's salary for another year after two years of illness.

We therefore strongly advise you to always keep the reintegration file meticulously updated. Of course, you can always contact your HR Adviser for advice and support.

Kind regards,
HR Service Desk

5.1.2.e

Van: 5.1.2.e
Verzonden: woensdag 24 maart 2021 09:15
Aan: 5.1.2.e
Onderwerp: RE: Nieuwe datalekmelding | 3/24/2021 7:47:27 AM | 5.1.2.e @wur.nl

Dank en doe ik!

Met vriendelijke groet/ Kind regards,

5.1.2.e
+31(0)6 5.1.2.e
Afw op wo-mi en vrij-ocht
Absent on Wed afternoons and Fri mornings

CC-mail gaat naar een aparte folder en lees ik onregelmatig
CC-mail is filtered by a rule and read at irregular intervals

---

Van: 5.1.2.e @wur.nl>
Verzonden: Wednesday, March 24, 2021 8:50 AM
Aan: 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
Onderwerp: FW: Nieuwe datalekmelding | 3/24/2021 7:47:27 AM | 5.1.2.e @wur.nl
Urgentie: Hoog

Ter info hieronder de registratie van het incident in ons datalekkenregister. Bedankt voor je vlotte reactie.

Mocht er in de toekomst nog eens een incident zijn waarbij je twijfelt of sprake is van een datalek, neem dan vooral contact op met 5.1.2.e of meld het via de oranje meldknop op https://intranet.wur.nl/umbraco/nl/over-wur/beleid-regelingen/privacy-persoonsgegevens/.

Groet, 5.1.2.e

[redacted] Corporate Governance & Legal Services

Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317-5.1.2.e
www.wur.nl/disclaimer

Van: Privacy <privacy@wur.nl>
Verzonden: woensdag 24 maart 2021 08:48
Aan: Privacy <privacy@wur.nl>; 5.1.2.e @wur.nl>
Onderwerp: Nieuwe datalekmelding | 3/24/2021 7:47:27 AM | 5.1.2.e @wur.nl
Urgentie: Hoog

Beste collega,

Zojuist is er een nieuw datalek gemeld via het digitale meldformulier:

* * *

1. Geef een zo gedetailleerd mogelijke omschrijving van het incident
Bij de inrichting van de Optare Workflow is door een menselijke fout de inrichting van de signalen niet juist geconfigureerd. Dit heeft tot gevolg gehad dat e-mailsignaleringen zijn verstuurd aan een groep van ca. 495 medewerkers met een Professional Self Services (PSS)-rol. Die e-mails bevatten persoonsgegevens (naam, e-mailadres, werknemernummer, contracttype, aard van de taak (‘flexibele uitruil’)) van in totaal 5 medewerkers van WUR. Er is geen toegang tot andere informatie over de medewerker en geen sprake van verwerking van bijzondere persoonsgegevens. De ontvanger van de e-mails had ook geen toegang tot verdere informatie over de betreffende 5 medewerkers. De soort uitruil is ook niet benoemd in het mailbericht (uitsluitend: “aanvraag flexibele arbeidsvoorwaarden”). Deze signaleringen zijn verstuurd op 18 maart 2021. Het automatisch versturen van de signaleringen is na de ontdekking uitgezet. Het incident is vandaag binnen CHR geëvalueerd en CHR zal borgen dat de inrichting van signalen voortaan zorgvuldiger en met meer differentiatie gebeurt.

2. Wat is de aard van het incident?
Inzage door onbevoegden

3. Hoelang heeft het incident geduurd?
Eén dag

4a. Gedurende welke periode heeft het incident plaatsgevonden?

4b. Op welke datum heeft het incident plaatsgevonden?
2021-03-18

5. Van welke categorie personen zijn persoonsgegevens gelekt?
["Medewerkers"]

6. Van hoeveel personen zijn mogelijk persoonsgegevens gelekt?
5

7. Op welke datum/tijdstip is het incident ontdekt?
18 maart 2021

8. Wat voor soort persoonsgegevens zijn betrokken in het incident?
["NAW-gegevens"]

9. Welke acties zijn ondernomen naar aanleiding van het incident?
Het automatisch versturen van de signaleringen is na de ontdekking uitgezet. Het incident is vandaag binnen CHR geëvalueerd en CHR zal borgen dat de inrichting van signalen voortaan zorgvuldiger en met meer differentiatie gebeurt.

* * *

Met vriendelijke groet,
5.1.2.e

[redacted]
Corporate Privacy Officer | 5.1.2.e

Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317 5.1.2.e

5.1.2.e

Van: 5.1.2.e
Verzonden: dinsdag 23 maart 2021 18:57
Aan: Functionarisgegevensbescherming
Onderwerp: FW: Herinnering: beoordelen flexibele arbeidsvoorwaarden

Ter info.

5.1.2.e
Corporate Governance & Legal Services

Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e, Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317 5.1.2.e
www.wur.nl/disclaimer

Van: 5.1.2.e @wur.nl>
Verzonden: dinsdag 23 maart 2021 17:26
Aan: 5.1.2.e @wur.nl>
CC: 5.1.2.e @wur.nl>
Onderwerp: RE: Herinnering: beoordelen flexibele arbeidsvoorwaarden

Dag 5.1.2.e

2 kleine aanpassinkjes, zie hieronder geel gearceerd.

Met vriendelijke groet/ Kind regards,

5.1.2.e
+31(0)6 5.1.2.e
Afw op wo-mi en vrij-ocht
Absent on Wed afternoons and Fri mornings

CC-mail gaat naar een aparte folder en lees ik onregelmatig
CC-mail is filtered by a rule and read at irregular intervals

---

Van: 5.1.2.e @wur.nl>
Verzonden: Tuesday, March 23, 2021 5:13 PM
Aan: 5.1.2.e @wur.nl>
CC: 5.1.2.e @wur.nl>
Onderwerp: RE: Herinnering: beoordelen flexibele arbeidsvoorwaarden

Dag 5.1.2.e

Wat mij betreft op zich helder. Begrijp ik vraag 1 goed dat het de betreffende medewerker van CSA dus de medewerkers van AFSG en SSG in zijn 'subset' moeten hebben staan?

Vat ik het dan zo goed samen:

> Bij de inrichting van de Optare Workflow is door een menselijke fout de inrichting van de signalen niet juist geconfigureerd. Dit heeft tot gevolg gehad dat e-mailsignaleringen zijn verstuurd aan een groep van ca. ~~650~~ 495 medewerkers met een Professional Self Services (PSS)-rol. Die e-mails bevatten persoonsgegevens (naam, e-mailadres, werknemernummer, contracttype, aard van de taak ('flexibele uitruil')) van in totaal 5 medewerkers van WUR. Er is

geen toegang tot andere informatie over de medewerker en geen sprake van verwerking van bijzondere persoonsgegevens. De ontvanger van de e-mails had ook geen toegang tot verdere informatie over de betreffende 5 medewerkers. De soort uitruil is ook niet benoemd in het mailbericht (uitsluitend: "aanvraag flexibele arbeidsvoorwaarden"). Deze signaleringen zijn verstuurd op 18 maart 2021. Het automatisch versturen van de signaleringen is na de ontdekking uitgezet. Het incident is vandaag binnen CHR geëvalueerd en CHR zal borgen dat de inrichting van signalen voortaan zorgvuldiger en met meer differentiatie gebeurt.

Ik neem even met 5.1.2.e op te kijken of wij ook vanuit privacy kunnen bijdragen aan de op opschoning van bestaande autorisaties en inrichting van signaleringen. Mocht je nog aanvullingen hebben op mijn samenvatting (die registreer ik in ons *interne* datalekkenregister) dan hoor ik het graag!

Groet, 5.1.2.e

[redacted] Corporate Governance & Legal Services

Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e, Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317-5.1.2.e
www.wur.nl/disclaimer

Van: 5.1.2.e @wur.nl>
Verzonden: maandag 22 maart 2021 09:45
Aan: 5.1.2.e @wur.nl>
CC: 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>; HR functioneelbeheer <hr.functioneelbeheer@wur.nl>; Functionarisgegevensbescherming <functionarisgegevensbescherming@wur.nl>; 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
Onderwerp: RE: Herinnering: beoordelen flexibele arbeidsvoorwaarden
Urgentie: Hoog

Dag 5.1.2.e

Hierbij cfm tel afspraak vrijdag alsnog de beantwoording van de vragen:
Er zijn in totaal over 5 Optare (Flex Ben) transacties van medewerkers mailberichten (signalen) verstuurd.

1. De email berichten zijn verstuurd naar iedereen binnen de WUR organisatie met een PSS (zogenaamde professional) rol binnen ADP Workforce, die de aangegeven medewerker in zijn/haar subset heeft staan. De subset is afhankelijk van afdeling en daarbij behorende rechten. Dit was een menselijke fout in de inrichting van de signalen.
2. De inhoud van het bericht was voor iedereen gelijk aan het aangegeven bericht; er is geen toegang tot andere informatie over de medewerker. De soort uitruil (bijv Vakbond) wordt niet benoemd in het mailbericht.
3. ADP heeft dit niet bij ons gemeld, omdat het geen ADP fout betreft. Het betreft een instelling in de inrichting van de Optare workflows die vanaf 11 maart open zijn gezet voor de medewerkers. Deze instelling is inmiddels uitgezet. De lopende aanvragen (vanaf 11-3-2021 t/m 18-3-2021) worden nu verwerkt. Als de verwerking door de PSA medewerkers is uitgevoerd, vervallen deze meldingen. Dit is na 5 mailtjes geëffectueerd.

We hebben dit vandaag intern geëvalueerd en zullen borgen dat de inrichting van signalen voortaan zorgvuldiger en met meer differentiatie gebeurt.

Is dit voor nu afdoende?

Met vriendelijke groet/ Kind regards,

5.1.2.e **Manager Shared Service Centre Human Resources a.i.**
Wageningen University & Research
Wageningen Campus - Droevendaalsesteeg 4 - gebouw Atlas 104
Postbus 9101, 6700 HB Wageningen

T +31 5.1.2.e
M +31 5.1.2.e
E-mail 5.1.2.e @wur.nl
http://www.wur.nl
http://www.wur.nl/nl/Disclaimer.htm
Afwezig op woensdagmiddag en vrijdagochtend
Absent on Wednesday afternoons and Friday mornings

CC-mail gaat naar een aparte folder en lees ik onregelmatig
CC-mail is filtered by a rule and read on an irregular basis

Van: 5.1.2.e @wur.nl>
Verzonden: Friday, March 19, 2021 11:30 AM
Aan: 5.1.2.e @wur.nl>
CC: 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>; HR functioneelbeheer <hr.functioneelbeheer@wur.nl>; Functionarisgegevensbescherming <functionarisgegevensbescherming@wur.nl>; 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
Onderwerp: RE: Herinnering: beoordelen flexibele arbeidsvoorwaarden

Dag 5.1.2.e

Dank voor je bericht. Ik signaleer dit incident omdat onze F-G meerdere datalekmeldingen krijgt vanuit de organisatie en wij daar niet op kunnen reageren omdat wij niet op de hoogte zijn gesteld.

Zodra sprake is van onbevoegde verwerking is sprake van een datalek in de zin van de AVG, ongeacht de oorzaak (bijv. te ruim ingerichte autorisaties of het doorsturen aan de verkeerde 5.1.2.e). De beoordeling of bij een incident sprake is van een datalek ligt daarom bij privacy. Als iedereen in de organisatie zelf gaat beoordelen of sprake is van een meldplichtig incident en besluit zaken niet bij ons te melden lopen wij daarmee compliancerisico's. Daarom bij twijfel: melden.

In dit geval zijn e-mailattenderingen verstuurd met persoonsgegevens (naam, e-mailadres, werknemernummer en contracttype, aard van de taak ('flexibele uitruil')). Die attenderingen zijn terecht gekomen bij personen die die gegevens niet hadden moeten krijgen (bijv. iemand van CSA die attenderingen krijgt over medewerkers bij AFSG en SSG). Ik begrijp uit jouw bericht dat dit komt omdat de autorisaties in DPI niet goed ingericht kunnen worden. Eerder begreep ik ook dat dit komt door een menselijke fout (die herinneringen waren niet goed ingericht). Hoe dan ook zou dit nooit moeten kunnen gebeuren. Nu gaat het niet om bijzondere persoonsgegevens, maar bij sommige soorten uitruil wel (bijv. vakbond). Het is voor onze beoordeling alsnog nuttig om antwoord te krijgen op de vragen in mijn e-mail hieronder. Zou jij dit alsnog willen oppakken?

Mocht je het hier niet mee eens zijn dan kun je altijd contact opnemen met de F-G (in de cc.).

Bedankt alvast!

Groet, 5.1.2.e
5.1.2.e

5.1.2.e | Corporate Governance & Legal Services

Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e Droevendaalsesteeg 4, 6708 PB Wageningen

Tel. 0317[redacted]
www.wur.nl/disclaimer

Van: [redacted]@wur.nl>
Verzonden: vrijdag 19 maart 2021 09:47
Aan: [redacted]@wur.nl>
CC: [redacted]@wur.nl>; [redacted]@wur.nl>; HR functioneelbeheer <hr.functioneelbeheer@wur.nl>; Privacy <privacy@wur.nl>; Functionarisgegevensbescherming <functionarisgegevensbescherming@wur.nl>; [redacted]@wur.nl>; [redacted]@wur.nl>
Onderwerp: FW: Herinnering: beoordelen flexibele arbeidsvoorwaarden
Urgentie: Hoog

Goedemorgen allen,

Dank voor de attente signalering; er is hier nadrukkelijk geen sprake van een datalek, omdat het systeem en de autorisaties werken zoals ontworpen.

Deze transacties stonden nl. inderdaad een week open bij de PSS-rol (Professional Self Services, bedoeld voor HR Professionals), omdat men met de maandafsluiting van maart bezig was en daarom is er een " escalatiesignaal" gegaan naar iedereen die deze rol heeft.
Weliswaar zijn de autorisaties voor de PSS (Professional Self Services, HR Professionals) m.i. te ruim toebedeeld in de organisatie en daarom zijn de mailtjes naar veel personen gegaan.
Dit heeft te maken met het autorisatiemodel, naar ik gisteren begreep heeft men de PSS rol nodig om in DPI management-informatie te kunnen opvragen.

Herontwerp van het autorisatiemodel incl opschoning van bestaande autorisaties staat op onze backlog en vraagt een inspanning van de organisatie bedrijfsvoering-breed.

De signalen zijn voor nieuwe transacties uitgezet en de transacties worden verwerkt zodat de mailtjes voor deze transacties in de pijplijn niet meer worden getriggerd.

Excuses voor eventueel ongemak en nogmaals dank voor de alertheid.

Met vriendelijke groet/ Kind regards,

[redacted] **Manager Shared Service Centre Human Resources a.i.**
Wageningen University & Research
Wageningen Campus - Droevendaalsesteeg 4 - gebouw Atlas 104
Postbus 9101, 6700 HB Wageningen
T +31 ([redacted]
M +31 [redacted]
E-mail [redacted]@wur.nl
http://www.wur.nl
http://www.wur.nl/nl/Disclaimer.htm
Afwezig op woensdagmiddag en vrijdagochtend
Absent on Wednesday afternoons and Friday mornings

CC-mail gaat naar een aparte folder en lees ik onregelmatig
CC-mail is filtered by a rule and read on an irregular basis

WAGENINGEN
UNIVERSITY & RESEARCH

Van: Privacy <privacy@wur.nl>
Verzonden: donderdag 18 maart 2021 14:01
Aan: 5.1.2.e @wur.nl>
CC: 5.1.2.e @wur.nl>; Functionarisgegevensbescherming <functionarisgegevensbescherming@wur.nl>
Onderwerp: FW: Herinnering: beoordelen flexibele arbeidsvoorwaarden
Urgentie: Hoog

Ha 5.1.2.e

Zoals zojuist besproken. Hieronder en bijgaand een bericht van een medewerker van CSA waarin hij e-mails krijgt van medewerkers buiten zijn afdeling (CSA) – iemand van SSG en iemand van AFSG. Mijn specifieke vragen aan jou zijn:

1. Hoe kan het dat iemand van CSA een bericht krijgt over medewerkers buiten zijn eigen groep?
2. Is in alle gevallen ten hoogste in de herinnering opgenomen: "aanvraag flexibele arbeidsvoorwaarden van [naam] (werknemernummer [ ] – [contract])"?
3. Heeft ADP dit bij ons gemeld en hebben zij zelf actie ondernomen?

Ter verdere toelichting:

Het is een datalek omdat sprake is van onbevoegde kennisname van informatie over de betreffende natuurlijke personen (de AVG geeft aan dat sprake is van een datalek bij een inbreuk die "per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens;").

Bij de beoordeling of het gemeld moet worden bij de toezichthouder komt pas de vraag op of er sprake is van een waarschijnlijkheid op negatieve effecten voor de betrokkenen. Bij bijzondere persoonsgegevens (zoals zwangerschap / vakbondlidmaatschap) is dat in beginsel altijd het geval, maar in dit geval waarschijnlijk niet (maar dat hangt ook af van het antwoord op vraag 2).

Ik hoor graag terug!

Groet, 5.1.2.e

Corporate Privacy Officer | 5.1.2.e

Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e, Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317-5.1.2.e
www.wur.nl/disclaimer

Van: Functionarisgegevensbescherming <functionarisgegevensbescherming@wur.nl>
Verzonden: donderdag 18 maart 2021 11:33
Aan: 5.1.2.e @wur.nl>;5.1.2.e @wur.nl>
Onderwerp: FW: Herinnering: beoordelen flexibele arbeidsvoorwaarden
Urgentie: Hoog

Belangrijke info

Met vriendelijke groet,

5.1.2.e

5.1.2.e Functionaris Gegevensbescherming | Wageningen University & Research | Postbus 9101, 6700 HB Wageningen | +31 (0)317 5.1.2.e www.wur.nl

---

From: CSA <CSA@wur.nl>
Sent: Thursday, March 18, 2021 11:08 AM
To: 5.1.2.e @wur.nl>
Subject: FW: Herinnering: beoordelen flexibele arbeidsvoorwaarden
Importance: High

Ha 5.1.2.e

Ik krijg onderstaande HRM gerelateerd bericht toegestuurd?
Lijkt me niet de bedoeling #datalekpersoonsgegevens en ik zal het ook even bij HRM melden.

Grtz

CSA

From: noreply@adp.nl <noreply@adp.nl>
Sent: Thursday, March 18, 2021 10:45 AM
To: CSA
Subject: Herinnering: beoordelen flexibele arbeidsvoorwaarden
Importance: High

Beste CSA,

In uw Inbox staat een aanvraag flexibele arbeidsvoorwaarden van SSG (werknemernummer X - contract 1) reeds een week klaar om door u in behandeling te worden genomen. Bij deze het verzoek deze taak (nummer: 561578) zo spoedig mogelijk af te handelen.

Het is mogelijk dat de taak reeds is afgehandeld door een gebruiker met dezelfde rechten waardoor deze niet meer in de Inbox aanwezig is.

Privacy

Van: Privacy
Verzonden: woensdag 7 april 2021 15:16
Aan: Functionarisgegevensbescherming
CC: 5.1.2.e
Onderwerp: RE: Herinnering: beoordelen flexibele arbeidsvoorwaarden

Ha 5.1.2.e
Het gaat hier steeds om 'oude' meldingen waar de signaleringsfunctie niet goed voor was ingericht. In totaal resteren nog ca. 50 van dit soort meldingen. Inmiddels kunnen die 'oude' meldingen door de collega's die ze moeten afhandelen goed worden onderscheiden (er staat een geel/rood vlaggetje voor).
De opties om het probleem op te lossen zijn:

1. Benaderen van de resterende 50 medewerkers om hun melding terug te trekken
2. Sneller afhandelen van de binnengekomen meldingen

Vanuit het oogpunt van proportionaliteit en kosten/baten hebben 5.1.2.e en ik zojuist de volgende werkafspraak gemaakt:

1) Iedere dag wordt gecheckt of er meldingen conform het 'oude' signaleringsregime zijn binnengekomen. Die meldingen worden z.s.m. afgehandeld, maar in ieder geval zodanig tijdig dat er geen signalering uit kan gaan.
2) Als dit niet werkt en er sijpelt alsnog een signalering doorheen dan worden de resterende <50 medewerkers individueel benaderd om hun melding terug te trekken.

Groet, 5.1.2.e

Corporate Privacy Officer | 5.1.2.e
Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317 5.1.2.e
www.wur.nl/disclaimer

Van: Functionarisgegevensbescherming <functionarisgegevensbescherming@wur.nl>
Verzonden: woensdag 7 april 2021 14:08
Aan: 5.1.2.e @wur.nl>; Privacy <privacy@wur.nl>; 5.1.2.e @wur.nl>
CC: HR functioneelbeheer <hr.functioneelbeheer@wur.nl>; 5.1.2.e @wur.nl>
Onderwerp: RE: Herinnering: beoordelen flexibele arbeidsvoorwaarden

Hierbij nog twee stuks.
Met vriendelijke groet,

5.1.2.e

WAGENINGEN UNIVERSITY & RESEARCH

5.1.2.e | Functionaris Gegevensbescherming | Wageningen University & Research | Postbus 9101, 6700 HB Wageningen | +31 (0)317 5.1.2.e | www.wur.nl

---

From: Functionarisgegevensbescherming
Sent: Wednesday, April 07, 2021 1:44 PM
To: 5.1.2.e @wur.nl>; Privacy <privacy@wur.nl>; 5.1.2.e @wur.nl>
Cc: HR functioneelbeheer <hr.functioneelbeheer@wur.nl>; 5.1.2.e @wur.nl>
Subject: RE: Herinnering: beoordelen flexibele arbeidsvoorwaarden

Beste 5.1.2.e
Bijgaande mail is alweer van een paar dagen geleden. Ook nasleep?!
Geheel met 5.1.2.e eens. Als dit niet professioneel kan worden opgelost dan zullen we het anders moeten aanvliegen.

Hoeveel 'oude' transacties staan er nog open? Is dat na te gaan?
Met vriendelijke groet,

5.1.2.e

WAGENINGEN
UNIVERSITY & RESEARCH

5.1.2.e | Functionaris Gegevensbescherming | Wageningen University & Research | Postbus 9101, 6700 HB Wageningen | +31 (0)317 5.1.2.e | www.wur.nl

---

From: 5.1.2.e @wur.nl>
Sent: Wednesday, April 07, 2021 1:23 PM
To: Privacy <privacy@wur.nl>
Cc: Functionarisgegevensbescherming <functionarisgegevensbescherming@wur.nl>; HR functioneelbeheer <hr.functioneelbeheer@wur.nl>; 5.1.2.e @wur.nl>
Subject: Re: Herinnering: beoordelen flexibele arbeidsvoorwaarden

Is helaas nog nasleep, niets anders aan te doen dan zsm de oude transacties met dit signaal erop afhandelen...

Outlook voor Android downloaden

From: Privacy <privacy@wur.nl>
Sent: Wednesday, April 7, 2021 1:08:03 PM
To: 5.1.2.e @wur.nl>
Cc: Functionarisgegevensbescherming <functionarisgegevensbescherming@wur.nl>; HR functioneelbeheer <hr.functioneelbeheer@wur.nl>; 5.1.2.e @wur.nl>
Subject: RE: Herinnering: beoordelen flexibele arbeidsvoorwaarden

Ha 5.1.2.e collega's van HR functioneelbeheer,
Op een gegeven moment moet deze notificatiefunctie uitgezet worden totdat volledig uitgezocht is hoe dit steeds kan en hoe dit in de toekomst voorkomen kan worden. Voor mij is dat moment inmiddels aangebroken; dit is de derde melding in twee weken tijd.
Kunnen jullie met prioriteit aandacht aan dit defect besteden?
Groet, 5.1.2.e

Corporate Privacy Officer 5.1.2.e
Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e, Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317-5.1.2.e
www.wur.nl/disclaimer

Van: 5.1.2.e @wur.nl>
Verzonden: woensdag 7 april 2021 13:02
Aan: Privacy <privacy@wur.nl>
Onderwerp: Fwd: Herinnering: beoordelen flexibele arbeidsvoorwaarden

Ben nu vrij maar wederom eenzelfde datalek, zucht.
Outlook voor Android downloaden

From: noreply@adp.nl <noreply@adp.nl>
Sent: Wednesday, April 7, 2021 12:27:34 PM
To: 5.1.2.e @wur.nl>
Subject: Herinnering: beoordelen flexibele arbeidsvoorwaarden

Beste 5.1.2.e ,

In uw Inbox staat een aanvraag flexibele arbeidsvoorwaarden van 5.1.2.e reeds een week klaar om door u in behandeling te worden genomen. Bij deze het verzoek deze taak (nummer: 564316) zo spoedig mogelijk af te handelen.

Het is mogelijk dat de taak reeds is afgehandeld door een gebruiker met dezelfde rechten waardoor deze niet meer in de Inbox aanwezig is.

5.1.2.e

Van: 5.1.2.e
Verzonden: donderdag 18 maart 2021 13:44
Aan: Functionarisgegevensbescherming; 5.1.2.e
Onderwerp: RE: Herinnering: beoordelen flexibele arbeidsvoorwaarden

Ha 5.1.2.e ,

Ik begrijp van 5.1.2.e dat er onterechte e-mailherinneringen zijn uitgestuurd door ADP bij de inrichting van ADP online. De inhoud van die herinneringen is niet anders dan onderstaande (dus geen andere tekst dan "aanvraag flexibele arbeidsvoorwaarden" + naam medewerker).

5.1.2.e gaf aan dat de e-mails zijn ontvangen door personen die binnen een bepaalde afdeling een bepaalde rol hebben toebedeeld gekregen in Workforce. Het is wat dat betreft vreemd dat 5.1.2.e een bericht krijgt van iemand van SSG, maar misschien is hij voor heel WUR geautoriseerd.

Ik stem vanmiddag nog even kort met 5.1.2.e af en zal 5.1.2.e morgen even bellen om te kijken of wij nu volledige helderheid hebben over dit incident en wat we eventueel nog aan acties moeten ondernemen.

Groet, 5.1.2.e

[redacted] Corporate Governance & Legal Services

Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e, Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317 5.1.2.e
www.wur.nl/disclaimer

Van: Functionarisgegevensbescherming <functionarisgegevensbescherming@wur.nl>
Verzonden: donderdag 18 maart 2021 11:33
Aan: 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
Onderwerp: FW: Herinnering: beoordelen flexibele arbeidsvoorwaarden
Urgentie: Hoog

Belangrijke info

Met vriendelijke groet,

5.1.2.e

WAGENINGEN UNIVERSITY & RESEARCH

5.1.2.e | Functionaris Gegevensbescherming | Wageningen University & Research | Postbus 9101, 6700 HB Wageningen | +31 (0)317 5.1.2.e www.wur.nl

From: 5.1.2.e @wur.nl>
Sent: Thursday, March 18, 2021 11:08 AM
To: 5.1.2.e @wur.nl>
Subject: FW: Herinnering: beoordelen flexibele arbeidsvoorwaarden
Importance: High

Ha 5.1.2.e

Ik krijg onderstaande HRM gerelateerd bericht toegestuurd?
Lijkt me niet de bedoeling #datalekpersoonsgegevens en ik zal het ook even bij HRM melden.

Grtz

5.1.2.e

From: noreply@adp.nl <noreply@adp.nl>
Sent: Thursday, March 18, 2021 10:45 AM
To: 5.1.2.e @wur.nl>
Subject: Herinnering: beoordelen flexibele arbeidsvoorwaarden
Importance: High

Beste 5.1.2.e

In uw Inbox staat een aanvraag flexibele arbeidsvoorwaarden van 5.1.2.e reeds een week klaar om door u in behandeling te worden genomen. Bij deze het verzoek deze taak (nummer: 561578) zo spoedig mogelijk af te handelen.

Het is mogelijk dat de taak reeds is afgehandeld door een gebruiker met dezelfde rechten waardoor deze niet meer in de Inbox aanwezig is.

Privacy

Van: 5.1.2.e
Verzonden: donderdag 18 maart 2021 15:29
Aan: Privacy; 5.1.2.e
CC: Functionarisgegevensbescherming
Onderwerp: RE: Herinnering: beoordelen flexibele arbeidsvoorwaarden

Hallo 5.1.2.e

De meldingen zijn inderdaad al uitgezet.

P.s. Graag alle mailwisselingen verzenden naar HR.Functioneelbeheer@wur.nl. Mijn collega's zijn de ook meteen van op de hoogte.

Groet,

5.1.2.e

Van: Privacy <privacy@wur.nl>
Verzonden: donderdag 18 maart 2021 14:32
Aan: 5.1.2.e @wur.nl>
CC: 5.1.2.e @wur.nl>; Functionarisgegevensbescherming <functionarisgegevensbescherming@wur.nl>
Onderwerp: RE: Herinnering: beoordelen flexibele arbeidsvoorwaarden

Ha 5.1.2.e

Nog even voor de goede orde, ik ga ervan uit dat als er bij ons of ADP iets moet gebeuren om de herinneringen uit te zetten, dat al in gang gezet is (en niet dat we op morgen hoeven te wachten). Het laatste bericht dat ik bijvoegde was van 12.15 uur.

Groet, 5.1.2.e

[redacted]
Corporate Privacy Officer 5.1.2.e

Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e, Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317-5.1.2.e
www.wur.nl/disclaimer

Van: 5.1.2.e @wur.nl>
Verzonden: donderdag 18 maart 2021 14:27
Aan: Privacy <privacy@wur.nl>
CC: 5.1.2.e @wur.nl>
Onderwerp: RE: Herinnering: beoordelen flexibele arbeidsvoorwaarden

Hallo 5.1.2.e

Ik heb je vraag doorgestuurd naar hr.functioneelbeheer@wur.nl + 5.1.2.e .

Uiterlijk morgen zullen we je een reactie geven.

Met vriendelijke groet/Kind regards,

5.1.2.e
Functioneel Applicatiebeheerder CHR

Aanwezig: maandag t/m vrijdag
Wageningen University & Research
Corporate HR - Shared Service Center
Postbus 9101, 6700 HB Wageningen
Wageningen Campus - Gebouw 104 (Atlas)
Droevendaalsesteeg 4, 6708 PB Wageningen
T: 0317-5.1.2.e
E: 5.1.2.e @wur.nl
www.disclaimer-nl.wur.nl

Van: Privacy <privacy@wur.nl>
Verzonden: donderdag 18 maart 2021 14:02
Aan: 5.1.2.e @wur.nl>
CC: 5.1.2.e @wur.nl>; Functionarisgegevensbescherming <functionarisgegevensbescherming@wur.nl>
Onderwerp: RE: Herinnering: beoordelen flexibele arbeidsvoorwaarden

PS: als iemand anders dit vandaag kan oppakken hoor ik het ook graag!

5.1.2.e
Corporate Privacy Officer | 5.1.2.e

Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317 5.1.2.e
www.wur.nl/disclaimer

Reeds beoordeeld

Privacy

Van: 5.1.2.e
Verzonden: zaterdag 24 april 2021 08:45
Aan: Privacy
CC: 5.1.2.e
Onderwerp: Re: Nieuwe datalekmelding | 4/23/2021 4:47:39 PM | 5.1.2.e @wur.nl

Ha 5.1.2.e

Ik zou zeggen: better safe than sorry. Een voorlopige melding lijkt mij dus wel op z'n plaats.

Wel goed denk ik om straks te evalueren waarom er bij IT geen back up is om hier naar te kijken. Daarom 5.1.2.e en 5.1.2.e ook maar even in de cc gezet.

Fijn weekeinde,
5.1.2.e

Verstuurd vanaf mijn iPhone

Op 23 apr. 2021 om 19:38 heeft Privacy <privacy@wur.nl> het volgende geschreven:

> Ha 5.1.2.e
>
> Deze kreeg ik vanavond binnen. Het gaat kennelijk om een situatie waarbij sprake is geweest van onbevoegde inzage in tekenstukken binnen de muren van WUR. Vanwege de gevoelige aard van de gegevens lijkt dit mij prima facie ook een meldplichtig incident, maar het is m.i. nog de vraag of inderdaad sprake is van onrechtmatige verwerking en of niet sprake is van een technische fout of ongeluk. Maandagochtend rond 9 uur verstrijkt de 72-uurstermijn.
>
> Vind jij dat we een voorlopige melding moeten doen? Mocht je nog kans zien te reageren dan hoor ik het graag. Ik stuur je anders zondag even een appje.
>
> Groet en goed weekend,
> 5.1.2.e
>
> [redacted]
> Corporate Privacy Officer | Corporate Governance & Legal Services
>
> Wageningen University & Research
> Postbus 9101, 6700 HB Wageningen
> B:104 (Atlas) | 5.1.2.e Droevendaalsesteeg 4, 6708 PB Wageningen
> Tel. 0317 5.1.2.e
> www.wur.nl/disclaimer
>
> **Van:** Privacy <privacy@wur.nl>
> **Verzonden:** vrijdag 23 april 2021 18:48
> **Aan:** Privacy <privacy@wur.nl>; 5.1.2.e @wur.nl>
> **Onderwerp:** Nieuwe datalekmelding | 4/23/2021 4:47:39 PM | 5.1.2.e @wur.nl
> **Urgentie:** Hoog

Beste collega,

Zojuist is er een nieuw datalek gemeld via het digitale meldformulier:

* * *

1. Geef een zo gedetailleerd mogelijke omschrijving van het incident
4 documenten die voor een upload in ADP WF bedoeld waren vanuit de applicatie DocuSign zijn door een onbekende partij binnen WUR opgepakt van de fileserver "verdwenen". De documenten bevatten personele gegevens die niet mogen lekken, incl 2 arbeidsovereenkomsten. Vandaag bleek niemand aanwezig bij Technisch Beheer van IT die wellicht kon helpen zoeken naar de partij die de docs van de server heeft gehaald. Maandag 26/4 gaat het onderzoek dus verder. Gemeld bij teamleider 5.1.2.e .

2. Wat is de aard van het incident?
Inzage door onbevoegden binnen WUR (technisch beheer).

3. Hoelang heeft het incident geduurd?
Eén dag

4a. Gedurende welke periode heeft het incident plaatsgevonden?

4b. Op welke datum heeft het incident plaatsgevonden?
2021-04-23

5. Van welke categorie personen zijn persoonsgegevens gelekt?
["Medewerkers"]

6. Van hoeveel personen zijn mogelijk persoonsgegevens gelekt?
4

7. Op welke datum/tijdstip is het incident ontdekt?
23/4 9:30 u

8. Wat voor soort persoonsgegevens zijn betrokken in het incident?
["NAW-gegevens","Geboortedatum/-plaats, geslacht, nationaliteit","Financiële gegevens (salaris, tarieven)","Persoonsgebondennummers (BSN, paspoortnummer, studentnummer)","Kopie paspoort/rijbewijs/ID-bewijs"]

9. Welke acties zijn ondernomen naar aanleiding van het incident?
API koppeling DocuSign - ADP WF/ WUR is stilgelegd en er is door Functioneel Applicatiebeheer contact gezocht met alle bekende technisch beheerders die mogelijk toegang tot dezelfde fileserver zouden kunnen hebben om na te gaan waar de bestanden zijn gebleven.Uiteindelijk geëscaleerd naar 5.1.2.e binnen IT. Tot nu toe geen respons van IT. Ma 26/4 verder.

* * *

Met vriendelijke groet,
5.1.2.e

Corporate Privacy Officer 5.1.2.e

Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317 5.1.2.e

Privacy

Van: 5.1.2.e
Verzonden: donderdag 29 april 2021 09:06
Aan: Privacy
Onderwerp: RE: Nieuwe datalekmelding | 4/23/2021 4:47:39 PM | 5.1.2.e @wur.nl

Opvolgingsvlag: Opvolgen
Vlagstatus: Voltooid

Ha 5.1.2.e,

Nee, niets vernomen van IT Technisch Beheer, we zoeken vandaag verder, ik ga ook escaleren op de non-respons en non-aanwezigheid van de juiste WUR IT medewerkers, kan echt niet.
Wordt vervolgd!

Met vriendelijke groet/ Kind regards,

5.1.2.e
Afw op wo-mi en vrij-ocht
Absent on Wed afternoons and Fri mornings

CC-mail gaat naar een aparte folder en lees ik onregelmatig
CC-mail is filtered by a rule and read at irregular intervals

---

Van: Privacy <privacy@wur.nl>
Verzonden: Wednesday, April 28, 2021 9:44 PM
Aan: 5.1.2.e @wur.nl>
Onderwerp: RE: Nieuwe datalekmelding | 4/23/2021 4:47:39 PM | 5.1.2.e @wur.nl

Ha 5.1.2.e

Ik ben even nieuwsgierig: hebben jullie al een conclusie kunnen trekken over de verloren documenten?

Groet, 5.1.2.e

Corporate Privacy Officer | Corporate Governance & Legal Services

Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e, Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317 5.1.2.e
www.wur.nl/disclaimer

Van: 5.1.2.e @wur.nl>
Verzonden: zondag 25 april 2021 20:33
Aan: Privacy <privacy@wur.nl>
Onderwerp: RE: Nieuwe datalekmelding | 4/23/2021 4:47:39 PM | 5.1.2.e @wur.nl

Ha 5.1.2.e

Je hoort van mij zodra bekend is wat er met de files is gebeurd, kan nog van alles zijn, incl automatische vernietiging ;). Wordt vervolgd!

Met vriendelijke groet/ Kind regards,

5.1.2.e
[redacted]
Afw op wo-mi en vrij-ocht
Absent on Wed afternoons and Fri mornings

CC-mail gaat naar een aparte folder en lees ik onregelmatig
CC-mail is filtered by a rule and read at irregular intervals

---

Van: Privacy <privacy@wur.nl>
Verzonden: Saturday, April 24, 2021 7:29 PM
Aan: 5.1.2.e [redacted] @wur.nl>
Onderwerp: RE: Nieuwe datalekmelding | 4/23/2021 4:47:39 PM |5.1.2.e [redacted] @wur.nl

Ha 5.1.2.e

Dank voor de melding. Ik hoor graag de uitkomst van jullie onderzoek en met name of inderdaad sprake is van onrechtmatige verwerking en of niet sprake is van een technische fout of ongeluk. Aangezien maandagochtend rond 9 uur de 72-uurstermijn verstrijkt heb ik hem op verzoek van 5.1.2.e wel alvast gemeld bij de Autoriteit Persoonsgegevens, maar die melding kan ik altijd achteraf intrekken.

Groet, 5.1.2.e

[redacted]
Corporate Privacy Officer | Corporate Governance & Legal Services

Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317-5.1.2.e
www.wur.nl/disclaimer

Privacy

Van: Privacy
Verzonden: donderdag 29 april 2021 18:36
Aan: 5.1.2.e
Onderwerp: RE: URG! Datalek 4 documenten

Heel fijn. Dan zal ik het incident terugtrekken. Dank voor de opvolging en jij ook fijne avond!
Groet, 5.1.2.e

Corporate Privacy Officer | Corporate Governance & Legal Services
Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e, Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317-5.1.2.e
www.wur.nl/disclaimer

Van: 5.1.2.e @wur.nl>
Verzonden: donderdag 29 april 2021 18:34
Aan: Privacy <privacy@wur.nl>
Onderwerp: RE: URG! Datalek 4 documenten

Idd ligt de bal nu bij ADP!
En je conclusie is juist mbt toegang door onbevoegden. Gelukkig. Pff.
Fijne avond 5.1.2.e
Met vriendelijke groet/ Kind regards,
5.1.2.e
Afw op wo-mi en vrij-ocht
Absent on Wed afternoons and Fri mornings
CC-mail gaat naar een aparte folder en lees ik onregelmatig
CC-mail is filtered by a rule and read at irregular intervals

Van: Privacy <privacy@wur.nl>
Verzonden: Thursday, April 29, 2021 5:14 PM
Aan: 5.1.2.e @wur.nl>
Onderwerp: RE: URG! Datalek 4 documenten

Ha, dat is in ieder geval fijn. Zou het niet een logische stap zijn om bij ADP zelf na te vragen wat er is gebeurd?
Hoe dan ook: kunnen wij nu ook uitsluiten dat 'onbevoegden' toegang hebben gehad?
Groet, 5.1.2.e

Corporate Privacy Officer | Corporate Governance & Legal Services
Wageningen University & Research
Postbus 9101, 6700 HB Wageningen
B:104 (Atlas) | 5.1.2.e, Droevendaalsesteeg 4, 6708 PB Wageningen
Tel. 0317-5.1.2.e
www.wur.nl/disclaimer

Van: 5.1.2.e @wur.nl>
Verzonden: donderdag 29 april 2021 14:21
Aan: Privacy <privacy@wur.nl>
Onderwerp: FW: URG! Datalek 4 documenten

Ter info, lijkt technisch binnen de ADP/DocuSign "muren" te zijn gebleven. :)
Met vriendelijke groet/ Kind regards,
5.1.2.e
Afw op wo-mi en vrij-ocht
Absent on Wed afternoons and Fri mornings
CC-mail gaat naar een aparte folder en lees ik onregelmatig
CC-mail is filtered by a rule and read at irregular intervals

Van: 5.1.2.e @wur.nl>
Verzonden: Thursday, April 29, 2021 1:11 PM
Aan: 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
CC: 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>; HR functioneelbeheer <hr.functioneelbeheer@wur.nl>; 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
Onderwerp: RE: URG! Datalek 4 documenten

Goedemiddag,
Vanmorgen hebben 5.1.2.e en ik even bij elkaar gezeten. Zover we nu hebben kunnen achterhalen zijn de documenten niet buiten het traject Docusign/ADP gekomen.
Documenten door de koppeling geplaatst bij ADP worden daar alleen door ADP opgepakt en verwerkt en dus niet door processen buiten ADP om. Enkele documenten waar het hier om gaat lijken ook terug te vinden te zijn in de folder waar documenten worden geplaatst door ADP als de verwerking niet goed is gegaan. Ook dat lijkt een indicatie te zijn dat ADP de documenten heeft opgepakt. De onduidelijkheid zit vooral in het feit dat we niet precies weten hoe het proces verloopt aan de kant van ADP nadat deze de documenten heeft opgepakt welk zijn aangeboden door de WUR.
Aan de hand van logging van de verschillende processen proberen we ondertussen nog meer inzicht te kunnen in het traject van de betreffende documenten.
Vrgr.,

5.1.2.e
Facilitair Bedrijf, onderdeel van Wageningen University & Research
Afdeling Informatie Technologie
Postbus 59, 6700 AB Wageningen
Gebouw 116 (Actio), Akkermaalsbos 12, 6708 WB Wageningen
Tel. +31 (0)317 5.1.2.e
www.wur.nl, www.disclaimer-nl.wur.nl

From: 5.1.2.e @wur.nl>
Sent: Thursday, 29 April 2021 10:38
To: 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
Cc: 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>; B5.1.2.e @wur.nl>; HR functioneelbeheer <hr.functioneelbeheer@wur.nl>; 5.1.2.e @wur.nl>
Subject: URG! Datalek 4 documenten
Importance: High

Goedemorgen 5.1.2.e en 5.1.2.e en ik kennen elkaar al wel, 5.1.2.e wij nog niet, maar ik begrijp dat jij 5.1.2.e vervangt en zij per 1 mei weg is, dus vandaar even aan jullie.
Afgelopen vrijdag is er een datalek ontstaan door het in productie testen van een nieuwe API tussen DosuSign en ADP WF.
Daarbij waren 4 documenten beoogd te worden geüpload in ADP WF (Digitaal Personeelsdossier) die als ondertekende output uit DocuSign waren gekomen.
Nu zijn de 4 documenten spoorloos geraakt ergens in het landschap, ik kan het even niet anders verwoorden.
2 documenten waren Arbeidsovereenkomsten en bevatten dus privacy gevoelige gegevens, dit is als een datalek door mij gemeld en door 5.1.2.e aan de Autoriteit Persoonsgegevens.
Wat mij verbaast en de reden van deze escalatie is dat er op heden door niemand van WUR IT is gereageerd hierop noch medewerking verleend in het onderzoek wat er met de 4 documenten is gebeurd.
Vrijdag 23/4 geen reactie/ aanwezigheid van de technisch beheerders waarvan wij de namen hadden, maandag 26/4 geen reactie op de mail van 5.1.2.e aan 5.1.2.e en tot op heden verder geen reactie. Mogelijk hebben wij (nog) niet naar de juiste personen geëscaleerd, zijn daarin ook zoekende.
Hoe kan dit? Hebben wij de verkeerde contactpersonen (bekend zijn 5.1.2.e -> vrij, 5.1.2.e -> Buitenland, 5.1.2.e -> was nog niet ingewerkt door 5.1.2.e) en/of zijn er geen sluitende roosters/

voicemails/ OOO-berichten ingesteld qua aanwezigheid/bereikbaarheid/ back-ups voor dit soort noodgevallen?
Graag jullie aandacht voor dit datalek en het helpen opsporen van wat er gebeurd is met de 4 documenten en ik ben ook geïnteresseerd in een correct en volledig lijstje met contactpersonen en roosterinfo voor mijn HR Functioneel Beheer (cc) team, zodat we elkaar in dit soort gevallen beter kunnen bereiken.
Contactpersonen voor de inhoud van de docs/ technische gegevens van de API zijn 5.1.2.e en evt 5.1.2.e (functioneel PO).
Alvast hartelijk dank!
Met vriendelijke groet/ Kind regards,

5.1.2.e **| Manager Shared Service Centre Human Resources a.i.**
Wageningen University & Research
Wageningen Campus - Droevendaalsesteeg 4 - gebouw Atlas 104
Postbus 9101, 6700 HB Wageningen
T +31 (0)3175.1.2.e
M +31 (0)65.1.2.e
E-mail 5.1.2.e @wur.nl
http://www.wur.nl
http://www.wur.nl/nl/Disclaimer.htm

Afwezig op woensdagmiddag en vrijdagochtend
Absent on Wednesday afternoons and Friday mornings
CC-mail gaat naar een aparte folder en lees ik onregelmatig
CC-mail is filtered by a rule and read on an irregular basis

Van: 5.1.2.e @wur.nl>
Verzonden: Friday, April 23, 2021 1:37 PM
Aan: 5.1.2.e @wur.nl>; 5.1.2.e @wur.nl>
Onderwerp: 4 documenten

Beste 5.1.2.e
Ik ben 5.1.2.e, functioneel beheerder ADP Workforce/MyHR.
Via 5.1.2.e heb ik je naam doorgekregen. Ik wil melding maken van het feit dat er op dit moment 4 documenten voor mij onzichtbaar ergens bij (server)beheer zijn binnen gekomen. Korte uitleg: vanuit HR zijn we bezig met een geautomatiseerde koppeling vanuit Docusign naar een SFG server van ADP Workforce via API. 5.1.2.e en 5.1.2.e zijn hier bij betrokken. Deze koppeling hebben we vanmorgen tijdelijk life gehad. Wat 5.1.2.e en ik direct zagen is dat de 4 documenten direct van de SFG server werden verwijderd/opgehaald. Omdat wij niet kunnen achterhalen wie of wat deze documenten heeft opgehaald, hebben we dit direct weer stil gelegd. Normaliter zou ik met 5.1.2.e 5.1.2.e of 5.1.2.e schakelen, maar die zijn beiden afwezig en ik kwam bij 5.1.2.e uit.
Omdat deze 4 documenten personele gegevens bevatten, wil ik deze documenten achterhalen en laten vernietigen om een mogelijk datalek te voorkomen.
Graag je (re)actie/hulp.
Met vriendelijke groet/Kind regards,

5.1.2.e
Functioneel Applicatiebeheerder CHR

Aanwezig: maandag, dinsdag, donderdag
Wageningen University & Research
Corporate HR - Shared Service Center
Postbus 9101, 6700 HB Wageningen
Wageningen Campus - Gebouw 104 (Atlas)
Droevendaalsesteeg 4, 6708 PB Wageningen
T: 065.1.2.e
E: 5.1.2.e @wur.nl
www.disclaimer-nl.wur.nl

www.wur.nl

Ontvangstbevestiging

Uw verzoek tot het indienen van een melding wordt in behandeling genomen.
U kunt de melding niet online raadplegen. Maak daarom een print voor uw eigen administratie. Doe dit voordat u deze pagina afsluit. Na het afsluiten van deze pagina zijn de gegevens die u heeft opgegeven niet meer beschikbaar. Onder het onderstaande meldingsnummer is de melding bekend bij de Autoriteit Persoonsgegevens. U heeft het meldingsnummer nodig om de melding aan te kunnen passen of in te kunnen trekken. Vermeld het meldingsnummer bij eventuele correspondentie met de Autoriteit Persoonsgegevens over de melding.

Tijdstip ontvangst	24-04-2021 19:33:21
Uniek nummer	5.1.2.e

0. Over deze melding

Gaat het om een nieuwe of bestaande melding?	Een nieuwe melding indienen
Op grond van welke wettelijke bepaling doet u deze melding?	Algemene verordening gegevensbescherming (AVG)

1. Contactgegevens en overige algemene informatie

1.1 Contactgegevens

Over welke organisatie of welk bedrijf gaat het?

Registratienummer bij de Kamer van Koophandel	09215846
Naam van het bedrijf of de organisatie	Wageningen University
Adres	Droevendaalsesteeg 4
Postcode	6708PB
Plaats	Wageningen
In welke sector is de organisatie of het	Onderwijs - Tertiair onderwijs

bedrijf actief?

Wie meldt het datalek?

Naam	5.1.2.e
Functie	corporate privacy officer
E-mailadres	privacy@wur.nl
Telefoonnummer	0317 5.1.2.e

Met wie kan de Autoriteit Persoonsgegevens contact opnemen voor nadere informatie over de melding?

De melder is contactpersoon	Nee
Naam contactpersoon	5.1.2.e
Functie contactpersoon	functionaris voor de gegevensbescherming
E-mailadres contactpersoon	dpo@wur.nl
Telefoonnummer contactpersoon	0317 5.1.2.e

1.2 Betrokkenheid andere organisatie

Was er een andere organisatie betrokken bij de inbreuk?	Nee

2. Tijdlijn

Exacte datum waarop de inbreuk was, indien bekend	23-04-2021
Duurt de inbreuk op dit moment nog voort?	Nee
Wanneer werd de inbreuk ontdekt?	23-04-2021

3. Gegevens over het datalek

3.1 Aard van de inbreuk

Inbreuk op de vertrouwelijkheid van de gegevens	Ja
Inbreuk op de integriteit van de gegevens	Nee
Inbreuk op de beschikbaarheid van de	Ja

gegevens

3.2 Aard van het incident

Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest?	Persoonsgegevens verstuurd of afgegeven aan verkeerde ontvanger

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest

Vier tekenstukken zijn door een vooralsnog onbekend persoon opgepakt van de fileserver en daarna verdwenen. De documenten bevatten persoonsgegevens, waaronder twee arbeidsovereenkomsten. Op vrijdagavond 23 april jl. was het nog niet mogelijk uitsluitsel te geven op de vraag of hier sprake is geweest van onrechtmatige verwerking. Maandag 26 april gaat het onderzoek verder.

4. Persoonsgegevens die betrokken zijn bij het datalek

4.1 Persoonsgegevens in het algemeen

Naam	Ja
Geslacht, geboortedatum en/of leeftijd	Ja
Burgerservicenummer (BSN)	Ja
Contactgegevens	Ja
Toegangs- of identificatiegegevens	Nee
Financiële gegevens	Ja
(Kopieën van) paspoorten of andere legitimatiebewijzen	Ja
Locatiegegevens	Nee
Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen	Nee

4.2 Bijzondere categorieën van persoonsgegevens

Persoonsgegevens waaruit iemands ras of etnische afkomst blijkt	Nee

Persoonsgegevens waaruit iemands politieke opvattingen blijken	Nee
Persoonsgegevens waaruit iemands religieuze of levensbeschouwelijke overtuigingen blijken	Nee
Persoonsgegevens waaruit iemands lidmaatschap van een vakbond blijkt	Nee
Gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid	Nee
Gegevens over iemands gezondheid	Nee
Genetische gegevens	Nee
Biometrische gegevens	Nee

4.3 Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords ("gegevensregisters") zijn getroffen door de inbreuk	4

5. De groep mensen van wie persoonsgegevens betrokken zijn bij het datalek

Werknemers	Ja
Klanten (huidig en potentieel)	Nee
Leerlingen of studenten	Nee
Patiënten	Nee
Minderjarigen	Nee
Personen uit kwetsbare groepen	Nee

Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk.

Het betreft in ieder geval de arbeidsovereenkomsten van twee medewerkers.

Van minimaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?	2
Van maximaal hoeveel personen zijn	2

persoonsgegevens betrokken bij de inbreuk?	

6. Maatregelen die zijn getroffen voordat het datalek plaatsvond

Waren de persoonsgegevens op het moment dat de inbreuk zich voordeed versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk voor onbevoegden?	Nee

7. Gevolgen van het datalek

7.1 Gevolgen van de inbreuk op de vertrouwelijkheid, de integriteit en/of de beschikbaarheid van de gegevens.

Onbevoegden hebben kennis kunnen nemen van de gegevens	Ja
De gegevens kunnen op een onbehoorlijke of onrechtmatige manier worden misbruikt	Ja
Er worden binnen uw eigen organisatie mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens gebruikt	Nee
Er worden mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens hergebruikt voor andere doeleinden of doorgegeven aan andere organisaties	Nee
Een essentiële dienst kan tijdelijk niet meer worden verleend aan de betrokkenen	Nee
Een essentiële dienst kan permanent niet meer worden verleend aan de	Nee

betrokkenen

7.2 Lichamelijke, materiële en immateriële schade voor de betrokkenen

Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkenen?

Discriminatie	Nee
Identiteitsdiefstal of -fraude	Nee
Financiële verliezen	Nee
Reputatieschade	Nee
Verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens	Nee
Ongeoorloofde ongedaanmaking van pseudonimisering	Nee
Betrokkenen kunnen hun rechten en vrijheden niet uitoefenen	Nee
Betrokkenen worden verhinderd controle over hun persoonsgegevens uit te oefenen	Nee

Andere gevolgen, namelijk:

Verlies van vertrouwelijkheid van de arbeidsovereenkomsten

Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkenen	2. Beperkt

8. Vervolgacties naar aanleiding van het datalek

8.1 Informeren van de betrokkenen

Heeft u het datalek gemeld aan de betrokkenen of bent u van plan dat te gaan doen?	Nog niet bekend
Hoeveel betrokkenen heeft u geïnformeerd of gaat u informeren?	0
Welk communicatiemiddel of welke	n.n.b.

communicatiemiddelen gebruikt u of gaat u gebruiken om de betrokkenen te informeren?	

8.2 Maatregelen om de inbreuk aan te pakken

Welke technische en organisatorische maatregelen heeft uw organisatie getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?
Vooralsnog is onduidelijk wat er precies gebeurd is. Het lijkt geen structureel incident, maar een eenmalige onbevoegde inzage.

8.3 Internationale aspecten

Heeft de inbreuk zich voorgedaan in een grensoverschrijdende gegevensverwerking, en is de AP voor deze verwerking de leidende toezichthouder?	Nee
Heeft uw organisatie of bedrijf, het datalek gemeld bij privacytoezichthouders in een of meer andere EU-landen, of gaat u dat nog doen?	Nee
Heeft uw organisatie of bedrijf, het datalek gemeld bij Europese toezichthouders op andere meldplichten, of gaat u dat nog doen?	Nee

9. Overig

Is naar uw mening deze melding compleet?	Nee, er komt later een vervolgmelding met aanvullende informatie over deze inbreuk

Ontvangstbevestiging van melding inbreuk

Dit is de kopie van uw melding van een inbreuk aan de Autoriteit Persoonsgegevens ten behoeve van uw eigen administratie.

Bewaar deze kopie goed. Bij twijfel kunt u met deze kopie achteraf aantonen dat u een melding van een inbreuk heeft gedaan bij de AP.

Meldingsnummer: 5.1.2.e

Melddatum: 08 juni 2021

Meldtijdstip: 17:12

1 Introductie

1.1 De melding van een inbreuk

Wat wilt u doen?	Een bestaande melding intrekken
Beschikt u over het meldingsnummer van de oorspronkelijke melding?	Ja
Dit is het meldingsnummer:	5.1.2.e

2 Intrekking

2.1 Wie dient de intrekking in?

Naam	5.1.2.e
Functie	corporate privacy officer
E-mailadres	privacy@wur.nl
Telefoonnnummer	0317 5.1.2.e
2.2 Is de indiener de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen	voor nadere informatie over de melding en intrekking?

Nee	
Naam contactpersoon	5.1.2.e
Functie contactpersoon	functionaris voor de gegevensbescherming
E-mailadres contactpersoon	dpo@wur.nl
Telefoonnummer contactpersoon	03175.1.2.e

2.3 Waarom wilt u uw melding intrekken?

[✓] De inbreuk heeft niet daadwerkelijk geleid tot onbevoegde toegang tot persoonsgegevens

Kunt u uitsluiten dat onbevoegd toegang heeft plaatsgevonden, bijvoorbeeld aan de hand van logbestanden?	Ja
2.4 Licht toe waarom u uw melding wilt intrekken	De melding betreft het 'kwijtraken' van vier tekenstukken. Die tekenstukken zijn teruggevonden. Het betreft vier documenten die het tekenproces niet goed hebben doorlopen en daarom in een folder waren geplaatst waar documenten worden geplaatst als de verwerking niet goed is gegaan.

Indien beschikbaar: upload hier relevante documentatie ter ondersteuning van uw beslissing om de melding in te trekken.

11 Verzenden

[✓] Door dit vakje aan te vinken verklaart u dit formulier naar waarheid in te vullen

[✓] Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen namens uw organisatie.

Privacyverklaring

[✓] Ik ben op de hoogte van de inhoud van de Privacyverklaring van de AP