Netwerkreglement Wageningen University (WU) 2022 voor studenten

Samenvatting

Wageningen University, biedt aan studenten de mogelijkheid om netwerkfaciliteiten, apparatuur, software en gegevens (hierna samen: de Faciliteiten) te gebruiken. Zo hebben studenten binnen onze gebouwen, alsmede binnen de studentenwoningen op de campus, de mogelijkheid om internet te gebruiken ten behoeve van de studie. Ook worden aan studenten een persoonlijke e-mailbox en toegang tot een digitale leeromgeving beschikbaar gesteld, ten behoeve van de studie.

Dit reglement is van toepassing op al het gebruik van onze Faciliteiten door studenten van WU en door bezoekende studenten, zoals gast- en uitwisselingsstudenten. Voor studenten die ook werknemer van WU zijn, geldt ook het netwerkreglement voor werknemers en overige medewerkers en gelden dus beide reglementen. De hoedanigheid waarin de Faciliteiten worden gebruikt, bepaalt in dat geval welk reglement leidend is.

Bij het inloggen met een nieuw account of bij een volgende door het college van bestuur vastgestelde update van dit reglement, wordt iedereen tijdens de eerste inlog met het (nieuwe) account eenmalig aan de hand van een pop up in de gelegenheid gesteld kennis te nemen van de inhoud van dit reglement. Daar dient men zich vervolgens akkoord mee te verklaren alvorens kan worden ingelogd. Men wordt daarnaast gewezen op de vindplek van de geldende versie van dit netwerkreglement.

Wat is acceptabel gebruik van de Faciliteiten?

Wanneer je gebruik maakt van de Faciliteiten, die we jou als student aanbieden ten behoeve van je studie, dien je je te houden aan verschillende gedragsregels, in het kader van de informatieveiligheid, beschikbaarheid, rechten van ons en eventuele derden en een goede gang van zaken in onze gebouwen en op onze terreinen. Deze regels zijn in dit reglement opgenomen.

De volgende beginselen gelden voor elk gebruik:

I) De Faciliteiten worden niet gebruikt voor activiteiten die in strijd zijn met geldende wetgeving of de goede zeden.
II) De Faciliteiten worden niet gebruikt voor activiteiten die schadelijk, bedreigend of aanstootgevend zijn voor anderen.
III) De beschikbaarheid, integriteit en vertrouwelijkheid van (informatie binnen) de Faciliteiten wordt door het gebruik van de Faciliteiten niet in gevaar gebracht.

Deze beginselen worden in het reglement nader uitgewerkt in concrete gedragsregels, bijvoorbeeld ten behoeve van de beveiliging en ter voorkoming van overlast.

Hoe kunnen wij het gebruik en de veiligheid van de Faciliteiten controleren?

Om te controleren of de Faciliteiten niet worden gebruikt op een manier die in strijd is met de regels van dit reglement of met geldende wet- en regelgeving en om te zorgen dat de Faciliteiten en de informatie binnen deze Faciliteiten te allen tijde veilig zijn en niet overbelast worden, kunnen wij het gebruik van de Faciliteiten monitoren op de manieren zoals beschreven in dit reglement. Wij streven daarbij naar een goede balans tussen verantwoord en veilig gebruik van de Faciliteiten en de privacy van studenten. We zorgen er daarom voor dat controles door of namens ons proportioneel zijn: hoe groter de risico's en hoe specifieker de aanwijzingen op een overtreding, hoe ingrijpender en gerichter de controle.

Algemene controle

Controle vindt in eerste instantie geautomatiseerd plaats op het niveau van geaggregeerde gegevens. Dit betekent dat algemene controles worden uitgevoerd op gegevens die zo zijn samengevoegd dat er een totaalbeeld van het gebruik van (een deel van) de Faciliteiten ontstaat. Gegevens die herleidbaar zijn naar een individu worden pas geraadpleegd als een geautomatiseerde melding daar aanleiding voor geeft.

Naast algemene controles die plaatsvinden op basis van geaggregeerde gegevens, worden bij bepaalde vormen van algemene controle, zoals Mobile Device Management en aanvalssimulaties op netwerken en/of systemen, gegevens verzameld die wel herleidbaar zijn tot individuele gebruikers. Deze gegevens worden alleen gebruikt voor het doel waarvoor ze zijn verzameld, namelijk het uitvoeren van de controle op en handhaving van de naleving van dit reglement. De gegevens worden verwijderd zodra ze niet meer nodig zijn voor dat doel.

Gericht onderzoek

Van gericht onderzoek is sprake wanneer gegevens over een specifieke student worden vastgelegd naar aanleiding van een zwaarwegend vermoeden van een overtreding van dit reglement door de student. Wij kunnen dan bijvoorbeeld de inhoud van communicatie of bestanden controleren op daadwerkelijke overtredingen.

Wat zijn de consequenties van overtreding van dit reglement?

Indien het nodig is om schade te voorkomen, kan (een deel van) het gebruik van de Faciliteiten onmiddellijk worden geblokkeerd. Wanneer wij een overtreding van dit reglement constateren, zal de betrokken student de kans krijgen om een zienswijze te geven, voordat wordt overgegaan tot eventuele disciplinaire maatregelen. Naast disciplinaire maatregelen kunnen wij aangifte doen in het geval van strafbare feiten en/of de geleden schade op de overtreder verhalen.

Hoe wordt de privacy van de student beschermd?

Wij leven bij de uitvoering van dit reglement de geldende wet- en regelgeving, waaronder de Algemene verordening gegevensbescherming (AVG), na. De persoonsgegevens die wij bewaren naar aanleiding van algemene controle en gericht onderzoek worden passend beveiligd. Alleen medewerkers voor wie dat noodzakelijk is, een zeer beperkte groep, heeft toegang tot de persoonsgegevens. Er wordt altijd naar gestreefd om zo min mogelijk persoonsgegevens te verzamelen om de doelen van dit reglement te bereiken. In de gevallen dat wij persoonsgegevens verwerken, hebben zo min mogelijk personen daar toegang toe en worden deze passend beveiligd. Zie deze link bij dit reglement voor meer informatie over de persoonsgegevens die wij van de student verwerken, hoe we dit doen en waarom.

Contents

1. Gebruik van de Faciliteiten

Wij stellen aan jou als student computer- en netwerkfaciliteiten (zoals openbare computers, draadloze en/of bedrade netwerkaansluitingen, opslagcapaciteit, printers en elektronische leeromgevingen) (hierna: de Faciliteiten) ter beschikken ten behoeve van de studie, onder meer voor het kunnen maken van opdrachten, verslagen en scripties, het bijhouden van de studievoortgang, het raadplegen van bronnen en het communiceren met docenten en medestudenten.

Als student mag je eigen apparatuur en toepassingen op onze Faciliteiten gebruiken, zolang je je bij dit gebruik houdt aan de regels van dit reglement en niet in strijd handelt met geldende wet- en regelgeving en maatschappelijke fatsoensnormen. Het veranderen van instellingen in apparatuur en toepassingen, die door ons beschikbaar gesteld zijn, is alleen toegestaan met onze toestemming. Het aansluiten van eigen netwerkapparatuur waarmee de verbinding kan worden gedeeld met derden op netwerkaansluitingen is te allen tijde verboden.

Dit reglement geldt ook indien je als gast gebruik maakt van netwerkvoorzieningen van andere instellingen, waarbij toegang wordt verkregen op basis van de inloggegevens van de eigen Instelling (Eduroam).

Bepaalde Faciliteiten zijn alleen toegankelijk met behulp van inloggegevens. Deze zijn persoonsgebonden en het is niet de bedoeling dat je deze gegevens met anderen deelt. Wij kunnen nadere eisen stellen aan de kwaliteit van wachtwoorden en andere beveiligingsaspecten zoals nader geformuleerd in het Informatiebeveiligingsbeleid. Bij een vermoeden van misbruik van een wachtwoord of authenticatiemiddel kunnen wij per direct het betreffende account ontoegankelijk maken.

1.1. Beveiliging

Wij nemen informatiebeveiliging erg serieus. Wij hanteren dan ook een strikt beveiligingsbeleid en treffen passende technische en organisatorische maatregelen om de infrastructuur en de informatie van WU en haar studenten en medewerkers te beveiligen tegen verlies, diefstal, criminele activiteiten, verlies van vertrouwelijkheid, schending van privacyrechten en schending van intellectuele eigendomsrechten.

Dit is een gezamenlijk belang. Niet alleen wij hebben hier belang bij, maar ook de gebruikers van de Faciliteiten. Hieronder val ook jij als student. Daarom verwachten wij ook van studenten een proactieve houding en dat zij serieuze stappen nemen om de eigen computer en andere apparatuur (zoals smartphones of tablets) voldoende te beveiligen. Zo is de student te allen tijde zelf verantwoordelijk voor het gebruik van de eigen apparatuur en de op deze apparatuur opgeslagen gegevens.

In het bijzonder dien je, indien je met eigen apparatuur gebruik maakt van onze netwerkaansluiting, in het kader van beveiliging:

- deze apparatuur te voorzien van een goede virusscanner en firewall;
- onrechtmatige toegang tot onze systemen te voorkomen door sterke, unieke wachtwoorden en/of pincodes te gebruiken;
- deze apparatuur up-to-date te houden wat betreft software-instellingen;
- versleuteling toe te passen.

De Central Informatie Security Officer (CISO) zal een lijst publiceren met veiligheidsmaatregelen, welke regelmatig zal worden herzien. We verwachten van jou als student dat je de maatregelen, die op jou van toepassing zijn, stipt opvolgt.

1.2. PRIVÉGEBRUIK EN OVERLAST

Hoewel de Faciliteiten bedoeld zijn voor het gebruik ten behoeve van de studie, mag je onze Faciliteiten, in beperkte mate ook voor andere doeleinden gebruiken. Wel dien je er rekening mee te houden dat het gebruik van de Faciliteiten nooit illegaal of storend voor de goede orde mag zijn en geen overlast mag veroorzaken voor anderen. Bovendien mag je geen inbreuk maken op rechten van WU of derden en mag je niet de integriteit en de veiligheid van het netwerk aantasten.

Onder illegaal, storend en/of overlast veroorzakend gebruik van de Faciliteiten, verstaan wij in ieder geval:

- het in openbare ruimtes raadplegen van internetdiensten met een pornografische, racistische, discriminerende, beledigende of aanstootgevende inhoud of het verzenden van berichten met een dergelijke inhoud;
- het verzenden van berichten met een (seksueel) intimiderende inhoud of van berichten die blijk geven van of (kunnen) aanzetten tot discriminatie, haat en/of geweld;
- het versturen van berichten aan grote aantallen ontvangers tegelijk, het versturen van kettingbrieven of het verspreiden van kwaadaardige software zoals virussen, ransomware en spyware;
- Het verspreiden van fake news dan wel desinformatie
- filesharing- of streamingdiensten te gebruiken wanneer dit overmatig veel dataverkeer genereert, zodanig dat het de beschikbaarheid van de Faciliteiten kan aantasten;
- films, muziek, software en overig auteursrechtelijk beschermd materiaal te downloaden van enige illegale bron of wanneer je weet/moet weten dat dit in strijd met auteursrechten is;
- films, muziek, software en overig auteursrechtelijk beschermd materiaal te verspreiden (uploaden) naar derden zonder toestemming van de rechthebbenden.

Het gebruik van de Faciliteiten ten behoeve van eigen commerciële activiteiten is uitsluitend toegestaan, wanneer hiervoor voorafgaand schriftelijk toestemming is verleend door WU.

Wanneer je in je studentenwoning, die zich op de campus bevindt, gebruik maakt van onze netwerkfaciliteiten, is het gebruik hiervan niet beperkt, behoudens voor zover noodzakelijk om de integriteit en de veiligheid van het netwerk te kunnen bewaren, of om de gevolgen van congestie te beperken. Wanneer we ingrijpen om de gevolgen van congestie te beperken, zullen gelijke soorten verkeer gelijk worden behandeld. De overige bepalingen in dit reglement zijn onverkort van toepassing wanneer je in je woonruimte gebruik maakt van onze netwerkfaciliteiten.

1.3. INTELLECTUEEL EIGENDOM EN VERTROUWELIJKE INFORMATIE

Het wordt van jou als student verwacht dat je geen inbreuk op onze intellectuele eigendomsrechten en die van derden maakt en de licentie afspraken, zoals die van toepassing zijn binnen WU, respecteert.

De zeggenschap over de informatie van WU, zoals die bijvoorbeeld voortvloeit uit de onderwijsexamenregistratie en waarbij geheimhouding van bijvoorbeeld tentamenvragen aan de orde is, berust bij ons. Jij hebt als student geen zelfstandige zeggenschap over de informatie, behalve als dit jou expliciet is toegekend door WU.

Tenzij dat nodig is voor de studie, mag je geen grote hoeveelheden artikelen uit de bestanden van de digitale bibliotheek downloaden of substantiële delen van de bestanden of databases in de digitale bibliotheek systematisch kopiëren.

Indien je in het kader van je studie of het uitvoeren van taken voor ons toegang krijgt tot vertrouwelijke of privacygevoelige informatie, dien je die informatie strikt vertrouwelijk te behandelen.

Wij verwachten in dat geval van jou dat je bijzondere aandacht besteedt aan het treffen van maatregelen, zoals in dit reglement genoemd onder Beveiliging in paragraaf 1.1. Dit geldt in het bijzonder bij het uitvoeren van taken waarbij de verwerking van vertrouwelijke informatie buiten de controle van WU noodzakelijk is, zoals via e-mail, het opnemen in niet instellingsgebonden cloud-toepassingen of op eigen apparatuur of opslagmedia. Daar waar mogelijk dien je in verband met de veiligheid altijd applicaties te gebruiken die door WU worden aangeboden.

Je dient je bij de verwerking van vertrouwelijke en privacygevoelige informatie te houden aan de geldende wet- en regelgeving. Indien we met betrekking tot het waarborgen van de vertrouwelijkheid en de intellectuele eigendomsrechten nadere voorschriften hebben opgesteld, dien je deze daarnaast strikt op te volgen.

2. Controle en monitoring

Wij controleren de naleving van dit reglement. Wij zullen bij de controle op het gebruik van de Faciliteiten handelen binnen de geldende wet- en regelgeving.

We streven, in het kader van de controle en monitoring naar maatregelen, die inzage in privacygevoelige informatie of persoonsgegevens van individuele studenten zo veel mogelijk beperken. Wij zullen daarbij uitgaan van de juiste balans tussen toezicht en controle op de handhaving van dit reglement en de bescherming van jouw privacy. Wij zullen, waar mogelijk, slechts geautomatiseerd controleren of filteren, zonder daarbij inzage te verkrijgen in gedrag van individuele personen.

2.1. Voorwaarden voor controle

De controle op en het monitoring van het gebruik van de Faciliteiten vindt slechts plaats in het kader van de handhaving van de regels uit dit reglement en uitsluitend voor de doelen zoals genoemd in hoofdstuk I. Belangrijk is dat dit gebeurt ten behoeve van de goede orde, de bewaking van de integriteit en de veiligheid van onze Faciliteiten.

2.1.1. Controle op incidenten

Monitoring en logging
Om de controle uit te kunnen voeren op bedreigingen voor de integriteit, beschikbaarheid en vertrouwelijkheid van WUR-systemen worden doorlopend alle activiteiten en gegevens van alle gebruikers van de Faciliteiten geautomatiseerd verwerkt (monitoring en logging).

Deze logging gegevens worden door automatische processen verwerkt die volgens voorgedefinieerde regels kunnen leiden tot een melding.

Analyse van incidenten
Enkel als uit de voorgedefinieerde regels volgt dat een melding uit het systeem aanleiding geeft tot nader onderzoek (bijvoorbeeld een virus detectie of afwijkende aanlogpogingen), zal er een verdere analyse uit worden gevoerd van de meldingen door de beheerders van de dienst en/of de (externe) analisten. Onderdeel van de analyse kan zijn het herleiden van de meldingen naar een systeem of persoon. Dit betekent dat systeembeheerders van WUR en externe analisten op dat moment toegang kunnen krijgen tot de inhoud van de gegevens en activiteiten van de betreffende student van WUR, voor zover de melding daarop betrekking heeft (bijv. de inhoud van het phishingbericht).

In spoedeisende gevallen en waar noodzakelijk ter voorkoming van (verdere) verwezenlijking van risico's of schade, kunnen deze medewerkers besluiten tot het nemen van technische maatregelen, zoals een blokkering van de toegang tot een bepaalde dienst of het beperken van de mogelijkheden van het apparaat in kwestie om het netwerk te kunnen gebruiken. Het gaat daarbij altijd om tijdelijke maatregelen voor ten hoogste de duur van het incident. Indien de situatie het toestaat wordt vooraf getoetst door de information security officer (ISO) of de maatregel passend is. In spoedgevallen wordt de ISO zo snel mogelijk na het toepassen van de maatregel geïnformeerd.

2.1.2 Controle individu
Wanneer WU vermoedt dat een student de regels overtreedt, kan gedurende een vastgestelde (korte) periode, gerichte controle worden uitgevoerd in de reeds beschikbare logging zoals genoemd in 2.1.1. Alleen als blijkt dat hiervoor zwaarwegende redenen zijn, vindt gerichte controle op de inhoud plaats. De procedure voor gericht onderzoek wordt in paragraaf 2.3. beschreven.

2.2. Uitvoering van algemene controle
Om controle uit te kunnen voeren op de naleving van dit reglement, kunnen wij enkele specifieke maatregelen treffen, te weten:

- Wij kunnen, op basis van steekproefsgewijze content-filtering, een controle uitvoeren op het uitlekken van vertrouwelijke informatie, waartoe jij in het kader van je studie of het uitvoeren van taken voor ons toegang hebt. Verdachte berichten kunnen daarbij apart gezet worden voor nader onderzoek.
- Daarnaast zullen wij de controle in het kader van kosten- en capaciteitsbeheersing beperken tot het op basis van verkeersgegevens nagaan van de bronnen van kosten of capaciteitsvraag. Als deze bronnen tot grote kosten of overlast leiden, worden zij geblokkeerd of afgeknepen, zonder daarbij de vertrouwelijkheid van de inhoud van de communicatie te schenden.

2.2.1. Aanvalssimulaties en social engineering
Om kwetsbaarheden in kaart te brengen is het nodig om aanvalssimulaties en social engineering acties uit te voeren op de Faciliteiten. Dergelijke aanvalssimulaties en social engineering acties worden alleen uitgevoerd in overleg met en na formele goedkeuring van de ISO. Voor social engineering acties worden aanvullend vooraf de privacyrisico's vastgesteld en zo veel mogelijk beperkt in samenspraak met de Functionaris Gegevensbescherming (FG) middels een gegevensbeschermingseffectbeoordeling (GBEB, ook wel DPIA genoemd).

Voorbeelden van dergelijke acties zijn red teaming en pentesten. Acties in het kader van aanvalssimulaties en social engineering worden uitgevoerd in lijn met de geldende privacywetgeving. Bij aanvalssimulaties en social engineering kunnen bijvoorbeeld op de volgende manieren persoonsgegevens worden verzameld:

- Social engineering: Een gebruiker kan verleid worden om handelingen uit te voeren of gegevens zoals zijn wachtwoord af te geven;
- Aanvalssimulatie: Er kan worden geprobeerd in te loggen in apparaten of systemen (bijvoorbeeld het studentinformatiesysteem) onder een account met hoge privileges waardoor mappen en bestanden (met daarin mogelijk persoonsgegevens en andere gegevens van vertrouwelijke aard) kunnen worden ingezien.

Met de uitvoerende partij worden afspraken gemaakt om te zorgen dat aangetroffen persoonsgegevens vertrouwelijk worden behandeld. Aangetroffen (persoons)gegevens worden niet langer bewaard dan noodzakelijk voor de test. (Persoons)gegevens worden passend beveiligd. Mappen en bestanden die expliciet als 'privé' zijn aangemerkt, worden niet doorzocht, tenzij het redelijkerwijs niet te voorkomen is.

2.3. Uitvoering van gericht onderzoek

Van gericht onderzoek is sprake wanneer verkeersgegevens of andere gegevens betreffende een specifieke student, naar aanleiding van concrete aanwijzingen van het overtreden van dit reglement, worden vastgelegd en geanalyseerd op daadwerkelijke overtredingen.

Wij kunnen gericht onderzoek uitvoeren naar aanleiding van een zwaarwegend vermoeden van een overtreding van dit reglement door de student. Wij zullen uitsluitend gericht onderzoek uitvoeren na schriftelijke opdracht vanuit de directeur Facilitair bedrijf, na advies te hebben ingewonnen bij de CISO en de FG, welke de redenen zal noemen waarom deze opdracht wordt gegeven. Het college van bestuur ontvangt een afschrift van de opdracht en een geaggregeerde samenvatting van de uitkomst van het onderzoek. Indien het advies van de CISO en/of de FG afwijkt van de opdracht vanuit de directeur Facilitair Bedrijf, dient het college van bestuur vooraf in te stemmen met de opdracht tot het uitvoeren van het onderzoek. Wanneer het onderzoek geen aanleiding geeft tot verdere maatregelen, wordt de vastlegging geanonimiseerd of vernietigd.

Ook kunnen wij, op basis van concrete aanwijzingen zoals genoemd in 2.1.1, gericht onderzoek uitvoeren naar de beveiliging of integriteit van geautomatiseerde systemen of randapparatuur (zoals, routers of printers). In afwijking van het hiervoor genoemde, is in dit geval een schriftelijke opdracht van de directeur Facilitair Bedrijf niet nodig. De resultaten van dit onderzoek worden alleen met jou gedeeld met het doel de beveiliging of integriteit van de randapparatuur te verbeteren.

Gericht onderzoek naar aanleiding van een zwaarwegend vermoeden van een overtreding van dit regelement beperkt zich in eerste instantie tot de data uit reeds beschikbare logging zoals genoemd in 2.1.1 van een individuele gebruiker of systeem. Als gericht onderzoek nader bewijs oplevert, kunnen wij overgaan tot het kennisnemen van de inhoud van communicatie of opgeslagen bestanden. Dit vereist opnieuw schriftelijke toestemming van de directeur Facilitair Bedrijf, conform het proces zoals hierboven omschreven, welke de redenen zal noemen waarom toestemming wordt verleend.

Enkele specifieke persoonsgebonden maatregelen ter controle die wij kunnen uitvoeren, zijn:

- de controle op het uitlekken van vertrouwelijke informatie. Dit vindt plaats op basis van steekproefsgewijze controle op trefwoorden. Verdachte berichten worden apart gezet voor nader onderzoek in overleg met het bestuur;

- de controle op verboden gebruik van e-mail en andere elektronische communicatiemiddelen. Dit vindt door twee personen plaats door, op basis van een overtuigend onderbouwde klacht, elektronische berichten te openen en de inhoud te raadplegen. Deze personen zijn gebonden aan geheimhouding over de inhoud.

Indien je wordt verdacht van overtreding van dit reglement wordt je binnen drie weken schriftelijk geïnformeerd door de directeur Facilitair Bedrijf over de aanleiding, de uitvoering en het resultaat van het onderzoek. Je wordt in de gelegenheid gesteld een zienswijze te geven over de aangetroffen gegevens. Uitstel van het informeren mag alleen als informeren het onderzoek daadwerkelijk zou kunnen schaden en uitsluitend voor de periode die noodzakelijk is om onmiddellijk disciplinaire maatregelen te treffen. Advies wordt vooraf ingewonnen bij de FG.

Medewerkers van WU, die de directe verantwoordelijkheid voor toezicht en controle op de naleving van dit reglement hebben, verschaffen zich, behoudens in dringende gevallen of bij een duidelijk vermoeden van schending van dit reglement, slechts toegang tot de inhoud van documenten, e-mail of andere bestanden als je daarvoor schriftelijk toestemming hebt gegeven. Je zal in dat geval achteraf worden geïnformeerd over de uitkomst van het onderzoek.

2.4. Waarborging privacy bij controle

Bij het toezicht en de controle op de naleving van dit reglement en het monitoren van de Faciliteiten verwerken wij persoonsgegevens van de gebruikers van de Faciliteiten, de inhoud van communicatie of opgeslagen bestanden. Wij houden ons bij het controleren en monitoren op het niveau van persoonsgegevens onverkort aan de AVG en andere relevante wet- en regelgeving, zoals omschreven in dit hoofdstuk.

2.4.1. Maatregelen ten behoeve van privacy

Doelbinding
Wij verwerken de persoonsgegevens van studenten uitsluitend voor de doeleinden zoals omschreven in hoofdstuk 1.

Juistheid
Wij treffen, in het kader van de controle op dit reglement, de nodige maatregelen, zodat persoonsgegevens, gelet op de doeleinden waarvoor zij verwerkt worden, juist en nauwkeurig zijn.

Dataminimalisatie
Wij hebben het controleproces zo ingericht dat de verwerking van persoonsgegevens beperkt blijft tot wat noodzakelijk is voor de doeleinden zoals genoemd in hoofdstuk 1. Onder meer doordat monitoring van het gebruik van Faciliteiten uitsluitend plaatsvindt via geautomatiseerde verwerking, zonder dat sprake is van geautomatiseerde besluitvorming. Uitsluitend indien sprake is van een concrete melding of bij een gericht onderzoek kunnen beheerders en (externe) analisten toegang krijgen tot de inhoud van internet-, data- en e-mailverkeer van studenten.

Opslagbeperking
Persoonsgegevens, die zijn vastgelegd in het kader van toezicht en controle op de naleving van dit reglement, worden zo kort mogelijk bewaard. Alleen wanneer er een redelijk vermoeden bestaat van onrechtmatig gebruik kan deze periode worden verlengd, zolang als nodig is om het onderzoek wat daaruit voortvloeit af te ronden. Zodra een onderzoek is afgerond en dit niet leidt tot disciplinaire maatregelen

tegenover een betrokkene, worden de gegevens geanonimiseerd of verwijderd. Wanneer een onderzoek wel leidt tot een disciplinaire maatregel, worden de gegevens bewaard zolang dat noodzakelijk is voor de bewijslast of voor de uitvoering van de disciplinaire maatregel.

Integriteit en vertrouwelijkheid
Daarnaast treffen wij passende technische en organisatorische maatregelen om de bij toezicht en controle op de naleving van dit reglement vastgelegde persoonsgegevens tegen verlies en/of tegen enige vorm van onrechtmatige verwerking te beveiligen. Dit omvat onder andere de volgende maatregelen:

- Via technische, organisatorische en juridische maatregelen waarborgen wij dat medewerkers van WUR en externen geen toegang kunnen krijgen tot de inhoud van (persoons)gegevens, behoudens voor zover bepaald in dit reglement.
- Alleen die medewerkers hebben toegang tot de persoonsgegevens, voor wie toegang noodzakelijk is in het kader van de uitvoering van hun werkzaamheden.
- Alle medewerkers die in het kader van toezicht en controle op dit reglement kennis moeten nemen van persoonsgebonden informatie zijn bovendien contractueel gebonden aan een aanvullende geheimhoudingsverplichting, behalve als enig wettelijk voorschrift hen tot mededeling verplicht of uit hun taak de noodzaak tot mededeling voortvloeit.
- WUR zal periodiek toetsen of de beheerders van de dienst zich bij de uitvoering van hun werkzaamheden houden aan de voor hen geldende afspraken ten aanzien van autorisatie, doelbinding en geheimhouding.
- Wij zullen periodiek toetsen of de partijen met wie de gegevens worden gedeeld zich houden aan de gemaakte afspraken.

2.4.2. Derde partijen

Wij delen de vastgelegde persoonsgegevens enkel met derde partijen wanneer dit noodzakelijk is voor de uitvoering van het onderzoek en de uitvoering van de eventuele disciplinaire maatregel. Zo kunnen wij de persoonsgegevens doorgeven aan de politie bij een vermoedelijk of geconstateerd strafbaar feit. Wij waarborgen dat, waar WUR persoonsgegevens deelt met externe organisaties, bindende afspraken worden gemaakt rond de verwerking van die gegevens door die externen die ten minste voldoen aan de uitgangspunten van artikel 28 AVG.

Het verstrekken van privé e-mailcommunicatie of privé-informatie op gegevensdragers van WU of het anderszins toegankelijk maken van de e-mail communicatie en informatie van een overledene aan nabestaanden, staat op gespannen voet met het integriteitsbelang van een overledene en het privacybelang van betrokken communicatiepartners[1]. Uitsluitend overdracht van de gevraagde informatie onder bepaalde waarborgen aan een betrouwbaar en in overleg met WU geselecteerd onafhankelijk bureau dat de informatie beoordeelt en vervolgens toestemming vraagt aan de communicatiepartners voor vrijgave, behoort tot de mogelijkheden. De aanvragende partij dient dit bureau zelf in te huren en de kosten hiervoor te dragen.

1

Er is immers het belang te respecteren dat over de e-mailcommunicatie niet meer bekend wordt dan wat overledene en communicatiepartners zelf aan derden (hebben) willen prijsgeven.

2.4.3. RECHTEN VAN BETROKKENEN, CONTACTGEGEVENS EN ALGEMENE BEPALINGEN

Het Reglement bescherming persoonsgegevens van WUR is van toepassing op de verwerking van persoonsgegevens in het kader van dit reglement. Klik hier voor meer informatie over de omgang met persoonsgegevens door WU, zoals ook de mogelijkheden voor het uitoefenen van de rechten op grond van de AVG

3. Consequenties van overtreding van dit reglement

Bij handelen in strijd met dit reglement of de algemeen geldende wet- of regelgeving en fatsoensnormen bij het gebruik van de Faciliteiten, kan het college van bestuur, afhankelijk van de aard en de ernst van de overtreding, disciplinaire maatregelen treffen, Faciliteiten blokkeren of juridische stappen nemen.

3.1. DISCIPLINAIRE MAATREGELEN

Hieronder vallen een waarschuwing, berisping, een tijdelijke afsluiting of beperking van de Faciliteiten (maximaal een jaar) en in extreme gevallen een beëindiging van de inschrijving als student.

Wij kunnen geen disciplinaire maatregelen (behalve een waarschuwing) treffen enkel op basis van een langs geautomatiseerde weg uitgevoerde verwerking van persoonsgegevens, zoals een constatering van een automatisch filter of automatische blokkade. Bovendien worden geen disciplinaire maatregelen getroffen zonder dat jij de gelegenheid hebt gekregen jouw zienswijze naar voren te brengen.

Voor zover er geen andere beroepsprocedures openstaan, heb je het recht om bezwaar te maken tegen onze beslissing tot het overgaan tot disciplinaire maatregelen. Je kan hiervoor terecht bij Loket Rechtsbescherming Studenten: legalprotection.students@wur.nl. Bezwaar dient schriftelijk en binnen zes weken na dagtekening van het besluit aangetekend te worden. Ben je het niet eens met de uitkomst van onze bezwaarprocedure, dan kan je binnen zes weken na dagtekening van het besluit op het bezwaarschift schriftelijk beroep aantekenen bij het College van Beroep voor het Hoger Onderwijs.

3.2. BLOKKEREN FACILITEITEN

Bij een constatering van een overtreding of verdacht gedrag kunnen wij, geautomatiseerd of handmatig, een tijdelijke blokkade van de betreffende faciliteit invoeren. Deze blokkade zal zolang worden gehandhaafd tot aangetoond is dat de oorzaak is weggenomen. Bij herhaling van de oorzaak kunnen disciplinaire maatregelen worden genomen.

3.3. AANGIFTE EN SCHADEVERGOEDING

Wij zijn te allen tijde gerechtigd om, na gedocumenteerd overleg met de hiervoor meest aangewezen disciplines binnen WU, aangifte te doen in geval van vermoede of geconstateerde strafbare feiten. Wanneer bij een strafrechtelijk onderzoek om onze medewerking wordt verzocht, zullen wij deze medewerking in lijn met de wet verlenen. Schade voortvloeiend uit een overtreding van dit reglement kan in opdracht van het college van bestuur door WU op de overtreder worden verhaald.

4. Slotbepalingen

Dit reglement kan door het bestuur worden herzien. Wijzigingen worden alleen bij het begin van een collegejaar doorgevoerd, behalve in dringende gevallen of wanneer wij door omstandigheden van buitenaf gedwongen zijn tot een snellere invoering.

Wijzigingen worden alleen ingevoerd, nadat de medezeggenschapsraad van de instelling daarmee heeft ingestemd. Het college van bestuur zal feedback van studenten in overweging nemen, alvorens de wijzigingen in te voeren.

In gevallen waarin dit reglement niet voorziet, beslist het college van bestuur.

Dit reglement is vastgesteld op 29 maart 2022 en is van kracht vanaf 1 september 2022.