Report on the topic of

Possible Implications of the EU Data Act on IoT Implementations and Data Practices in Arable Farming*

by

Can Atik**

November 2022

* This report (including any enclosures and attachments) has been prepared for the exclusive use and benefit of the BO Akkerbouw and solely for the informative purposes based on the author's (limited) capacity on the subject matter. The author does not accept any liability if this report or any evaluation in it is used for an alternative purpose other than it is intended, nor to any third party in respect of this report.

** PhD Candidate at Tilburg Law School with affiliation to the Tilburg Law and Economics Center (TILEC) and Tilburg Institute for Law, Technology, and Society (TILT).

I sincerely thank **Simone van der Burg** for her valuable comments and guidance during the writing process of this report.

Table of Contents

Executive Summary

This report offers an analysis of the Data Act proposal, released by the European Commission on 23 February 2022. The analysis looks at every article of the Data Act proposal and clarifies what it means for arable farmers. Furthermore, it draws conclusions with respect to the revision of the Code of Conduct on Arable Data Use that BO Akkerbouw formulated (Gedragscode Datagebruik Akkerbouw). We will look at whether and to what extent (a) the Data Act makes the Code of Conduct superfluous, and (b) whether the code needs to be revised to be compatible with the essential requirements of the Data Act, and (c) whether the code can be updated in a way that addresses the remaining issues, to which the Data Act proposal does not sufficiently attend. While reading, it is important to keep in mind that this is a legislative proposal and its provisions might be slightly amended until it passes through the European Parliament and Council. In the proposal, it is stated that the Data Act is effective 12 months after it is adopted, which means there will be no binding and enforceable set of data rights before 2024.

The Data Act proposal contains several layers. It provides data access and sharing rights for users of IoT devices. It imposes obligations on manufacturers of IoT devices (data holders) and third parties receiving data upon users' request. Provisions about unfair contractual terms aim to protect the weaker side of the contractual parties, which is most often the party, who has less digital knowledge and expertise. The Data Act proposal provides the conditions for public sector bodies' access to data in exceptional situations. Also, extra obligations are imposed on operators of data spaces, providers of cloud and edge services and vendors of smart contract applications regarding interoperability. To ensure compliance with the provided rights and rules, the new Data Act brings a mechanism for lodging a complaint to the competent authority that can impose penalties on breachers. The Commission will also publish model contractual terms for the stakeholders, to facilitate making contracts around the sharing of data.

What are the most important developments for farmers?

The most prominent provisions of the Data Act proposal for arable farmers are the right to data access (Art. 4) and the right to share data with third parties (Art. 5). At the outset it is however also important to realize that these provisions of the Data Act have some limitations, such as the following:

- Access and sharing rights are only applicable to farm data sets when they are collected by IoT devices (farm machinery) that are owned, rented or leased by a farmer, and if they are stored/controlled by the manufacturers of these IoT devices.
- Our analysis demonstrated that other farm data collection methods (such as via stable soil sensors, camera recordings and images, and manual observations that are digitalised later on) and locked-in farm data sets in the hands of other players (such as technology providers, data intermediaries or data cooperatives) seem not to fall under these data rights due to the very restrictive definitions.
- Furthermore, raw data sets can be accessible or shareable, but the information that is derived/inferred from the raw data sets such as ag-data driven solutions, suggestions or prescriptions, is outside the scope of this Regulation.

What are the potential challenges for farmers after the Data Act?

Data rights are granted to users, which refer to the ones who own, rent or lease the IoT device. This design may cause some problems in arable farming.

- Farmers do not always buy, rent or lease agricultural machinery from their manufacturers. Instead, they sometimes receive (for instance, harvesting) services from companies that own the machinery. This entails that they have to negotiate the conditions for access to data collected from their own fields with the company that provides the IoT service and which owns the technological device, rents it, or leases it from its manufacturer.
- Moreover, if several farmers buy a data-collecting IoT machine (like a tractor) together and share ownership, all owners seem to have equal rights to access and share all the data stored by the manufacturer regardless of who collected which data and at whose farm. This may give rise to confidentiality and trust issues in common agricultural machinery usage in arable farming as every user can access each other's farm data.

How will the Data Act intervention affect the data re-use (sharing) conditions?

- The Data Act allows data re-use (sharing) upon the request of users (farmers).
- However, there is an ambiguity about whether data holders (IoT device manufacturers) can share data with third parties even without the users' request.
- The Data Act leaves room for data holders to share the data if the possibility of sharing is stated in the contracts with users and if sharing does not harm the commercial position of users.
- It is not clear, though, whether the inclusion of a general statement about data sharing in the contract will be valid or whether the details of the data sharing should be specified in the contracts. Therefore, farmers should still be careful about the contractual clauses regarding the re-use of the data sets.

What are the prominent obligations of the data holders (IoT device manufacturers)?

There are specific obligations imposed on data holders in the Data Act.

- The data holders (the IoT device manufacturers) are obliged to be fair, reasonable, non-discriminatory and transparent when making data available to data recipients (e.g. another IoT device manufacturer, a digital service provider, a seed company etc.), who access the data from data holders upon users' (such as the farmer's) request.
- Data holders and data recipients will need to enter into an agreement regarding data access. The clauses of these agreements will not be binding if they restrict the users' rights over data.
- The Data Act also forbids data holders' discriminatory actions between their own enterprises and other data recipients when making data available.
- To protect users (farmers), the Data Act proposal prohibits data holders from using data to undermine users' commercial operations; for example, sharing the data of a farmer with competitors is prohibited.

What are the prominent obligations of the data recipients (ones who access data upon users' request from data holders)?

There are also specific obligations for third-party data recipients.

- They can only use data for the specific purpose that the user determined and they are obliged to delete the data when it is no longer needed for the agreed purpose.
- Coercing, deceiving or manipulating the user or preventing them to share data with others is clearly forbidden.
- The data recipients are not allowed to share data with other third parties.
- They are also obliged not to use the data to develop a product with the purpose to compete with the data holder (the IoT device manufacturer).
- These obligations are only valid for third parties with a turnover that exceeds the SME threshold; meaning that small start-ups and medium-sized companies are not obliged to follow these rules. The size of a company may, therefore, be a factor to consider for farmers before signing an agreement to share data with that company.

What are the essential requirements of the relationship between data holders and data recipients?

- Data recipients, who will access data upon users' requests (allowed under Article 5), will have to pay 'reasonable' compensation to data holders when accessing these data. In contrast, the right to data sharing can be used by users (farmers) free of charge. If the data recipient is an SME, then the amount it will have to pay will be up to *"the costs directly related to making the data available"*. Determining what 'reasonable compensation' is could be a major challenge in practice unless the Commission releases some guidelines to determine this.
- Parties can apply to dispute settlement bodies to settle their conflicts regarding the compensation to be paid. Decisions will need to be taken within 90 days.
- The data holders (the IoT manufacturers) are responsible for taking technical protection measures to prevent any unauthorised data access. In case of unauthorised data access, the data recipient is obliged to destroy the data sets and stop all business activities that are developed based on this unauthorised access. This sanction will not be enforced, though, when such access did not cause significant harm to the data holder or when it would be a disproportionate sanction. In practice, however, it may not be easy to clarify what 'significant harm' means and which data access causes significant harm, or to separate between a proportionate and disproportionate sanction, unless the Commission releases a detailed guideline.

What are the rules for the validity of contractual terms concerning data access and use?

The Data Act aims to protect the weaker party in contractual agreements.

- Unfair terms, which are unilaterally imposed on SMEs (and farms are also most often SMEs), will not be binding in the contracts.
- Thus, it is made impossible for powerful parties i) to limit their liability for intentional acts or gross negligence, ii) to exclude remedies in case of non-performance or breach of the contractual terms, and iii) to have an exclusive right to determine or interpret the contractual clauses when it comes to data access and sharing. These are *per se* unfair terms, which means they are always considered unfair.

- Beyond the *per se* unfair terms, the proposal also lists some 'presumably' unfair terms in contracts such as clauses about terminating the contract with unreasonably short notice, limiting the imposing parties' responsibilities in case of non-performance of contractual obligations or preventing other contracting parties from using the data without a legitimate ground.
- These provisions are a positive development for SME farms because they frequently face standard terms and conditions that can be considered as unilaterally imposed by the technology providers or machine manufacturers. However, while this is good news for farmers, it has to be noted that the statements about what 'unfair' terms are not fully clear and clarification of ambiguities may take several years in practice after many cases and court decisions. Therefore, it is important that farmers develop their own ideas about what unfair terms are and pay attention to them in contracts about data sharing and access until the law is clarified in this respect.

What are the other relevant provisions of the Data Act proposal for arable farmers?

- Chapter V of the Data Act proposal regulates exceptional situations where public bodies can access data such as, in the case of a public emergency.
- There are additional obligations in Chapter VI for the providers of cloud and edge services to ensure that their users are able to switch to an alternative cloud service providers smoothly. These obligations can be useful for the ones (such as farmers or other players in arable farming) who use cloud services to store their data sets. However, this part of the Data Act does not apply to agricultural technology providers or machine manufacturers, who control or store data but are outside the scope of these additional switching obligations.
- Chapter VIII of the Data Act provides specific 'interoperability' obligations for i) operators of data spaces, ii) cloud service providers and iii) vendors of smart contract applications. If the Commission creates a common European agricultural data space soon, the interoperability specifications for the operators of these data access hubs (including the one for agriculture) may indirectly help the development of sectoral data standards. However, the Data Act proposal does not provide any generally applicable obligation that can be used to force technology providers or machine manufacturers to develop data standards or comply with interoperability specifications. . Even if there are data rights for users (farmers) to access or share data with third parties, the data recipient may not meaningfully read and process the received data unless there are common data standards and interoperability specifications. This is a limitation from the sectoral perspective, where there are technical barriers to transferring data. As it may not be realistic to expect a huge change in the Data Act at this stage, possible future sectoral regulatory intervention should provide effective solutions towards sectoral data standards and interoperability solutions in the sector.
- For the enforcement of the Data Act, the Member States will have to assign enforcement powers to one or more competent authorities at the national level. There will be a mechanism to process complaints by these authorities and to impose financial penalties in case of non-compliance. This can be a trust-building development for the agriculture sector as far as the provisions of the Regulation cover farmers' concerns. However, Article 33(1) leaves the regulation of penalties up to the Member States and does not provide a framework with (minimum) boundaries that should be imposed. Unless the Commission will release further

guidelines for the Member States, trespassers may receive different fines in different countries.

- The European Commission will develop (sectoral) model contractual terms that may serve as guidance for companies to update their terms and conditions. This is also useful for users (farmers) when they enter into a contract, as it allows them to compare the alternative companies' terms and conditions with the use of this reference.

Despite the mentioned limitations of the horizontal Data Act proposal from the sectoral perspective, it is a step forward for arable farming, where the use of agricultural machinery is prominent. For the remaining issues that the Data Act does not yet cover, follow-up sectoral data regulations tailored to each specific sector (including an ag-data regulation) are signalled in the Data Act. Sectoral stakeholders and institutions (including BO Akkerbouw) can play a key role in providing deeper insights to policymakers in this regard. This would allow making policymakers more aware of the unsolved issues in agriculture when they are designing sectoral provisions, and this would increase the effectiveness of the possible future sectoral ag-data regulation.

Until then, BO Akkerbouw may update its code of conduct in line with the prominent principles of the Data Act preferably with some additional progressive rules to address the remaining issues from the sectoral perspective (as section 4 of this report provides a detailed list of suggestions in this regard). It may also enlighten farmers about their rights and warn them regarding possible nuances and limitations of the Data Act.

1.0 Introduction

On 23 February 2022, the European Commission ('the Commission' henceforth) released the proposal for a Regulation on harmonised rules on fair access to and use of data, namely the 'Data Act'.[1] The purpose of this regulatory intervention was stated to generate a *"cross-sectoral governance framework for data access and use by legislating on matters that affect relations between data economy actors, in order to provide incentives for horizontal data sharing across sectors."*[2] It particularly aims to address problems of the data economy connected to i) power imbalances between users and companies, ii) data concentration in the hands of a few players, iii) high entry barriers in data-driven markets, and thus, iv) restricted potential of data access and re-use.[3]

The Data Act provides a data access regime that includes obligations for manufacturers of 'products' to make data accessible,[4] users' rights to access and use data,[5] users' right to share data with third parties,[6] and obligations for third parties receiving data that are requested by the user[7] in addition to other provisions related to setting obligations for data holders to make data available,[8] addressing unfair terms related to data access and use between enterprises,[9] making data available to public sector bodies based on exceptional need,[10] or imposing interoperability obligations for the operators of data spaces.[11]

This is a proposal for now, and provisions in the regulation can be (slightly) changed before it enters into force. This poses an important opportunity for the affected stakeholders to respond and provide feedback on the design of this regulatory intervention. It is not certain yet when the Regulation will pass through the European Parliament and Council, but it is clearly

[1] Proposal for a Regulation (COM/2022/68 final) of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), 23.2.2022.

[2] Explanatory Memorandum, p. 1.

[3] Ibid., p. 2.

[4] Data Act, Article 3.

[5] Ibid., Article 4.

[6] Ibid., Article 5.

[7] Ibid., Article 6. User-centric data rights are listed in Chapter II of the regulation.

[8] See provisions in Ibid., Chapter III.

[9] See provisions in Ibid., Chapter IV.

[10] See provisions in Ibid., Chapter V.

[11] See provisions in Ibid., Chapter VIII.

declared in Article 42 of the proposal that provisions in the Data Act will apply 12 months after its entry into force. Therefore, even in the most optimistic scenario, it is not realistic to expect a binding and enforceable set of data rights before 2024.

As the Regulation brings 'basic rules for all sectors' as a horizontal intervention, one can wonder about the possible impacts of this Regulation on different sectors. This report will investigate the possible implications on data practices in arable farming. To evaluate the likely impacts, this report will use the prominent data practices and data-related problems connected to the implementation of the Internet of Things ('IoT') in arable farming as a starting point. Thus, it will seek answers to the following questions: *What will change when the new Data Act is implemented? How will stakeholders be affected?* And *To what extent would the Data Act be able to solve the data-related problems in the sector or mitigate their detrimental effects on the stakeholders?*

To start, section 2 provides an outline of the prominent IoT implementations and actors in arable farming as well as an overview of connected data access problems as a basis for the following evaluations regarding possible implications of the Data Act. Section 3 scrutinises the provisions of the Data Act article by article in order to identify to what extent it will affect IoT data usage practices and problems in arable farming. Section 4 provides general evaluations by answering specific questions for the readers who would prefer to skip the long legal technical analysis in section 3 and desire to directly reach the practical extracts. Section 5 concludes with the overall findings.

2.0 IoT Implementations and Data-driven Decision-Making in Arable Farming

The growing population of the world and increasing concerns regarding climate change pose a particular challenge to the capacity to ensure a sustainable food supply while also (at the same time) reducing the environmental impact of food production processes.[12] With the proliferation of IoT technologies, data-driven solutions in farming practices are increasing, and this paradigm shift from old-school decision-making towards data-driven farm management has tremendous potential to increase food production and make it more efficient and less burdensome for the environment.[13] IoT enables data flow between different data collection sources such as sensors, monitoring devices, machines, or even satellites, which allows

[12] See the earlier evaluations in this regard in Godfray et al., (2010) and Tilman, Balzer, Hill, & Befort, (2011).

[13] See, for instance, Wolfert, Ge, Verdouw and Bogaardt, (2017).

automatic data processing and analysis, supports decision-making on farms, and ultimately generates value and efficiency in agricultural production and management of farms.[14] At the same time, IoT technologies can be helpful to reduce the environmental impact of farming practices by avoiding unnecessary usage of chemical inputs such as pesticides, insecticides or fertilizers and natural inputs like water thanks to the early detection of problems and taking swift actions that offer responses specifically tailored to the needs of plants and soil by also taking into account weather conditions and predictions.[15] Thus, data-driven 'smart farming' practices promise an unprecedented potential to reconcile apparently incompatible objectives of increasing food supply and reducing environmental impact.[16]

2.1 Arable Farming and IoT Revolution

To discuss the impact of the Data Act proposal, it is important to know what we are talking about. Therefor we should first explore smart farming practices including the prominent data usage and sharing situations, and relevant actors in arable farming.

Being aware of the fact that it is not possible to list all the data-related practices and players in arable farming, this section only aims to distinguish the most important IoT implementations in arable farming and provides some examples of data collection, use and re-use. Furthermore, it will describe and position the sectoral actors. This will be used as a background when discussing the provisions of the recent Data Act proposal below.

2.1.1 IoT Usage in Arable Farming

Although there is no central registration of all the IoT practices in arable farming, there are open sources that provide some useful examples. IoT systems are mainly used in arable farming for four different purposes: monitoring the fields, documentation, forecasting possible outcomes and controlling agricultural operations.[17]

This section provides a basic outline of the IoT practices in arable farming and more detailed examples will be discussed below when evaluating possible implications of the particular provisions of the Data Act proposal.

[14] Villa-Henriksen et al., (2020).

[15] Villa-Henriksen et al., (2020).

[16] Foley et al., (2011).

[17] Villa-Henriksen et al., (2020).

2.1.1.1. Sensors collect data from the fields

In arable farming, sensors are used to measure different soil conditions such as moisture, composition, density, and crop location in order to generate insights regarding the use of inputs (water, fertilizer or chemicals) as well as timing, method and amount of these inputs.[18] Also, direct camera recordings and sensors equipped with cameras play a significant role to monitor many parameters such as detecting diseases.[19] Based on this measurement, different actuators, devices or machines equipped with IoT technologies are used for, for instance, seeding, weeding, spreading fertiliser, and spraying pesticides according to the needs of the soil or crops in the fields.[20] The notion of 'sensors' here is understood comprehensively. Data is collected by using sensors deployed in soil or attached to farm machinery as well as other methods. For instance, a remote technology, namely, near-infrared reflectance (NIR) is used to measure various things such as moisture, starch, protein, and oil content of a crop that can be critical for determining the harvesting time.[21] Also, 'remote sensing' covers the sensors installed in, for instance, Unmanned Aerial Vehicles (UAV) or even satellites.[22] Data collected by these various sensors are combined to produce the information that IoT offers to facilitate food production management.

2.1.1.2. IoT devices need smooth communication in the farming operations

Ensuring coordination of machines when reaping, threshing and winnowing the crops such as wheat, barley, oats, or oilseed is critical.[23] Communication facilitates automatic synchronisation to ensure the smooth operation of different machines on the field and to avoid any problem in the application of, for instance, spraying, fertilising or seeding.[24] The interoperability of various machines and sensors is, therefore, critical in this regard.

[18] Atzberger, (2013)

[19] Steen, Villa-Henriksen, Therkildsen, & Green, (2012); Thiessen and Heege (2013); Midtiby et al., (2018).

[20] Blackburn, (2006); Yanbo, Lee, Thomson, and Reddy, (2016).

[21] Caporaso, Whitworth, and Fisk (2018).

[22] Lieder, S., and Schröter-Schlaack, C. (2021)

[23] See De Baerdemaeker and Saeys (2013).

[24] Villa-Henriksen, Edwards, Pesonen, and Sørensen (2020).

2.1.1.3. Complementary data sets are needed beyond farm-specific data

Some combine harvesters have yield monitoring sensors to evaluate the conditions of the harvested grains and to generate yield maps.[25] Harvesters are also connected to the Global Navigation Satellite System, and thus, the relevant applications can identify the more or less fertile parts or the field.[26] By also using the retrospective analysis of the previous years' performance in the related parts of the fields, farmers are enabled to compare performance over previous years and use the information to take informed decisions about the application of the right amounts of agrochemicals in a tailored way.[27]

GPS data is also important to ensure that the harvester operates on the exact same route as the planter did in order to conduct precise harvesting without crop loss. In today's technology, satellite systems in agricultural machines let farmers drive on the required position only with a few centimetres deviation. [28] There is also fully automated agricultural machinery available which can operate without human operation or constant supervision.[29]

2.1.2 Distinct Features of IoT Technology in Arable Farming

Compared to the relatively controlled agricultural practices such as greenhouses or orchards, arable farming has certain distinct features when it comes to IoT implementation and data-driven Smart Farming practices;[30]

- The first difference is strictly related to the scale. Arable farming may be carried out on very large lands. This affects the design of the sensor deployment in the fields, data collection from the fields, and analysis of these farm data sets. Consequently, the role of spatial data is important in arable farming and serves to increase the precision of field insights. Spatial data is also critical to enable machinery employment for automatic recognition and actuation.[31]

[25] Pinter Jr et. al. (2003)4

[26] Mutschler, Ulicny and Reuters (2018).

[27] Corentin at al. (2018)

[28] See Corentin at al. (2018); Zagórda and Walczykova (2018); Du and Noguchi (2017); Michihisa , Ikemura, Suguri, and Masuda (2010).

[29] Ibid.

[30] Villa-Henriksen et al., (2020).

[31] Zude-Sasse, Fountas, Gemtos, & Abu-Khalaf, (2016).

- Heavy reliance on mobile sensors and other devices on farm machinery creates another novelty. Operation of different vehicles and machines requires smooth coordination that is dependent on mobile networks, communication implementations and real-time interoperability among machines and devices manufactured by different brands.[32]
- Large amounts of heterogeneous data sets coming from various sources need to be integrated smoothly. This requires the integration of stationary sensors, moving vehicles and implements, satellites, or data from web services.
- Environmental conditions and other external factors have a large impact on arable farming, as annual crops grown in open fields[33] are more vulnerable to geographical characteristics and weather conditions compared to other types of farming, such as fruit growing which uses permanent plants with deeper roots[34] or protected plants in greenhouses. This mandates that data processing in arable farming should include different data sets in order to reach precise insights and offer relevant information to farmers to enable them to take related measures.
- Data collection and processing is highly complex in arable farming due to the distinct types of field tasks. Each task from soil preparation and crop establishment or from highly varying plant nursing tasks to harvesting requires different treatment in terms of data collection, processing and actuation. Therefore, there is a need for perfect coordination between these stages.

2.1.3 Categorisation of Agricultural Data Sets

There are different categorisations of data sets used in agriculture. The European Commission categorised the following agricultural data sets: 1) farm data (collected from farms via sensors, machines or directly by farmers for tailor-made agronomic prescriptions); 2) complementary data (such as weather and other environmental data); and 3) proprietary data (such as data of an agricultural inputs company about its agronomic products (e.g. seeds, fertilisers or pesticides), research and development results, and any other exclusive information).[35]

[32] Martínez, Pastor, Alvarez, & Iborra (2016); Peets, Mouazen, Blackburn,Kuang, & Wiebensohn, (2012)

[33] It is important to note that horticulture is also done in open fields and has annual crops,

[34] Zude-Sasse et al., (2016)

[35] See Case No COMP/M.8084 – *Bayer/Monsanto*, European Commission Decision (29 May 2018), para. 2453.

Next to this categorization of data, there is also a different categorisation described in the literature, which is based on agricultural data collection processes. This categorization distinguishes between 1) machine-generated data (referring to data collection via sensors in machines, drones or even GPS data), 2) process-mediated data (commercial data coming from business processes of farms such as purchase or order records) and 3) human-sourced data (that are human recorded farm data sets to be digitalised later on).[36]

This report will mainly take into account the European Commission's categorisation as that provides a more logical analytical framework for the analysis of the possible implications of the recent Data Act proposal. However, the latter categorisation can also be helpful to distinguish the farm data sets based on their collection processes as machine-generated and human-sourced farm data are not the same from the Data Act perspective.

2.2 Prominent Problems Connected to Agricultural Data Access

Despite the numerous benefits of cost-efficient and environmentally friendly agricultural production, 'Smart Farming' is not free from problems. This section will explain the most prominent problems in the sector to sketch the background that is needed to understand the evaluation of the Data Act that will follow.

2.2.1 Legal problems

One of the most prominent discussions in the sector concerns a basic ambiguity regarding who has what rights over which agricultural data sets.[37]

The applicability of the General Data Protection Regulation[38] on agricultural data is considered unclear in earlier studies.[39] In 2018, a regulation on a framework for the free flow of non-personal data in the European Union was adopted to promote free data flow with

[36] Balducci, Impedovo, Informatica, and Moro (2018)

[37] See Jouanjean and others (2020); See the literature review regarding ag-data ownership discussions in van der Burg et al. (2019), pp. 3–5; Posada (2014), p. 9; Coble et al. (2016), p. 6; Rasmussen (2016), pp. 505, 507 and 515; Copa-Cogeca (2016), p. 4; EIP-AGRI (2016), p. 5; See also a detailed discussion in Atik and Martens (2021), pp. 373-379 and Atik (2022a).

[38] Regulation (EU) No. 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ('GDPR') [2016] OJ L 119/1.

[39] See Kritikos (2017); Jouanjean and others (2020); Atik (2021); Atik and Martens (2021) for the earlier discussions.

voluntary codes of conduct in data-driven sectors.[40] In line with this development, sectoral stakeholders in Europe developed voluntary rules regarding agricultural data sharing under the name of the 'EU Code of conduct on agricultural data sharing by contractual agreement'.[41] This code of conduct was a voluntary framework without any sanctioning mechanism for breachers.[42] The European Commission was indeed aware of the fact that the GDPR framework is not suitable for non-personal data-driven sectors and voluntary codes of conduct sometimes do not effectively address the sectoral problems.[43] Therefore, the Data Act aims to provide *"cross-sectoral governance framework for data access and use by legislating on matters that affect relations between data economy actors, in order to provide incentives for horizontal data sharing across sectors."*[44] This report will discuss to what extent Data Act is able to remove the present legal ambiguities over ag-data control.

2.2.2 Technical problems

Lack of data standards and interoperability problems between IoT devices constitute crucial technical challenges in Smart Farming.[45] Technical incompatibility prevents farmers from switching between digital services or machines, as they cannot always move their data sets from one provider to the next even if farmers are legally able to control the farm data sets.[46] The gap between systems of old devices and new devices can also be an element here as many farmers do not have the most up-to-data systems on their tractors and machines while modern devices on machines are better equipped to support data exchange, where as legacy systems are less equipped. So, it may also be up to the farmer to invest in updating the data systems (if that's possible) to make it work.

[40] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, OJ L 303, 59–68.

[41] EU Code of conduct on agricultural data sharing by contractual agreement (2018).

[42] See more evaluations on EU code of conduct in Atik and Martens (2021).

[43] See Explanatory Memorandum of Data Act.

[44] Ibid., p. 1.

[45] Esmeijer et al. (2015); Sundmaeker et al. (2016); Copa-Cogeca, (2016); Barbero and others, (2016); Jouanjean et al. (2020).

[46] Ibid.

Therefore, it is relevant to investigate whether the Data Act provides any obligation to generate and respect data standards for tech-providers of smart farming technologies or services or to ensure the interoperability of devices used in arable farming.

2.2.3 Particular consequences of the two problems related to ag-data control

As a result of these two main problems, there are particular problematic consequences in the sector. It is critical to be aware of them when discussing possible outcomes of the Data Act intervention.

2.2.3.1 Data Lock-ins

The absence of an undisputed legal mechanism for farmers to force the *de facto* data controllers to share data with third parties results in farm data lock-ins.[47] Farmers face struggles when switching to a rival technology provider or machine even if the alternative is much cheaper or better than the existing service or machine.[48] The bargaining power imbalances between farmers and the companies that exclusively control agricultural data sets create extra problematic consequences in such an environment.[49] The first-mover agricultural technology providers and/or machine producers have significant competitive advantages owing to exclusive control over the locked-in farm data sets while new entrants or smaller rivals face significant entry and expansion barriers due to the lack of data access.[50] It is also important to note that first-mover data controllers benefit from indirect network effects deriving from positive feedback loops (more users lead to more data that can be used to develop better services to attract more users in turn).[51]

The following analysis of the possible implications of the Data Act below will particularly consider whether the Data Act provisions are able to mitigate or remove the reasons or consequences of the lock-in problem in the sector.

[47] Jouanjean and others (2020), p. 9; Härtel (2020), pp. 7-9.

[48] SWD(2017) 2 final, p. 28; Sundmaeker et. al., (2016), p. 144; Wiseman, Sanderson, and Robb (2018), pp. 71–72; Jouanjean et al., (2020), pp. 17-25.

[49] See Sundmaeker et. al. (2016), p. 144; Verdonk (2019), pp. 118–119; Atik (2021), pp. 55 and 67-68; Atik and Martens (2021), p. 379.

[50] See detailed discussion in Atik and Martens (2021), pp. 373-379.

[51] Case No COMP/M.8084 – *Bayer/Monsanto*, European Commission Decision (29 May 2018), para 2837.

2.2.3.2 Lack of trust

Connected to the ambiguities regarding the legal control of data and possible consequences of adopting digital farming, farmers' lack of trust in technologies and services collecting their data is an important problem in the sector.[52] Considering that increasing the adoption rate of digital technologies in European agriculture is one of the policy aims,[53] addressing trust-related problems is critical.[54]

Therefore, the following discussion will also be focussing on the trust-related implications of the Data Act beyond general evaluations regarding the design of the provisions of this recent horizontal regulatory initiative.

2.2.3.3 Data fragmentation

Due to the legal and technical barriers, another connected problem in the sector is the fragmentation of ag-data sets.[55] In other words, the potential of 'Big Data' is significantly refrained by isolated data silos controlled by different technology and service providers exclusively. This hinders data-driven innovation and development of the sector.[56]

In this regard, this will be considered when evaluating the possible implications of the Data Act to identify whether the Data Act can be helpful to release the full potential of ag-data sets by addressing the problem of isolation of fragmented data sets.

2.2.3.4 Unanswered broader ag-data access needs

All these conditions result in unanswered ag-data access needs of third-party access seekers[57] to innovatively use ag-data sets in different markets in the farm-to-fork chain.[58] There

[52] Various sources report farmers' trust-related concerns in this regard. See, for instance, The Economist (2014); Esmeijer et al. (2015), pp. 26-27; Jouanjean et al. (2020); van der Burg, Wiseman and Krkeljas (2021).

[53] European Commission (2019)

[54] See, in particular, the importance of building trust in ag-data setting in 'Stakeholders Dialogue On Common European Data Spaces' (*Shaping Europe's digital future*, 2019) <https://digital-strategy.ec.europa.eu/en/library/stakeholders-dialogue-common-european-data-spaces> accessed 14 July 2022, pp. 5-8.

[55] Copa-Cogeca (2016), p. 3.

[56] Ibid.; Lianos and Katalevsky (2017).

[57] Referring to any other company, public body or non-profit organisation - beyond farmers and first-mover data controllers.

[58] See Atik (2022a) and Atik (2022b).

can be a lot of access seekers such as technology providers, landowners, agricultural land speculators, banks, insurance companies, data dealers, market operators of agricultural products, or agricultural investors.[59]

Therefore, the report will also discuss to what extent the Data Act can provide functional data governance for third parties' broader data access needs.

3.0 Data Act as a Horizontal Intervention and Possible Implications on IoT Usage in Arable Farming

To convey all the details regarding the legal implications of the recent Data Act on sectoral issues, this section will provide an elaborated legal analysis based on a chapter-by-chapter investigation of the Data Act provisions.[60]

Readers, who would like to directly reach more concentrated information regarding an overall evaluation of these provisions from the arable farming perspective or who seek some answers to specific questions, can skip this section and directly read section 4 below. They can always turn back this section for the details by using internal references provided within section 4.

3.1 Chapter I – General Provisions

Article 1(1) starts by declaring that the Regulation provides harmonised rules on making data available to users, data recipients and public sector bodies. The Regulation provides different provisions for different data access situations and actors. Article 1(2) follows by stating that the Regulation applies to manufacturers of 'products' or providers of 'related services' in the EU and their users.[61] Other parties to which the Regulation also applies are

[59] Coble et al. (2016), p. 6; See also Härtel (2020), pp. 9-10.

[60] The discussions in this section benefited from the previous academic research [see particularly Atik (2022a) and Atik (2022b)], but this report provides a distinct elaboration on the agricultural data access issues with the specific focus on IoT technology usage in arable farming. Also, this analysis takes into account the Data Act proposal document released on 23 February 2022 as there is no published new/updated official text yet as of 24 November 2022.

[61] There are two issues to be noted here. First, as the 'EU' emphasis is on the manufacturers, this formulation is open to the interpretation that users of these products or services can benefit from the Regulation regardless they are EU citizens/residents or not. It is obvious that companies that sell 'products' or 'related services' in the EU are bound by the rules regardless of their origin. Second, 'manufacturers of products' refers the IoT device manufacturers as it will be further elaborated in the discussion below.

listed as ‘data holders’, ‘data recipients’, ‘public sector bodies’ and providers of ‘data processing services’. Article 1(3) declares that the Regulation does not affect Regulation (EU) 2016/679 (known as the General Data Protection Regulation [GDPR]) and Directive 2002/58/EC (known as the e-Privacy Directive), but complements the right to data portability under Article 20 of the GDPR.

Article 2 provides definitions of the key notions used throughout the Regulation. This section does not cite them all here. They will be conveyed during the substantial discussion below when the occasion arises.

3.2 Chapter II - Business to Consumer and Business to Business Data Sharing[62]

3.2.1 Right to Data Access

Chapter II starts with Article 3 regarding the ‘obligation to make data generated by the use of products or related services accessible’;

> *“Products shall be designed and manufactured, and related services shall be provided, in such a manner that data generated by their use are, by default, easily, securely and, where relevant and appropriate, directly accessible to the user.”*[63]

Designing such a clear obligation on product (ag-machine) manufacturers is a positive development for farmers who are users of IoT devices in arable farming. Article 3(2) states that *“[b]efore concluding a contract for the purchase, rent or lease of a product or a related service, at least the following information shall be provided to the user, in a clear and comprehensible format”,* and also provide further details regarding this disclosure obligation,

[62] The Chapter II is summarised in the Explanatory Memorandum of the Data Act as follows: *“Chapter II increases legal certainty for consumers and businesses to access data generated by the products or related services they own, rent or lease. Manufacturers and designers have to design the products in a way that makes the data easily accessible by default, and they will have to be transparent on what data will be accessible and how to access them. Provisions in this Chapter shall not affect the possibility for manufacturers to access and use data from products or related services they offer, where agreed with the user. There is an obligation of the data holder to make such data available to third parties upon the request of the user. Users will be entitled to authorise the data holder to give access to the data to third party service providers, such as providers of aftermarket services. Micro and small enterprises will be exempt from these obligations.”* See, pp. 14-15.

[63] Article 3(1).

which are about data access conditions, possible third party access or communication channels with data holders. These are also useful provisions to build trust among users (farmers).[64]

Article 4 has the title of *"[t]he right of users to access and use data generated by the use of products or related services"* and Article 4(1) states that;

> *"Where data cannot be directly accessed by the user from the product, the data holder shall make available to the user the data generated by its use of a product or related service without undue delay, free of charge and, where applicable, continuously and in real-time. This shall be done on the basis of a simple request through electronic means where technically feasible."*

Having an explicit data access right, which has functional elements, is valuable for users (farmers). First of all, the notion of 'data' refers to any data regardless of personal or not.[65] This, therefore, undisputedly covers agricultural data sets, unlike GDPR provisions. Also, the "*continuously and in real-time"* emphasis is a functional addition here for the interoperability of different farm machinery and multiple technology services, especially considering that different operations such as seeding, irrigation or fertiliser/pesticide applications may require real-time access to the farm data (for instance, soil data).[66]

The remaining provisions in Article 4 provide some additional specifications regarding the enforcement of the right to access. Article 4(2) brings obligations for data holders to ensure necessary conditions for the users' data access, and Article 4(3) states trade secrets can only be shared if confidentiality against third parties is ensured. Article 4(4) prohibits users from using *"the data … to develop a product that competes with the product from which the data originate."*[67] As it is difficult to expect farmers to generate a competing IoT device by using the accessed data sets, this provision is more related to other sectors in which users have the capacity to produce competitive devices. Article 4(5) reminds the validity of the GDPR consent regime for situations where the data is personal.

Article 4(6) is particularly important from the sectoral perspective;

[64] However, there are significant limitations in terms of applicability of the provisions in this Chapter of the Regulation in the ag-data access setting. See following discussions below.

[65] Article 2(1).

[66] See Atik (2022b); See some evaluations on the technical part of the issue (interoperability) in Chapter VIII below.

[67] It is interesting that the provision restricts the creation of competitive 'products', but not for 'related services'. See also a detailed discussion on the prohibition of generating competing products when evaluating Article 6(2)(e) below.

"…The data holder shall not use such data generated by the use of the product or related service to derive insights about the economic situation, assets and production methods of or the use by the user that could undermine the commercial position of the user in the markets in which the user is active."

This brings important obligations to data holders that may relieve some of the farmers' concerns about, for instance, undesirable re-use of farm data to increase the prices of commodities, agricultural inputs or land rental prices based on their dependencies.[68] Recital 25 of the Regulation declares that this provision is indeed designed by considering (among other things) the farmers' concerns.[69] Therefore, this is a clear improvement for the sector and this may help build trust among farmers to a certain extent.[70]

The first sentence of Article 4(6) states that "*[t]he data holder shall only use any non-personal data generated by the use of a product or related service on the basis of a contractual agreement with the user…"* Connecting all the re-use possibilities to the users' discretion might seem a positive development from the farmers' autonomy perspective, but this limits the innovation possibilities, especially when considering the need for broader data access in and out of the farm-to-fork chain.[71] Also, it is not clear whether this is similar to the 'consent' mechanism in the GDPR (which is highly detailed and it is difficult to get a valid consent) or whether any generic provision for the re-use of data in contractual relations between users and machine producers would be sufficient.

Nevertheless, granting a clear right to data access is a significant step to protect users, and this design will have positive implications in the smart farming setting despite the limitations of these provisions that will be discussed below.

[68] See more about the concerns in Sykuta, (2016), pp. 64-65, and 70-71; Rasmussen (2016), pp. 511-515; Barbero et al. (2016), p. 224; Jouanjean et al. (2020), p. 7.

[69] *"This would, for instance, involve using knowledge about the overall performance of a business or a farm in contractual negotiations with the user on potential acquisition of the user's products or agricultural produce to the user's detriment, or for instance, using such information to feed in larger databases on certain markets in the aggregate (,e.g. databases on crop yields for the upcoming harvesting season) as such use could affect the user negatively in an indirect manner."*

[70] As mentioned above and will be discussed in detail below, these provisions are only applicable a part of agricultural data sets and only certain relationships between stakeholders on smart farming.

[71] See similar considerations about the consent provisions of EU and US voluntary codes of conduct in this regard in Atik and Martens (2021), pp. 384-386.

3.2.2 Right to Data Portability

Article 5 provides the *"[r]ight to share data with third parties"*. Article 5(1) states that;

> *"Upon request by a user, or by a party acting on behalf of a user, the data holder shall make available the data generated by the use of a product or related service to a third party, without undue delay, free of charge to the user, of the same quality as is available to the data holder and, where applicable, continuously and in real-time."*[72]

This is an extension of the right to access under Article 4. The design here is the same as the right to data access, and the same comments stated above are, therefore, valid. The main distinct function of this right is to transfer the data to a third party directly. This is also necessary for the interoperability of IoT devices and switching between different services. Therefore, it is a promising development for the sector to unlock farm data sets.

To ensure data would not be accumulated in the hands of powerful players as a result of this right, Article 5(2) excludes 'gatekeepers' defined in the Digital Markets Act[73] (DMA) from eligible third parties. Incentivising users to accumulate data is also forbidden for gatekeepers. It seems the legislator aims to prevent data accumulation in the hands of a few giants. This is also a relevant concern in the sector because vertically integrated agricultural conglomerates have more incentives and capabilities to accumulate ag-data.[74] One can wonder whether powerful sectoral players can be considered 'gatekeepers'. However, the term 'gatekeepers' only refers to core platform services listed in Article 2.2 of the DMA. This means agricultural technology providers or machine manufacturers are outside the scope of the definition even though there can be equally concerning consequences of data concentration in the hands of a few agri-business giants.[75]

The remaining provisions of Article 5 are largely a duplication of Article 4 in the context of the 'right to share data with third parties'. Article 5(4) particularly prohibits third parties from abusing any technical gap in the data holder's data infrastructure when accessing data under this provision.

[72] Article 5(1); Recital 31 also provides detailed statements on the matter.

[73] COM/2020/842 final.

[74] See a detailed discussion on the matter in the context of possible implications of ownership right design in the sector in Atik and Martens (2021), pp. 382-384.

[75] See early considerations in this regard in Atik and Martens (2021), p. 394.

These all seem relevant and promising for farmers and other stakeholders in arable farming, but there are significant limitations that need to be aware of in order to clearly see to what extent the Data Act really provides opportunities in arable farming.

3.2.3 Limitations of the Data Rights in the Ag-data Access Setting

The right to access (Article 4) and the right to share data with third parties (Article 5) are promising, but the formulation of these provisions and the definitions of the core concepts cause significant limitations for their applicability to the IoT practices in arable farming.

It has to be noted first that, Article 4 and Article 5 are only applicable to data generated by the use of a 'product' or 'related services', not all data. The beneficiaries of these rights are 'users' of the 'products' or 'related services'. Therefore, it is critical to understand the scope of these core notions to identify the applicability scope of these regulations in the ag-data access setting.

The notion of 'product' refers to *"tangible, movable item, including where incorporated in an immovable item, that obtains, generates or collects, data concerning its use or environment…"*[76] Farm machinery may fall under this definition.[77] However, It seems difficult to cover embedded sensors in the soil. Farmers' manual observations that are digitalised later on would not fall within the scope of the Regulation, as well. Also, Recital 15 clearly excludes recordings via cameras, tablets and smart phones from the scope of the Regulation.[78] This may exclude some important practices in the sector as camera recordings about crop developments, for instance, would not be considered product-generated data here. Therefore, it has to be noted that the 'product' definition does not undisputedly cover all farm data collection methods in the sector.

Indeed, 'product' is IoT devices in the eyes of the legislator. This can be easily seen from the statements in the Explanatory Memorandum where Article 4 is referred to *"[t]he*

[76] See Article 2(2).

[77] Indeed, Recital 14 clearly declares this by counting agricultural machinery amongst the possible 'products'. Beyond accessing machine-generated data, this can also be useful for aftermarket machine repair services. See Explanatory Memorandum, p. 6.

[78] "*In contrast, certain products that are primarily designed to display or play content, or to record and transmit content, amongst others for the use by an online service should not be covered by this Regulation. Such products include, for example, personal computers, servers, tablets and smart phones, cameras, webcams, sound recording systems and text scanners. They require human input to produce various forms of content, such as text documents, sound files, video files, games, digital maps."*

Internet of Things data access right" and Article 5 is stated as *"[t]he Internet of Things data access right for third parties upon the user's request"*.[79] Therefore, sole sensors, which are, for instance, embedded in the soil, waterways or storage spaces, might not be considered as 'product'. Also, data generated by these sensors are mostly not stored in the manufacturers of these sensors, but they are directly sent to the technology providers' databases, unlike the IoT devices whose manufacturers also store and control the data sets. Therefore, it is relevant to identify if the scope of the 'related service' covers sole technology providers that only process data and provide tailored agronomic solutions to farmers, suggestions or prescriptions, but that are not related to the IoT devices' production or control.

The notion of 'related service',[80] refers to services inter-connected with a 'product' (IoT device) to make it functional.[81] However, agricultural technology providers and their digital services that provide data-driven solutions, suggestions or prescriptions to farmers are sometimes unrelated to the function of the farm machines or any other IoT device that collects data. Farm machinery can be an actuator of these suggestions, but they can function without the suggestions of digital service providers, for instance, about irrigation, seeding, spraying or fertilising times and amounts. Technology providers store and process *inter alia* the farm data collected through any device, sensor, camera or even manually by farmers to provide tailored data-driven solutions, suggestions or prescriptions to farmers.[82] In this regard, most of the data

[79] See the relevant statement of *"… obligations of manufacturers of Internet of Things products or related services …"*, pp. 7-8; *"…there is a fairness problem with data generated in the Internet of Things context, and that manufacturers of connected products or related services should not be able to decide unilaterally on what happens to the data generated by such products…",* p. 10; "*The Internet of Things data access right for third parties upon the user's request limits the freedom to conduct a business and the freedom of contract of the manufacturer or designer of a product or related service. The limitation is justified in order to enhance consumer protection, in particular to promote consumer's economic interests. The manufacturer or designer of a product or related service typically has exclusive control over the use of data generated by the use of a product or related service, which contributes to lock-in effects and hinders market entry for players offering aftermarket services. The Internet of Things data access right addresses this situation by further empowering consumers using products or related services to meaningfully control how the data generated by their use of the product or related service is used and enabling innovation by more market players…"*, p. 13.

[80] defined as *"digital service, including software, which is incorporated in or inter-connected with a product in such a way that its absence would prevent the product from performing one of its functions"* See Article 2(3).

[81] Recital 16 have some further clarification in the same direction of this interpretation: *"It is necessary to lay down rules applying to connected products that incorporate or are interconnected with a service in such a way that the absence of the service would prevent the product from performing its functions..."*

[82] Wolfert et al. (2017), p. 72.

controlled by agricultural technology providers would be out of the scope of these data rights. Taken together, the data rights can barely be used for locked-in data sets in the hands of agricultural machine producers. This is a significant limitation for sectoral practices.

The definition of 'user' further limits the scope of the data rights under the Data Act proposal. 'User' refers *"a natural or legal person that owns, rents or leases a product or receives a services."*[83] Covering both legal and natural persons as entitlement holders is a plus for arable farming practices where farms may be run by individuals, families, or legal entities. However, *"that owns, rents or leases a product"*[84] part of the definition limits the scope for sectoral practices because not all data collection from the fields is done via owned, rented or leased machinery. Data collection can also be done by a third party that owns, rents or leases the farm machinery from the manufacturer. Without renting or leasing the machinery itself, farms sometimes enter into an agreement with a company to conduct the (for instance, seeding, spraying or harvesting) operation[85] in the field with their machines as farmers may not prefer to have all the machinery in its inventory. Similarly, farm machinery may be owned, rented or leased by a cooperative, but multiple farms use them. In these kinds of situations, farmers cannot access data directly from the machine manufacturers by using the right to access or right to share data. They would be dependent on the owners of these machinery to access data because the Data Act proposal links the rights over IoT devices and rights over data sets collected through their use. This entails that farmers need to negotiate with the machine owners when entering into agreements to access the data.

Another way of data collection from fields is 'remote sensing' referring to the sensors installed in, for instance, Unmanned Aerial Vehicles (UAVs) or even satellites,[86] and, therefore, the legal status of the data, which is collected by these devices, is critical to be discussed. Satellites and UAVs can take pictures of the fields and these are also important data sources in arable farming practices. Satellite images are considered as 'complementary data' instead of 'farm data' according to the Commission's categorisation of ag-data in the *Bayer/Monsanto* merger decision.[87] However, it is important the identify the applicability of the Data Act provisions here. The problem in this case of satellite images is related to the

[83] Article 2(5).

[84] See the same emphasis in Recital 18.

[85] Here, the provided operation (for instance, harvesting) cannot be considered a 'related service' as well because it is irrelevant to the function of a 'product' (harvester) – it is a sole harvesting operation.

[86] Lieder and Schröter-Schlaack (2021), pp. 6-7.

[87] See section 2.1.3 above.

definition of 'user' which refers to a legal or natural person who owns, rents or leases a 'product'. In this regard, it is impossible to access satellite images under the right to data access (Art. 4) or the right to share data with third parties (Art. 5) as it is unimaginable that farmers would own a satellite. However, the same cannot be said for UAVs or drones. As long as the farmer owns, rents or leases a UAV or drone, these rights can be enforceable against the producers of these 'products'. However, camera recordings seem outside of the scope of this regulation. [88] Even if other conditions are all met, video recordings may not be accessed or shared under the data rights of the Data Act. However, it has to be noted that UAVs or drones are sometimes equipped with a different kind of 'camera' than a normal video recording. So, one can easily argue that this is a recording that does not "*require human input to produce various forms of content"* unlike normal video recordings. Indeed, some remote sensing uses hyper and multispectral images[89] or thermal remote sensors for field scanning.[90] They may fall under the scope of the Regulation. However, video recordings or photos taken via smart phones or tablets by humans seem outside the scope of the Regulation even if they are related to the crops, fields and agricultural operations in arable farming. In this regard, the scope of the Data Act seems to exclude an important method of data collection in smart arable farming.

Also, Recital 14 states that *"The data represent the digitalisation of user actions and events and should accordingly be accessible to the user, while information derived or inferred from this data, where lawfully held, should not be considered within scope of this Regulation."* This means only raw farm data sets can be accessible and shareable by using the provided rights in Articles 4 and 5 and tailored data-driven suggestions, prescriptions or solutions are outside the scope.[91]

[88] *'In contrast, certain products that are primarily designed to display or play content, or to record and transmit content, amongst others for the use by an online service should not be covered by this Regulation. Such products include, for example, personal computers, servers, tablets and smart phones, cameras, webcams, sound recording systems and text scanners. They require human input to produce various forms of content, such as text documents, sound files, video files, games, digital maps.'* Recital 15 of the Data Act.

[89] Nasi et al., (2018)

[90] Khanal, Fulton, and Shearer (2017)

[91] Some argue that most of the data collection methods in the IoT setting contain some kind of data processing and, therefore, nearly all (raw) data sets can be excluded from the application of the Regulation. See Martens (2022). However, as this interpretation renders the Regulation nearly completely dysfunctional, practice would probably not adopt this reading.

Taken all together, only a part of locked-in farm data[92] in the hands of IoT device (ag-machine) producers will be accessible to farmers if they own, rent or lease the ag-machine, and other farm data sets[93] seem outside the scope unless the definitions of the core concepts are changed before the Regulation enters into force. It may not be realistic to expect a complete revision in a horizontal framework that will be applicable to all sectors. The Data Act focuses not just on agriculture, but on other sectors as well and these problems that play a role in agriculture may not (in the same way) play a role in other sectors. So, the design of the provisions is sometimes too general to cover some of the specific ag-data issues.

The most problematic part of the possible application of the Data Act provisions in arable farming is about data that is directly collected and sent to the technology providers' databases without parallel storage with the manufacturer of the IoT device or the data that is collected through stable sensors in the fields. Machine-collected ag-data sets, which are stored by the manufacturers of these devices, are more compatible with the envision of the legislator in this regard and they are supposed to be accessible and transferable by using Articles 4 and 5 of the Data Act as long as farmers rent, lease or own the agricultural machines.

Another problem of this design in the Data Act is about the situations where there is more than one owner of the farm machinery. Recital 20 states that the device can be owned, rented or leased by multiple parties that all have the rights to access and share data with third parties. This may cause confidentiality and trust related problems in the arable farming practice where the machine can be used by multiple farmers via a cooperative or a couple of farmers may commonly own some machines, and they may not want other users/owners of the machinery to access their data sets.

Also, it is not clear whether data rights and/or data control can be contracted out from the original rights holders (users).[94] By stating "*by a party acting on behalf of a user",* Article

[92] collected through farm machines and their connected services such as applications to track or control the automated farm machinery including milking robots' control apps or harvesting monitoring apps.

[93] Manual observation of farmers, data collected by embedded sensors in the fields, video recordings of the fields, data sets under the control of sole agricultural technology providers, and data collected by farm machineries that are not owned, rented or leased by the farmer.

[94] One may assume that data rights under Chapter II should be understood as inalienable by arguing that any other reading would make the provisions meaningless. However, in legal interpretation, one cannot add any meaning that does not exist in the text at all. More importantly, other chapters have clear statements to forbid changing the obligations via contracts. See Articles 8(2) and 12(2) in Chapter III as well as 13(8) in Chapter IV. This may even entail that the legislators intentionally kept silent in Chapter II in this regard. In particular, Art. 8(2) may appear

5 generates a possibility that users can assign their rights to other players. Powerful companies may collect these assignments from users (farmers) to control data flows. This may result in exacerbated lock-in situations.[95] Therefore, it is suggested that the Data Act should remove the "*by a party acting on behalf of a user"* part and clearly declare the inalienability of the rights from the original entitlement holders (users) before it enters into force.[96]

The limitations discussed above are about the user (farmer)-centric rights to access and share data. For the third-party data access seekers which can be any player in the farm-to-fork chain to develop a product or service, the Regulation does not provide any mandatory way of data access. Moreover, the first sentence of Article 4(6) restricts any data re-use possibilities with the contractual agreement between data holders and users. In this regard, voluntary sharing of data from data holders to other access seekers (without users' individual requests to share data) can only be possible if this is stated in data holders' contracts with users,[97] and if this sharing is not harmful to the commercial position of users.[98] It is not clear though whether particular data re-use conditions should be specified in detail or whether a general statement about letting data holders share data with third parties will be valid. This is a confusing design and highly restrictive in terms of third-party access possibilities while centralising users (farmers) for the fate of the data sets.

3.2.4 Obligations of Third Parties

Article 6 regulates *"[o]bligations of third parties receiving data at the request of the user";*

to cover the protection of original allocation in Chapter II, however, it is a provision under Chapter III and it only restricts contractual provisions for making the data available between data holders and data recipients. In other words, it is not for user and data holder contractual relations or an overarching statement to protect the original allocation of data rights in the Regulation. If the statements (similar to the ones after the first sentence of Art. 8(2)) had been placed at the end of Chapter II clearly, this ambiguity on waivability of rights would have not existed. So, at best, it is not crystal clear whether data rights under Chapter II are inalienable (waivable via contracts).

[95] A similar discussion is provided regarding the detrimental consequences of a data ownership design for farmers' autonomy in Atik (2022a).

[96] See suggestions to refine the Data Act design from the smart farming perspective in Atik (2022b).

[97] See the first sentence of Article 4(6).

[98] See the second sentence of Article 4(6).

"A third party shall process the data made available to it pursuant to Article 5 only for the purposes and under the conditions agreed with the user, … and shall delete the data when they are no longer necessary for the agreed purpose."[99]

This is a clear purpose limitation obligation for third parties. This is compatible with the user-centric design in the previous provisions of Chapter II. The addition here is the data deletion obligation for third parties whenever the purpose of access disappears. From the perspective of users (farmers), it may be considered a positive development to relieve their concerns regarding the unintended re-use of data. However, this may also cause data losses in exceptional situations. Users generally do not have parallel data storage and they are dependent on machine manufacturers or service providers to store and process their data sets. If the data is lost in hands of the data holder for any (technical) reason, this data deletion obligation for the third parties might cause irreversible user harm. To avoid this, it might be useful to insert an additional statement in this provision to oblige third parties to take explicit confirmation from users before the destruction of data sets before the Regulation enters into force.[100]

Article 6(2) prohibits third parties from (a) acting in a coercive, deceiving or manipulative way to limit autonomy, decision making or freedom of choice of users, (b) using the data for profiling individuals by referring to GDPR, (c) transferring data to another third party unless it is necessary for providing services to the user, (d) transferring data to a 'gatekeeper',[101] (e) using "*the data it receives to develop a product that competes with the product from which the accessed data originate or share the data with another third party for that purpose"*, and (f) preventing *"the user, including through contractual commitments, from making the data it receives available to other parties"*. Although these obligations can be considered an additional protection for farmers, they are only imposed on third parties, not the data holders. Also, the scope here is also restricted with 'data generated by the use of a product or related service' to be shared with third parties under the right to share data (Article 5). Therefore, it would be more functional if similar obligations (for the data holders that control the data in the first place) are inserted into the Regulation.

The content of the obligations in Article 6(2)(a) and 6(2)(f) are worth to be discussed in depth in the context of this report.

[99] Article 6(1).

[100] See a discussion on purpose limitation and its appropriateness in the context of non-personal ag-data, including the data deletion obligations in Atik and Martens (2021), p. 388. See also Atik (2022b).

[101] defined by the Digital Markets Act. See 3.2.2 above.

Article 6(2)(a), which emphasises autonomy, decision making and choice, can be better understood in light of the statements in Recital 34 regarding dark patterns;

> *"… third parties should not rely on so-called dark patterns in designing their digital interfaces. Dark patterns are design techniques that push or deceive consumers into decisions that have negative consequences for them. These manipulative techniques can be used to persuade users, particularly vulnerable consumers, to engage in unwanted behaviours, and to deceive users by nudging them into decisions on data disclosure transactions or to unreasonably bias the decision-making of the users of the service, in a way that subverts and impairs their autonomy, decision-making and choice."*

This kind of a prohibition would be useful for users (farmers) because there might be similar concerns in the sector. For instance, third parties that access data can be agricultural input usage prescription services, and they may prescribe their own brand agricultural inputs (seed, pesticide or insecticide) without a legitimate reason over alternative brands (self-preferencing) or they may prescribe more input than needed to increase their upstream input sales. However, this obligation is only valid for third parties, who access data upon users' request. Farmers' relations with digital services will remain untouched in the existing design. It can be suggested that the scope of this obligation should cover all data holders (instead of being limited to third parties) before the Regulation enters into force. Thus, the potential impact on the sector would increase.

Article 6(2)(f)[102] only prevents the third party from restricting users to transfer the data to another party via contractual commitments. That is a useful provision to protect users (farmers), especially from situations where their rights can be limited or contracted out due to standard terms and conditions. However, there is no open declaration that data rights in the Regulation cannot be contracted out. In other words, it is unclear what happens when users waive or transfer their data rights via contracts. Also, a similar obligation is missing for the data holders in the first place. Therefore, this provision may bring limited benefits as long as the original data holder can exclusively control the data. So, the same obligation for data holders should be inserted in the Regulation. As a more functional alternative, the rights under Articles 4 and 5 can explicitly be declared as inalienable and un-waivable from users. Thus, they can always access and transfer their data regardless of a contractual clause to limit them or to transfer the data rights to other parties.[103]

[102] "*Third party shall not … prevent the user, including through contractual commitments, from making the data it receives available to other parties."*

[103] See more about the origins of the argument in Atik (2022a).

3.2.5 Scope of the Provisions in Chapter II

Article 7(1) states that *"[t]he obligations of this Chapter shall not apply to"* SMEs. This entails that the exclusion of SMEs is not limited to the obligations imposed under Article 6, but covers any obligation provided in Chapter II including the obligation to make data available to users or third parties upon users' request.

The goal here seems to avoid overburdening SMEs with binding data rights and obligations in Chapter II to let them grow and compete with powerful rivals. However, this also means that SMEs can lock farm data sets in. This is a problematic situation from the users' perspective. If users are satisfied with the products of a small start-up, they would not leave. Otherwise, users should be free to switch to an alternative with their data sets. This is what the competition on merits is. Protecting inefficient players just because they are week without considering its effects on consumer welfare[104] is not compatible with the objectives of this Regulation. If the Regulation passes as is, this provision may cause users not to prefer working with small start-ups to avoid data lock-ins that further exacerbate the concerns regarding the domination of a few tech giants in the data-driven sectors.

[104] In the context of this analysis, farmer (as user) welfare would also affect the final consumers of the agricultural products.

3.3 Chapter III - Obligations for Data Holders Legally Obliged to Make Data Available[105]

3.3.1 Non-discrimination obligations

Chapter III of the Regulation starts with Article 8 on *"[c]onditions under which data holders make data available to data recipients".* Article 8(1) obliges data holders[106] to be fair, reasonable, non-discriminatory, and transparent when making data available to data recipients[107] under the provisions of Article 5 or any other (future) regulation that mandates data access.

Article 8(2) states that;

> *"A data holder shall agree with a data recipient the terms for making the data available. A contractual term concerning the access to and use of the data or the liability and remedies for the breach or the termination of data related obligations shall not be binding if it fulfils the conditions of Article 13 or if it excludes the application of, derogates from or varies the effect of the user's rights under Chapter II."*

This provision is valuable in terms of content because it is an attempt to protect users by declaring the invalidity of contractual clauses whenever they may limit the rights designed in Chapter II, but the same cannot be stated for its scope. These statements are only valid for the arrangements between data holders and data recipients. It does not cover the contractual

[105] The Chapter III is summarised in the Explanatory Memorandum of the Data Act as follows: "*Chapter III sets out general rules applicable to obligations to make data available. Where a data holder is obliged to make data available to a data recipient as in Chapter II or in other Union law or Member State legislation, the general framework addresses the conditions under which data is made available and the compensation for making data available. Any conditions will have to be fair and non-discriminatory, and any compensation will have to be reasonable, without precluding other Union law or national legislation implementing Union law from excluding compensation or providing for lower compensation for making data available. Any compensation set for SMEs cannot exceed the costs incurred for making the data available, unless otherwise specified in sectoral legislations. Dispute settlement bodies certified by the Member States may assist parties that disagree on the compensation or conditions to come to an agreement."* See p. 15

[106] defined as *"legal or natural person who has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation implementing Union law, or in the case of non-personal data and through control of the technical design of the product and related services, the ability, to make available certain data"* See Article 2(6).

[107] defined as "*a legal or natural person, acting for purposes which are related to that person's trade, business, craft or profession, other than the user of a product or related service, to whom the data holder makes data available, including a third party following a request by the user to the data holder or in accordance with a legal obligation under Union law or national legislation implementing Union law"* See Article 2(7).

relationship between data holders and users (farmers) in the first place.[108] The scope here is further limited to the terms regarding "*access to and use of the data",* which means other contractual terms that may prevent users from switching IoT devices or services such as imposing penal clauses are outside the scope.[109]

Article 8(3) forbids data holders' discriminatory actions between their own enterprises[110] and other data recipients when making data available: *"…it shall be for the data holder to demonstrate that there has been no discrimination."*[111] Article 8(4) complementarily states that *"[a] data holder shall not make data available to a data recipient on an exclusive basis unless requested by the user under Chapter II."* These provisions are only for the data access of data recipients upon users' request. Conditions for direct access to wide farm data sets by third parties are outside the scope of these non-discrimination obligations. This means whenever a company request data access from the data holder to train algorithms, to develop new services, or to generate a competitive service or product without users' particular request, free market conditions and general legal framework are valid. However, by considering the user-centric design of the Data Act, direct access to wide farm data sets may not be possible without the users' confirmation.[112]

3.3.2 Compensation for Data Access

Article 9 regulates *"[c]ompensation for making data available"* for data holders to be paid by data recipients. This means when users (farmers) are switching to a new company, they can use their right to share data with third parties (Article 5) for free, but the new company will have to pay compensation to the data holder. The compensation shall be 'reasonable',[113] and

[108] See also Article 12(1): *"[t]his Chapter shall apply where a data holder is obliged under Article 5, or under Union law or national legislation implementing Union law, to make data available to a data recipient."*

[109] It has to be noted that these kinds of actions are subject to general regulations of contract law, and they cannot be imposed limitlessly.

[110] *"'enterprise' means a natural or legal person which in relation to contracts and practices covered by this Regulation is acting for purposes which are related to that person's trade, business, craft or profession"* See Article 2(8)

[111] Recital 41 states that *"It is not unlawful discrimination, where a data holder uses different contractual terms for making data available or different compensation, if those differences are justified by objective reasons."* This is very close to the abuse of dominance defence model. It seems that the data holders are considered a dominant player in terms of exclusively controlling the necessary data sets.

[112] See the discussion in the end of 2.3.3 above.

[113] Article 9(1).

the amount shall not *"exceed the costs directly related to making the data available"* if the data recipient is an SME.[114] Also, the compensation shall not be discriminatory in accordance with Article 8(3).[115] Article 9(4) brings an obligation to data holders to provide details of the calculation to the recipient to let it verify the amount. However, there is no other detail about the envisaged model beyond these general statements.

Determining the compensation amount would be the main challenge in practice due to the limited and abstract statements in the Article. SMEs are protected with a relatively clear scope of "*costs directly related to making the data available"*, but players, which are bigger than SMEs, have to understand what 'reasonable' is based on free contractual relationships. Also, regardless of the compensation amount, it has to be kept in mind that data recipients (for instance, a new technology provider or machine manufacturer) can pay first, but the access costs would be transferred to users (farmers) in the end with higher prices of services or machines by considering the fact that companies would not absorb these costs by waiving profits.

Compensation amounts to be paid could have been designed as low as possible for all situations if consumer welfare[116] is centralised as a regulatory objective. Also, a uniform calculation model could have been preferred to increase clarity. At least, there is a need for guidelines to clarify the existing design of the provisions[117] such as the maximum amount to be charged and its calculation methods. Otherwise, the main discussions in the post-regulation period will be about the question of 'what is reasonable?'.

3.3.3 Dispute settlement between data holders and data recipients

Article 10 provides a mechanism to settle disputes regarding "*the determination of fair, reasonable and non-discriminatory terms for … making data available in accordance with Articles 8 and 9."*[118] The Member States are responsible to create dispute settlement bodies, which shall be impartial/independent, have the previous expertise in determining FRAND

[114] Article 9(2).

[115] Article 9(3) states that these provisions shall not preclude other (sectoral) regulations without compensation or with lower ones.

[116] to prevent higher prices for farmers and final consumers of the agricultural products in the context of the analysis of this particular report.

[117] See similar considerations in Graef and Husovec (2022).

[118] Article 10(1).

terms, use electronic communication to be easily accessible, and are capable of swift, efficient and cost-efficient decisions.[119]

Parties in conflict will express their arguments,[120] and the dispute settlement body will decide within 90 days.[121] This decision shall only be binding if this is agreed on by the parties before the dispute settlement.[122] So, parties can also apply court or tribunal of a Member State.[123] However, the data holders can prefer long judicial processes as a method to deter users from switching. This can happen, especially when the data sets are indispensable for a feasible switching and when users are not able to wait till the end of the dispute settlement process. To prevent this possibility, the design of the dispute settlement mechanism can be changed as mandatory. In addition to that, users may face problems, especially when accessing the data is time-sensitive and users (farmers) cannot wait 90 days. This can make the switching impossible for some users. Even if switching can still be possible, disconnection from the relevant data sets for up to 90 days may reduce the quality of the given service and users may suffer from this. This may significantly harm the ongoing (farming) operations of users (farmers).

Therefore, a complementary provision may need to be inserted in this Article. The data access should always be granted immediately upon users' request to prevent delays and any connected harm to users. The amount can always be paid retrospectively after the dispute settlement process end.[124] This may be a more user-friendly mechanism.

3.3.4 Consequences of unauthorised data access

Article 11(1) imposes an obligation to data holders to apply appropriate technical protection measures to prevent unauthorised data access and compliance with the users' data rights. Article 11(2) states that the data recipient shall destroy the data sets (that are gained through unauthorised access) and stop its business activities developed based on this unauthorised data access. The recipient does not have to stop business activities if such data use did not generate significant harm to the data holder or if this sanction would be disproportionate compared to the interests of data holders.[125]

[119] See Article 10(2).

[120] Article 10(6).

[121] Article 10(7).

[122] Article 10(8).

[123] Article 10(9).

[124] See Atik (2022b).

[125] Article 11(3).

Obviously, the legislator tried to seek a balance between deterring unauthorised access to data and not being too destructive for unauthorised data recipients. This is indeed compatible with the overarching aim of the Regulation, but the statements in this article are too open. In particular, it is not easy to determine whether the unauthorised access caused 'significant harm' to data holders or whether the destruction of business sanction would be 'proportionate' or not as there is no clear test proposed in the Regulation to determine 'significant harm' or 'proportionality'. Therefore, unless the Commission publish guidelines to clarify these open issues, this will be the main ambiguity in practice.

Although these provisions are another indicator of the user-centric design of the Data Act, there is no definition of authorised data access or unauthorised data access. One can assume that authorised access refers to data transfers upon users' request (Article 5). This strengthens the view that Data Act restricts data re-use opportunities at the users' discretion. This can provide users (farmers) significant control over data, but may have detrimental effects on data-driven innovation as broader access to non-rivalrous data[126] is critical for the development of digital technologies.

3.3.5 The Scope of the Provisions in Chapter III

Article 12(1) clarifies that *"[t]his Chapter shall apply where a data holder is obliged under Article 5, or under Union law or national legislation implementing Union law, to make data available to a data recipient."* This indeed confirms the evaluations above regarding the scope of the non-discrimination obligations. Article 12(2) states the invalidity of any contractual clause that prevents the effectiveness of the provisions in this chapter of the Regulation. Article 12(3) states the validity of the provisions in this chapter for a possible future EU law or national regulation that implements obligations to make data available.

[126] Data is not like physical objects that can be used by one party at one time. It is not possible to use a tractor by multiple farmers at the same time, but data can be processed by unlimited players without harming its original use. This does not fade the fact that there are other reasons to limit data access such as privacy, trade secrets, monetary exploitation of exclusive data access etc. See some discussions in this regard in Atik and Martens (2021).

3.4 Chapter IV - Unfair Terms related to Data Access and Use between Enterprises[127]

3.4.1 Invalidity of Unfair Terms Imposed on SMEs

Chapter IV starts with Article 13, which regulates *"[u]nfair contractual terms unilaterally imposed on a micro, small or medium-sized enterprise"*;

> *"A contractual term, concerning the access to and use of data or the liability and remedies for the breach or the termination of data related obligations which has been unilaterally imposed by an enterprise*[128] *on a micro, small or medium-sized enterprise*[129] *... shall not be binding on the latter enterprise if it is unfair."*[130]

This is also a positive step for the sector where a significant number of the users of technology providers can be considered SMEs (for instance, family farms).[131] However, bigger farms' presence as a user of digital technologies is likely to be more than their general representation in the traditional agriculture sector. The findings demonstrate that "*farm size has the largest average importance, followed by education…"* when it comes to the question of who adopts digital technologies most in the agriculture sector.[132] Therefore, the unfair

[127] The Chapter IV is summarised in Explanatory Memorandum as follows: *"Chapter IV addresses unfairness of contractual terms in data sharing contracts between businesses, in situations where a contractual term is unilaterally imposed by one party on a micro, small or medium-sized enterprise. This Chapter guarantees that contractual agreements on data access and use do not take advantage of imbalances in negotiating power between the contractual parties. The instrument of an unfairness test includes a general provision defining unfairness of a data sharing-related contractual term complemented by a list of clauses that are either always unfair or presumed to be unfair. In situations of unequal bargaining power, that test protects the weaker contractual party in order to avoid unfair contracts. Such unfairness impedes the use of data by both contractual parties. With that, the provisions ensure a fairer allocation of value in the data economy. Model contractual terms recommended by the Commission may assist commercial parties in concluding contracts based on fair terms."* p. 15. For model contractual terms, see Chapter IX below.

[128] defined as *"a natural or legal person which in relation to contracts and practices covered by this Regulation is acting for purposes which are related to that person's trade, business, craft or profession"* See Article 2(8).

[129] as defined in Article 2 of the Annex to Recommendation 2003/361/EC: *"... (SMEs) is made up of enterprises which employ fewer than 250 persons and which have an annual turnover not exceeding EUR 50 million, and/or an annual balance sheet total not exceeding EUR 43 million."*

[130] Article 13(1).

[131] Especially when considering the statistics that farming is predominantly a family business in Europe. See Eurostat (2016).

[132] See in Shang et al. (2021), p. 12.

contractual terms framework in the Data Act would not be applicable to big farming operations if they exceed the turnover limit of the SME definition. It should be kept in mind that the bigger the farming operations, the more the switching costs and the harsher the effects of data lock-ins. Also, having more turnover than SME definition as a farm business does not necessarily create bargaining power vis-à-vis vertically integrated agricultural giants and their standard terms and conditions. Therefore, this report suggests a change in the design of the Data Act. If not happens, a possible future sectoral intervention should be designed with more comprehensive provisions in accordance with the sectoral needs.[133]

An interesting issue to be noted here is that the article does not use the restrictive statement of "*data generated by the use of a product or related service"* that is used in the previous chapters. This brings about the ambiguity of whether this article refers to all data or this is just an omission issue. If the former is the case, the rules provided in this article can be valid for any data-related terms that are unilaterally imposed on SMEs. This theoretically covers the relationship between technology providers and farmers (as long as they are SMEs). This would be a positive interpretation for the sector as data rights under Chapter II are only applicable to a part of farm machinery data. If this is only an omission and the word 'data' in Article 13 refers "*data generated by the use of a product or related service"*, the scope of these provisions would be restricted to the relationships between farmers and machinery manufacturers - from the sectoral perspective. This ambiguity should be clarified in favour of the broader interpretation.[134]

3.4.2 Provisions that define 'unfair terms'

Article 13(2) states that *"[a] contractual term is unfair if it is of such a nature that its use grossly deviates from good commercial practice in data access and use, contrary to good faith and fair dealing."* Article 13(3) lists three *per se* unfair situations while Article 13(4) provides five presumably unfair contractual terms.

Article 13(3) provides that unilaterally imposed terms[135] are unfair if their object or effect is (a) to exclude or limit the intentional acts or gross negligence liability against SMEs,

[133] See previous suggestions in this regard in Atik (2022a) and Atik (2022b).

[134] Atik (2022b).

[135] *"A contractual term shall be considered to be unilaterally imposed within the meaning of this Article if it has been supplied by one contracting party and the other contracting party has not been able to influence its content despite an attempt to negotiate it. The contracting party that supplied a contractual term bears the burden of proving that that term has not been unilaterally imposed."* Article 13(5).

(b) to exclude remedies available for SMEs in case of non-performance of contractual obligations or the liability of imposing party for breach of those obligations, or (c) to provide the imposing party with an exclusive right to decide whether data supply is compatible with the contract or to interpret any term of the contract.

Article 13(4) lists presumably unfair terms that are (a) inappropriately limiting the remedies in case of non-performance of contractual obligations or the liability in case of breach of those obligations, (b) allowing the imposing party to access and use the data in a way that is significantly detrimental for the other contracting party, (c) preventing other contracting party from using the data contributed or generated by that party or limiting the use of such data without having entitlements to do so, (d) preventing the other contracting party from obtaining a copy of the data contributed or generated by that party during the period of the contract or within a reasonable period after the termination of contract, (e) enabling the imposing party to terminate the contract with an unreasonably short notice that limits the possibilities of the other contracting party to switch to an alternative service and that cause financial detriment, except where there are serious grounds for doing so.

These are valuable provisions to create, at least, a framework to invalidate unfair contractual terms imposed by the powerful side of the contractual parties. This is, therefore, promising for the farmers who have to accept the standard terms and conditions of the technology providers and machine manufacturers as a weaker side of the contract. However, it has to note that most of the statements especially Article 13(4) are highly open-ended and somehow ambiguous. For instance, the determining the real meanings of 'inappropriate' in Article 13(4)(a), 'significantly detrimental' in Article 13(4)(b), 'entitlement' in Article 13(4)(c), 'reasonable period' in Article 13(4)(d), and 'unreasonably short notice' or 'serious grounds' in Article 13(4)(e) is not an easy task for the courts, and this will take years to have a relatively clearer understanding with precedents (case law) on these matters.

However, it is still necessary to discuss the possible implications of the most relevant ones among these provisions from the sectoral perspective. For instance, 13(4)(b)[136] can particularly help to ease farmers' concerns regarding the unintended use of farm data by the companies by observing farmers' dependencies and charging higher prices for commodities or

[136] "*A contractual term is presumed unfair for the purposes of this Article if its object or effect is to … allow the party that unilaterally imposed the term to access and use data of the other contracting party in a manner that is significantly detrimental to the legitimate interests of the other contracting party."*

by undermining farmers' commercial position in any other way.[137] Article 13(4)(c)[138] and (d)[139] can be useful to address the possible contractual terms that limit farmers on the already collected farm data sets. This means unilaterally imposed clauses to prevent farms from using the data will be presumed unfair. Even though this is a less strong assumption compared to *per se* unfair terms, it is still important for the sector, especially when recalling that the data rights in Chapter II are not declared as inalienable and un-waivable. These provisions can support the users' data rights to a certain extent.

3.4.3 Limitations of the unfair terms provisions

Despite the explained benefits, there are significant limitations regarding the applicability of these rules from the sectoral perspective. The first limitation is related to the 'unilaterally imposed'[140] emphasis in the article because unilateral imposition allegations can be dropped by inserting a claptrap negotiation stage before parties enter into agreements. The negotiations might not change the outcome if users (farmers) have limited awareness of the consequences of the contractual clauses.[141] The second limitation is related to the fact that contractual terms can only be invalid when they are imposed on SMEs. This excludes bigger farms even though they may also suffer from unfair contractual terms with possibly higher detrimental impacts as explained above. The third limitation is about the scope of the rules,

[137] See the considerations in Chapter II above as well. Recital 25 and Article 4(6) also respond to farmers' concerns in this regard.

[138] preventing SMEs (with a unilaterally imposed term) from using the data, which are generated or contributed by the SMEs during the contractual period or limit "*use, capture, access or control such data or exploit the value of such data in a proportionate manner",*

[139] preventing SMEs (with a unilaterally imposed term) *"from obtaining a copy of the data contributed or generated by that party during the period of the contract or within a reasonable period after the termination thereof"*

[140] Definition of 'unilateral imposition' is provided in Article 13(5). However, recital 52 states that: *"... not all contractual terms should be subject to an unfairness test, but only to those terms that are unilaterally imposed on micro, small and medium-sized enterprises. This concerns 'take-it-or-leave-it' situations where one party supplies a certain contractual term and the micro, small or medium-sized enterprise cannot influence the content of that term despite an attempt to negotiate it. A contractual term that is simply provided by one party and accepted by the micro, small or medium-sized enterprise or a term that is negotiated and subsequently agreed in an amended way between contracting parties should not be considered as unilaterally imposed."*

[141] See some considerations on farmers' attitude in this regard in Jouanjean et al. (2020), p. 9 and Härtel (2020 b), pp. 7-9; A research in Australia shows that 74% of farmers were not aware of the terms and conditions of their digital service providers. See Wiseman et al. (2019), p. 3.

which are only applicable when the allegedly unfair term is about "*access to and use of data or the liability and remedies for the breach or the termination of data related obligations."*[142] Other contractual dependencies are outside the scope. Article 13(7) clearly declares that terms on the main subject matter of the contract and price are outside the scope of these unfair terms provisions. This brings another layer of ambiguity: which clauses are the main subject matter and are outside of the scope of these provisions. Also, one can wonder what happens when the subject matter of the contract is processing raw farm data to generate agronomic prescriptions for farmers. Although one can argue that the provisions apply with a teleological interpretation, clarification of statements before the Regulation enters into force would be preferable.

3.4.4 Other provisions

Article 13(6) states that *"[w]here the unfair contractual term is severable from the remaining terms of the contract, those remaining terms shall remain binding."* Article 13(8) concludes the chapter by rightfully preventing contractual parties from excluding the application of this article, derogating from it, or varying its effects.[143]

3.5 Chapter V - Making Data Available to Public Sector Bodies and Union Institutions, Agencies or Bodies based on Exceptional Need[144]

Article 14 imposes an obligation to data holders to share data with the public sector when there is an exceptional need to use that data. Only SMEs benefit from an exemption to

[142] See also Recital 53: *"Furthermore, the rules on unfair contractual terms should only apply to those elements of a contract that are related to making data available, that is contractual terms concerning the access to and use of data as well as liability or remedies for breach and termination of data related obligations. Other parts of the same contract, unrelated to making data available, should not be subject to the unfairness test laid down in this Regulation."*

[143] This is another example of fragmented attempts of protection of original allocation of obligations.

[144] The Chapter V is summarised in the Explanatory Memorandum, as follows: *"Chapter V creates a harmonised framework for the use by public sector bodies and Union institutions, agencies and bodies of data held by enterprises in situations where there is an exceptional need for the data requested. The framework is based on an obligation to make data available and would only apply in the case of public emergencies or in situations where public sector bodies have an exceptional need to use certain data, but such data cannot be obtained on the market, in a timely manner through enacting new legislation, or by means of existing reporting obligations. In case of an exceptional need to respond to public emergency, such as public health emergencies, or major natural or human-induced disasters, data would be made available for free. In other cases of exceptional need, including to prevent or assist the recovery from a public emergency, the data holder making the data available should be entitled to*

do so. Article 15 provides more details regarding the circumstances of 'exceptional need'. Article 15(a) emphasises 'public emergency', and Article 15(b) mentions the prevention of or recovery from 'public emergency'.

Article 15(c) has more relevance from the sectoral perspective as it states that public access to related data can be possible *"where the lack of available data prevents the public sector body or Union institution, agency or body from fulfilling a specific task in the public interest that has been explicitly provided by law"* This can be interpreted broadly to cover the possibility of data access for the purposes of the policies that are related to agriculture.[145]

Public access under Article 15(c) is dependent on further conditions. Public bodies' access to data is only possible when alternative data collection is not possible for them and when developing particular legislation for public access prevents timely availability of data[146] or when obtaining data *"substantively reduce the administrative burden for data holders or other enterprises."*[147] These criteria entail that this provision is not for regular data access or continuous surveillance by public bodies. This may only be used for highly exceptional situations and for one-off data access. Continuously accessing relevant ag-data would not be possible for public bodies unless it is specifically regulated for particular purposes.

The remaining Articles of Chapter V are about the relationship with other regulations for the public sector data access (Article 16), details of the public sector data request (Article 17), procedures about how the data holder would respond to these requests (18), purpose limitations and other obligations of the public bodies (Article 19), compensation amounts to be paid by public sector bodies for the data access (Article 20), possibilities to share the accessed data with research organisations or statistical bodies within the purpose of the public access (Article 21), and mutual assistance and cross-border cooperation of the public sector bodies within the purpose this data access (Article 22).

---

compensation that include costs related to making the relevant data available plus a reasonable margin. To ensure that the right to request data is not abused and that the public sector remains accountable for its use, the requests for data would need to be proportionate, clearly indicate the purpose to be achieved, and respect the interests of the enterprise making the data available. Competent authorities would ensure the transparency and public availability of all requests. They would also handle any resulting complaints." p. 15.

[145] It seems the Article was drawn by considering the European Green Deal. See Explanatory Memorandum, p. 6.

[146] Article 15(c)(1).

[147] Article 15(c)(2).

In general, this chapter regulates the really exceptional and urgent data access needs of public bodies. In normal conditions, public access to data is subject to the relevant specific regulations to do so. Therefore, this chapter is unlikely to affect the sector significantly.

3.6 Chapter VI - Switching between Data Processing Services[148]

Chapter VI imposes specific obligations on providers of 'data processing services'[149] to take all necessary measures to let customers easily switch to another 'data processing service' by removing commercial, technical, contractual and organisational obstacles. However, the notion of 'data processing services' refers to *"cloud and edge services"*,[150] and therefore, the provisions in Chapter VI do not apply to the direct relationships between farmers and technology providers or machine producers. In other words, these provisions are not helpful for farmers' lock-in problems with technology providers, machines, or even data cooperatives. Still, imposing further obligations on cloud service providers for smooth switching may be valuable for the agricultural data cooperatives or data intermediaries in the sector if they work with *"cloud and edge services"* to store data. Data cooperatives or data intermediaries may benefit from these provisions when changing the cloud service providers. Although this is a very exceptional situation considering the wide sectoral practices, the

[148] Chapter VI is summarised in the Explanatory Memorandum as follows: *"Chapter IV addresses unfairness of contractual terms in data sharing contracts between businesses, in situations where a contractual term is unilaterally imposed by one party on a micro, small or medium-sized enterprise. This Chapter guarantees that contractual agreements on data access and use do not take advantage of imbalances in negotiating power between the contractual parties. The instrument of an unfairness test includes a general provision defining unfairness of a data sharing-related contractual term complemented by a list of clauses that are either always unfair or presumed to be unfair. In situations of unequal bargaining power, that test protects the weaker contractual party in order to avoid unfair contracts. Such unfairness impedes the use of data by both contractual parties. With that, the provisions ensure a fairer allocation of value in the data economy. Model contractual terms recommended by the Commission may assist commercial parties in concluding contracts based on fair terms."* p. 16 For model contractual terms, see Article 34 below.

[149] Article 2(12) defines it as *"a digital service other than an online content service as defined in Article 2(5) of Regulation (EU) 2017/1128, provided to a customer, which enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources of a centralised, distributed or highly distributed nature."*

[150] Article 2(12); Recitals 69-86; Article 26(1) also lists some examples including servers, networks and virtual resources; In the Explanatory Memorandum, it is explicitly stated that these provisions are designed to address lock-in problems "*in the cloud and edge market."* See Explanatory Memorandum, pp. 2, 7 and 14.

following part will further evaluate the provisions in Chapter VI for any players in the sector, which may directly work with *"cloud and edge services"*.

3.6.1 Removing obstacles to effective switching between data processing services

The Chapter starts with Article 23 which obliges 'data processing services' to take the necessary measures "*to ensure that customers of their service can switch to another data processing service, covering the same service type, which is provided by a different service provider."* It is critical here that the scope is limited with horizontal portability in the same particular market. This cannot even be applied to another service in the broader cloud industry due to the "*covering the same service type"* emphasis. Obviously, the rule-makers preferred to be restricted as much as possible in this regard.

The Article continuous as follow;

> *"In particular, providers of data processing service shall remove commercial, technical, contractual and organisational obstacles, which inhibit customers from:*
>
> > *(a) terminating, after a maximum notice period of 30 calendar days, the contractual agreement of the service;*
> >
> > *(b) concluding new contractual agreements with a different provider of data processing services covering the same service type;*
> >
> > *(c) porting its data, applications and other digital assets to another provider of data processing services;*
> >
> > *(d) maintaining functional equivalence of the service in the IT-environment of the different provider or providers of data processing services covering the same service type, in accordance with Article 26."*

These providers are really helpful for smooth switching to a rival service. However, limiting the scope of these provisions only to the cloud and edge services and to the same type of service switching is a missed opportunity from the sectoral perspective.

3.6.2 Contractual terms concerning switching between data processing services

Article 24 provides that the contracts shall include clauses regarding the details of switching conditions such as data sets, applications and all other digital assets generated by customers. The transition period can be a maximum of 30 days and during this time data processing services shall ensure the full continuity of functions and services. The contracts shall also include details regarding configuration parameters, security settings, access rights and access logs to the service.

3.6.3 Switching charges

Article 25 regulates switching charges. The Data Act has a different design here. Till 3 years after the Data Act's entry into force, the charges shall not exceed the costs of the switching process. 3 years after the Data Act's entry into force, there will be no charge. The Commission may adopt delegated acts to introduce a monitoring system for the charges.

3.6.4 General Evaluations

As explained in section 3.2 above, data rights have some limitations from the sectoral perspective. These extra rules for switching could have played a complementary role to fill the gaps if they had been designed broadly. Nonetheless, some players (such as data cooperatives or data intermediaries), which use cloud and edge services to store data sets can benefit from these additional rules when switching to a rival cloud service.

3.7 Chapter VII - International Contexts Non-Personal Data Safeguards[151]

Chapter VII starts with Article 27, which imposes obligations to providers of 'data processing services' to *"take all the reasonable technical, legal and organisational measures … to prevent international transfer or governmental access to non-personal data"*[152] There are still possibilities for international access under certain conditions though. For instance, if there is a foreign judgement or decision by a competent court or tribunal in a third country, access may still be granted.[153] The providers of the data processing services shall inform the data holder in case of a data access request in this regard.[154] As these are not directly related to the scope of this report, further details are not provided or discussed here. However, it has to be

[151] Chapter VII is summarised in the Explanatory Memorandum as follows: *"Chapter VII addresses unlawful third party access to non-personal data held in the Union by data processing services offered on the Union market. The proposal does not affect the legal basis of data access requests made to data held by EU citizens or businesses and is without prejudice to the Union's data protection and privacy framework. It offers specific safeguards, by way of providers having to take all reasonable technical, legal and organisational measures to prevent such access that conflicts with competing obligations to protect such data under Union law, unless strict conditions are met. The Regulation complies with the Union's international commitments in the WTO and in bilateral trade agreements."*, p. 16.

[152] Article 27(1).

[153] Article 27(1) to (4).

[154] Article 27(5).

noted that this obligation is only imposed on the data processing services that refer to the cloud and edge services.

3.8 Chapter VIII - Interoperability[155]

The Chapter imposes specific interoperability requirements for operators of common European data spaces (Article 28), data processing services (Article 29), and smart contracts[156] for data sharing (Article 30).

3.8.1 Provisions for the operators of Data Spaces

Article 28 regulates the "*[e]ssential requirements regarding interoperability*" to facilitate interoperability of data, data sharing mechanisms and services. It obliges the operators of data spaces to describe "*the dataset content, use restrictions, licences, data collection methodology, data quality and uncertainty",*[157] "*the data structures, data formats, vocabularies, classification schemes, taxonomies and code lists"*[158] or *"application programming interfaces, and their terms of use and quality of service"*[159] These obligations are the basic requirements for the operators of data spaces. The details seem to be left to future regulatory interventions for (sectoral) data spaces.[160] The Commission can adopt delegated acts to further specify these essential requirements and harmonised standards.[161] The Commission is also empowered to provide guidelines regarding the functioning of common European data

[155] Chapter VIII is summarised in the Explanatory Memorandum as follows: "*Chapter VIII provides for essential requirements to be complied with regarding interoperability for operators of data spaces and data processing service providers as well as for essential requirements for smart contracts. The Chapter also enables open interoperability specifications and European standards for the interoperability of data processing services to promote a seamless multi-vendor cloud environment.",* p. 16.

[156] *"means a computer program stored in an electronic ledger system wherein the outcome of the execution of the program is recorded on the electronic ledger"* See Article 2(16).

[157] Article 28(1)(a).

[158] Article 28(1)(b).

[159] Article 28(1)(c).

[160] See the last sentence of Article 28(1) and Recital 79.

[160] Article 28(6).

[161] Article 28(5).

spaces.[162] These are all important steps towards an interoperable Common European Agricultural Data Space (CEADS).[163]

However, the obligations are imposed on operators of data spaces. This means there is no change for the sectoral players such as technology providers, ag-machine producers or data cooperatives. Therefore, this does not help sectoral problems deriving from lack of interoperability and data standards. Multiple brands of machines and different services within the single farm operation according to their needs would not be affected and the technical side of the farm data lock-in problem is likely to stay unsolved. Still, interoperability obligations for operators of CEADS may indirectly affect the sectoral players if CEADS becomes the central data access hub in the sector, but it would be a better situation if a possible future sectoral regulatory intervention will provide detailed solutions for the sector to ensure interoperability of different brands of machines and services at the same time smoothly.[164]

3.8.2 Interoperability for data processing services

Article 29(1) regulates the open interoperability specifications and European standards for the data processing services by stating that they (a) shall be performance oriented to ensure interoperability between data processing services that cover the same service type, (b) shall ensure the portability of all digital assets between different processing services that cover the same service type, (c) shall guarantee 'functional equivalence' between different processing services that cover the same service type – where technically feasible.

Article 29(2) states that open interoperability and European standards shall address;

> *"(a) the cloud interoperability aspects of transport interoperability, syntactic interoperability, semantic data interoperability, behavioural interoperability and policy interoperability;*
>
> *(b) the cloud data portability aspects of data syntactic portability, data semantic portability and data policy portability;*
>
> *(c) the cloud application aspects of application syntactic portability, application instruction portability, application metadata portability, application behaviour portability and application policy portability."*

The Commission is empowered to request from the European standardisation organisations to draft standards for the specific service types of data processing services[165] and

[162] Article 28(6).

[163] See more about the Commission's plans for CEADS in SWD(2022) 45 final.

[164] This can only be done effectively if the ag-data rights intervention is designed together with the creation of CEADS. See more detailed discussion on the matter in Atik (2022a).

[165] Article 29(4).

to adopt delegated acts to publish the reference of open interoperability specifications and European standards in this regard.[166] In this regard, these provisions are the general framework for detailed specifications to build interoperability among the cloud and edge services.

Developing standards and interoperability specifications are not only essential for cloud and edge services but also the digital agricultural services and devices. However, the legislator did not prefer to provide a general horizontal obligation for all sectors here. Contrarily, it even restricted its scope to the 'same service type' in the broader cloud sector. This may be related to the rationale that follow-up sectoral regulations can be better tailored to the needs of each specific sector or even sub-segments of these sectors.

3.8.3 Requirements for Smart Contracts

According to Article 30(1), the vendor of an application using smart contracts or the person whose trade, business or profession involves the deployment of smart contracts regarding data availability shall ensure (a) robustness to avoid functional errors and to withstand manipulation of third parties, (b) safe termination and interruption referring to have internal functions to stop or interrupt the operation to avoid future (accidental) executions, (c) data archiving and continuity referring to keep the record of the operations performed on the data in the past (auditability), and d) access control referring the protection through rigorous access control mechanisms at the governance and smart contract layers.

The vendor of an application using smart contracts or the person who deploys smart contracts shall perform a 'conformity assessment' to ensure that it fulfils all the essential requirements listed above.[167] They draw up 'the EU declaration of conformity' and they will be responsible for the compliance of the listed requirements above.[168] The Commission is also empowered to request to develop standards for Smart Contracts and it can implement acts to adopt common specifications in this regard.[169]

In the scope of this particular research, the application of smart contracts is not mentioned among the common practices between farmers and companies with regard to data collection, access or sharing in arable farming. However, blockchain technology and smart

[166] Article 29(5).

[167] Article 30(2).

[168] Article 30(3).

[169] Articles 30(4) - 30(6).

contracts are used in aftermarkets such as digital marketplaces for trading agricultural goods.[170] In this regard, the abovementioned horizontal standards regarding the basic specifications of the smart contracts could be useful, at least, for this segment of the farm-to-fork chain at this stage.

3.8.4 General Evaluations

Although it is valuable to provide certain provisions to ensure interoperability, it is also a missed opportunity for smart farming, which already suffers a lot from lack of data standards and interoperability of IoT devices in the fields. The most relevant provision in this chapter is Article 28 which imposes certain requirements for the operators of the European data spaces. Although this is only for the interoperability within the data spaces, one can optimistically expect that having certain standards and principles may affect the sectoral practice in time. Especially if the CEADS becomes a central data access hub in the sector, this would force the sectoral players to comply with the developed standards to smoothly operate through the CEADS. However, even if this optimistic approach can become reality, this takes several years. Therefore, focussing more on the possible follow-up sectoral regulations to provide some provisions to motivate and even obligate the sectoral players to develop data standards and technical specifications for the smooth interoperability of farm machinery and other IoT devices would be more functional and realistic.

3.9 Chapter IX - Implementation and Enforcement[171]

3.9.1 Competent Authorities and Penalties

The Chapter starts with Article 31 on competent authorities by stating that *"Each Member State shall designate one or more competent authorities as responsible for the application and enforcement of this Regulation..."*[172] It is specifically declared that *"for specific sectoral data exchange issues related to the implementation of this Regulation, the*

[170] See, for instance, Leduc, Kubler and Georges (2021).

[171] Chapter IX is summarised in the Explanatory Memorandum as follows: "*Chapter IX lays down the implementation and enforcement framework with competent authorities in each Member State, including a complaints mechanism. The Commission shall recommend voluntary model contractual terms on access to and use of data. Penalties shall apply for infringements of this Regulation."* p. 16.

[172] Article 31(1).

competence of sectoral authorities shall be respected"[173] This is a signal for future sectoral authorities. This is in line with the previous signals for follow-up sectoral regulations (possibly an ag-data regulation as well) in future.[174]

Among other matters, Article 31(3) provides some details regarding the tasks and powers of competent authorities including *"handling complaints arising from alleged violations…"* or *"imposing, through administrative procedures, dissuasive financial penalties."* Imposing financial penalties is, of course, one of the important tools to ensure wide compliance with the proposed rules and obligations.

Article 31(4) states that in case of multiple authorities are designated by the Member States, they shall coordinate their activities to ensure the consistent application of the Data Act by creating a coordinating competent authority. Member States will inform the Commission regarding the names and tasks and powers of their competent authorities, and the Commission will publish the registration of these authorities.[175] These competent authorities should be designated to be independent in the sense that they shall be free from any external influence and they shall not take direct or indirect instructions from any party.[176]

These basic requirements are, of course, critical for the functional enforcement of the Data Act. However, inserting some additional statements in this article may be helpful. For instance, an EU-wide coordinator competent authority can also be created to ensure smooth enforcement of the Data Act across the Member States. Also, a branch of this authority should be responsible for EU-wide coordination of sectoral ag-data competent authorities and enforcement of future ag-data rules.

3.9.2 Right to lodge a complaint with a competent authority

Article 32 states that;

> *"Without prejudice to any other administrative or judicial remedy, natural and legal persons shall have the right to lodge a complaint, individually or, where relevant, collectively, with the relevant*

[173] Article 31(2)(b).

[174] Explanatory Memorandum, pp. 5, 15; Recitals 25, 79, 87; and more importantly Article 40(2); See, in particular, Recital 81: "…*competent authorities designated under sectoral legislation should have the responsibility for application of this Regulation in their areas of competence."*

[175] Article 31(5).

[176] Article 33(6).

competent authority in the Member State of their habitual residence, place of work or establishment if they consider that their rights under this Regulation have been infringed."[177]

This statement can be understood in different ways. The right holder can go for litigation directly without applying the competent authority, it can apply the competent authority while following the litigation process at the same time or the right holder can apply to courts after the decision of the competent authority. The latter might be considered the usual procedure after the decisions of public bodies, but the first interpretation may render the competent authorities' power over the players non-functional. In this regard, the formulation of the sentence might be reconsidered to remove this ambiguity.[178]

Article 32(2) obliges the competent authority to inform the complainant regarding progress and decision while Article 32(3) stresses the cooperation duties of competent authorities when resolving the complaints such as information exchange without delay. These are all necessary specifications for functional enforcement.

3.9.3 Penalties

According to Article 33, the Member States will determine the penalties. It also provides that *"[t]he penalties provided for shall be effective, proportionate and dissuasive"*[179] and *"Member States shall ... notify the Commission of those rules and measures ... without delay of any subsequent amendment affecting them."*[180] Whenever the privacy authorities are in charge of personal data-related infringements of Chapters II, III and V of this Regulation, they can impose fines up to the amount referred to in Article 83(5) of GDPR.[181] For infringement of Chapter V, the supervisory authority can impose fines up to the amount referred to in Article 66(3) of Regulation (EU) 2018/1725.[182]

Based on these provisions, it is certain that the Netherlands will have to assign, at least, one of the existing authorities like the Authority for Consumers and Markets (ACM) or to create, at least, one new authority for the compliance oversight of the Data Act and impose fines. Also, the Netherlands will have to regulate the penalties to impose the infringement of

[177] Article 32(1)

[178] See Atik (2022b)

[179] Article 33(1).

[180] Article 33(2).

[181] Article 33(3)

[182] Article 33(4)

the Data Act. However, maximum or minimum fines or calculation methods are not determined when the data is non-personal. They are all up to the Member States when regulating penalties at the national level. However, this may result in very different sanctions for the same action across Europe. Therefore, the Commission should provide some guidelines for the Member States to set a coherent framework of national regulations.

3.9.4 Model contractual terms

Article 34 provides that;

> *"The Commission shall develop and recommend non-binding model contractual terms on data access and use to assist parties in drafting and negotiating contracts with balanced contractual rights and obligations."*

The creation of sectoral model contracts by being aware of the most prominent practices in each sector (including smart farming) can be highly beneficial for farmers, who need to have a reference when evaluating alternative companies' terms and conditions. Indeed, Recital 83 states that *"the Commission should develop and recommend non-mandatory model contractual terms ... taking into account the conditions in specific sectors and the existing practices with voluntary data sharing mechanisms."*[183] Providing model contracts for the sector may result in a kind of competition amongst digital agriculture companies and machine manufacturers on better contractual terms. If they follow the model terms, they may both increase their compliance with the Data Act and increase their reputation in the eyes of farmers. However, before being too optimistic about the possible effects of the model terms, it has to be noted that data holders can only renounce their exclusive control of data sets and locked-in users when market conditions force them via a competition on better terms and conditions. There is no clear incentive for first-mover exclusive data controllers to change earlier contracts, but a trend to have better terms may be effective for the choice of new 'digital farms' and, therefore, the companies may prefer to update terms and conditions to gain new customers.[184] To help the farmers and also to contribute to the policymakers, BO Akkerbouw may consider providing some sectoral model contractual terms when it comes to data collection and use in arable farming.

[183]

[184] See more about the possible effects of smart contracts in Atik (2022b).

3.10 Chapter X - Sui Generis Right under Directive 1996/9/EC[185]

The Chapter only has Article 35, which states that the *sui generis* right for databases under Article 7 of the Directive 96/9/EC "*does not apply to databases containing data obtained from or generated by the use of a product or a related service"* to ensure a smooth exercise of the right to access (Article 4) and right to share (Article 5) under this Regulation.

This is a necessary clarification to eliminate any ambiguity because the Database Directive (Directive 96/9/EC) provides exclusive rights for the creators of databases that could have prevented the effective usage of data access and sharing rights provided by the Data Act.

3.11 Chapter XI – Final Provisions[186]

Chapter XI provides some concluding provisions such as amendment of certain regulations,[187] the exercise of delegation,[188] committee and procedure,[189] evaluation and review,[190] and entry into force and application.[191]

---

[185] Chapter X is summarised in the Explanatory Memorandum as follows: *"Chapter X contains a provision so that the sui generis right established in Directive 96/9/EC does not apply to databases containing data obtained from or generated by the use of a product or related service to hinder the effective exercise of the right of users to access and use data in accordance with Article 4 of this Regulation or of the right to share such data with third parties in accordance with Article 5 of this Regulation."*

[186] Chapter XI is summarised in the Explanatory Memorandum as follows: *"Chapter XI allows the Commission to adopt delegated acts to introduce a monitoring mechanism on switching charges imposed on providers of data processing services, to further specify the essential requirements regarding interoperability, and to publish the reference of open interoperability specifications and European standards for the interoperability of data processing services . It also provides for the committee procedure to adopt implementing acts to facilitate the adoption of common specifications for interoperability and smart contracts where harmonised standards do not exist or are insufficient to ensure the conformity with essential requirements. The proposal also clarifies the relation to other Union legal acts governing data sharing rights and obligations."*, p. 16.

[187] Articles 36 and 37.

[188] "*The power to adopt delegated acts is conferred on the Commission*." Article 38.

[189] Article 39(1): *"The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011."*

[190] Article 41: "*By [two years after the date of application of this Regulation], the Commission shall carry out an evaluation of this Regulation and submit a report on its main findings to the European Parliament and to the Council as well as to the European Economic and Social Committee.*"

[191] Article 42: *"This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union. It shall apply from [12 months after the date of entry into force of this Regulation]."*

The most important provision of this chapter from the perspective of this particular report is provided by Article 40(2);

> *"This Regulation is without prejudice to Union legislation specifying, in light of the needs of a sector, a common European data space, or an area of public interest, further requirements, in particular in relation to:*
> *(a) technical aspects of data access;*
> *(b) limits on the rights of data holders to access or use certain data provided by users;*
> *(c) aspects going beyond data access and use."*

In line with the previous signals within the Regulation, this explicitly states the possibility of follow-up interventions with sectoral rules and/or the creation of data spaces. For instance, Recital 25 clearly states that *"[s]ectoral legislation may be brought forward to address sector-specific needs and objectives"* immediately after stating that *"[t]his Regulation should therefore build on recent developments in specific sectors, such as the Code of Conduct on agricultural data sharing by contractual agreement."* Also, Recital 87 states that;

> *"This Regulation should be without prejudice to rules addressing needs specific to individual sectors or areas of public interest. Such rules may include additional requirements on technical aspects of the data access, such as interfaces for data access, or how data access could be provided, for example directly from the product or via data intermediation services. Such rules may also include limits on the rights of data holders to access or use user data, or other aspects beyond data access and use, such as governance aspects. This Regulation also should be without prejudice to more specific rules in the context of the development of common European data spaces."*

The listed requirements are not exhaustive, and the sectoral intervention can theoretically be much broader in terms of regulating ag-data access and obligations as long as they do not contradict the horizontal framework provided by the Data Act.

Article 42 concludes by stating that the Regulation will apply 12 months later than its entry into force. This was stated in the recitals with the reasoning that market players need time to adapt their businesses to the proposed provisions in the Regulation.[192] By considering the time for review of this Regulation, stakeholders will have to wait a couple of years for a binding set of rules for non-personal data.

[192] Recital 89: *"In order to allow the economic actors to adapt to the new rules laid out in this Regulation, they should apply from a year after entry into force of the Regulation."*

4.0 Overall Evaluations by Answering Specific Questions

Beyond the detailed analysis of the provisions of the Data Act, it is also necessary to answer specific questions from the sectoral perspective to provide more targeted information for the sectoral stakeholders regarding the potential implications of this Regulation.

4.1 What will change when the new Data Act is implemented? How will consumers, producers, and intermediaries have to act differently, compared to the present situation?

Implications for Users (Farmers)

Data Act is a comprehensive regulation, which has several elements to address the problems in the digital age. However, the most prominent part of the regulation from the sectoral perspective is Chapter II regarding data access and control rights. Unlike the GPDR, these rights are granted to users regardless of whether they are natural or legal persons and the rights are applicable to any data sets generated by the use of a 'product' or 'related services' regardless of whether they are personal or not. So, this is a revolutionary improvement from the sectoral perspective considering the fact that it was a very controversial issue whether the right to data portability under the GDPR can be applied to agricultural data sets or whether ag-data sets can be classified as personal or not.[193]

However, as explained above, there are significant limitations in these rights in the ag-data setting due to the restrictive definitions of the core concepts.[194] Therefore, the data rights designed in Chapter II of the Data Act[195] are barely applicable to relationships between farmers and agricultural machine manufacturers if farmers own, lease or rent the machines from the manufacturers. Still, this is a remarkable improvement for the sector compared to the unregulated environment, especially when considering the importance of agricultural machinery in arable farming. After the Data Act, farmers can undisputedly access the data sets collected through their use of agricultural machinery and they can transfer these data sets to third parties if these data sets are stored/controlled by the device manufacturers. However, it is

[193] More importantly the only beneficiaries of the GDPR rights are real persons while most of the farms (even family farms) are run by legal entities (companies). See more discussion on the matter in Atik (2021) and Atik and Martens (2021).

[194] See the substantial discussion in section 3.2 above.

[195] The right to data access (Art. 4) and the right to share data with third parties (Art. 5).

important to recall that only raw farm data sets are under the scope and derived or inferred information such as data-driven agricultural solutions, suggestions or prescriptions provided by technology providers are outside the scope of the Regulation.[196]

Implications for Data Holders (IoT Device Manufacturers)

Data holders are obliged to be fair, reasonable and non-discriminatory as well as transparent when making data available to data recipients under the users' right to data sharing. Data holders and data recipients require to enter into an agreement regarding data access. The clauses of these agreements will not be binding if they restrict the users' rights over data. The Data Act also forbids data holders' discriminatory actions between their own enterprises and other data recipients when making data available. So, data holders are basically responsible to comply with the rules in the Data Act.[197]

Implications for Third-Party Data Recipients (including Data Intermediaries)

There are specific obligations over third parties. Article 6 clearly restricts the data usage for third parties, who access data upon users' request from the data holders (IoT device manufacturers), with the specific purpose of data access that is determined together with the user. When the access purpose disappears, then the third party is obliged to delete the data sets. Also, third parties shall not i) coerce, deceive or manipulate the user, ii) share data with other parties, iii) use the data to develop a rival product to the data holder (IoT device manufacturer), and prevent users to share data with other third parties. These obligations are only valid for third parties that are bigger than SMEs.[198]

Data recipients will have to pay compensation to data holders when accessing data under the right to data access. Users (farmers) can benefit from the right to share data with third parties (Article 5) for free, but the new company, which will access the data, will have to pay compensation to the data holder. However, the access costs would probably be transferred to users (farmers) in the end with higher prices of services or machines. The compensation amount is not determined in the Data Act. It only states that the compensation shall be 'reasonable'. If the data recipient is an SME, then the amount will be below "the costs directly related to making

[196] See more information about the scope of these rights in section 3.2.3 above.

[197] See more detailed evaluation and some limitations in these obligations in section 3.3.1 above.

[198] See more in 3.2.4 above.

the data available". Determining what 'reasonable' is would be the main challenge in practice unless the Commission releases some guidelines to determine this.

The Member States will assign dispute settlement bodies to solve the disputes regarding the compensation to be paid. The decisions of these bodies shall only be binding if this is agreed on by the parties before the dispute settlement. The dispute settlement bodies will decide within 90 days. Although 90 days appears acceptable, this time may sometimes jeopardise the users' smooth switching to another company.[199]

The data holders are also responsible for technical protection measures to prevent unauthorised data access and compliance with the users' data rights. In case of unauthorised data access, the data recipient is obliged to destroy the data sets and stop all related business activities developed based on this unauthorised access unless such access did not cause significant harm to the data holder or unless this will be a disproportionate sanction compared to the data holder's interests.[200]

Overall, the data recipients in the sector will have to comply with the particular rules and specific obligations provided by the Data Act after it enters into force and applies.

4.2 To what extent does the Data Act bring solutions to the ambiguities about data ownership, and what are the remaining issues? What duties and rights are sharpened with the new Data Act, which will influence the data position of the arable farmer?

The Data Act links the data rights (access and transfer) to the 'users' referring to the ones who own, rent or lease the IoT device. In this regard, legal control of the device is extended to the data control rights. Although farmers can be qualified as users when they own, rent or lease the IoT device, there are also distinct situations.

Other farm data collection methods and locked-in farm data sets in the hands of other players seem outside the scope of these rights. For instance, data collection via stable/sole sensors, camera recordings and images, and manual observations that are digitalised later on are unlikely accessed or shared depending on these rights. Also, farm data sets stored and processed by technology providers, data intermediaries or data cooperatives do not fall under these very restrictive definitions.

[199] See more details regarding the dispute settlement system in the Data Act and some suggestions to revise them in section 3.3.3 above.

[200] See more in section 3.3.4 above.

There may also be problems regarding machinery ownership. Farmers may have dependencies to access the data when the machinery is owned, rented or leased by another player than the farmer such as a company, which provides harvesting services, or a cooperative, which buys the machinery for common usage.[201] In these kinds of situations, the data will be accessible by the legal owners, renters or leasers of the machines and, thus, farmers would have to negotiate with them to indirectly access their farm data.

Also, when the machinery is owned, rented or leased by more than one user (farmer), the application of the data access rights may generate uncertainties. Although there is no clarity in the wording of Articles 4 and 5 on this matter, Recital 20 states that *"[i]n case several persons or entities own a product or are party to a lease or rent agreement and benefit from access to a related service, reasonable efforts should be made in the design of the product or related service or the relevant interface so that all persons can have access to data they generate."* This may cause some problems when multiple farms commonly buy a machinery because some farms may expect confidentiality of their data sets while the others can theoretically and legally access the data sets as long as they prove that they are one of the owners (or renter or leasers) of the machines because the Regulation itself repeats the statement that *"[t]he user or third party shall not be required to provide any information beyond what is necessary to verify the quality as user or as third party pursuant to paragraph 1"* in Articles 4 and 5.[202]

In this regard, the recent Data Act improved the understanding of who has which rights over which data compared to the unregulated environment for non-personal data in Europe,[203] but it is difficult to say that it eradicated the 'data ownership' debate in the agriculture sector completely. The reason for that is that the Data Act did not take into account relevant social aspects of daily farmers' life and the organisation of their work within communities. It is a horizontal regulation that is designed for all sectors.

[201] See a detailed discussion on the limitations in section 3.2.3 above.

[202] See Article 4(4) and 5(3).

[203] It has to be noted that application of the GDPR is highly ambiguous in the ag-data setting and the free flow of non-personal data regulation, which was released in 2018, only promote sectoral code of conducts instead of providing binding rights unlike the Data Act. See section 2.2.1 above.

4.3 What are the similarities and differences between the Code of Conduct for Data Use for Arable Farming and the Data Act? What would be the recommendations on updating the code of conduct of the BO Akkerbouw based on the novelties in the Data Act?

BO Akkerbouw's code of conduct is based on the combined insights from the 'privacy and security principles for farm data (AgGateway - North America)', which was adopted on May 5, 2015 and the 'code of conduct for data sharing (AgroConnect)', which was adopted on October 22, 2014 established by a number of large Dutch arable cooperatives. BO Akkerbouw expects all companies, which do business with companies in arable farming in the field of precision agriculture and data, to comply with these principles. This is a set of voluntary principles (a kind of self-regulation or soft law). The voluntariness and 'soft' nature of these principles constitute an inherent limitation compared to the binding rules in the Data Act. Indeed, it is clearly stated in the BO Akkerbouw's code of conduct that a company has the option of choosing not to implement the relevant principles or to implement them in a different way. Such a dissenting company must, however, explain the reasons for this in writing and with reasons. Such a 'comply or explain' principle possibly aims to incentivise possibly diverse participants in the arable farming chains to join the code.[204]

The code is based on a number of basic principles, namely:

Control: The basic principle is that the data supplier has control over (rights to) the information that is generated from its own actions. It is the grower's responsibility to agree to data use and sharing by data buyers, data service providers or third parties.

Transparency and consistency: Regardless of whether a data service provider is engaged to the code, data buyers inform data suppliers about the purposes for which they collect and use data.

Database, access and control: Data, which is stored in a database of the data recipient, the data service provider or third parties, may only be used or accessible with the explicit consent of the data supplier (authorisation).

Disclaimer, use and sale of data: Third parties, data service providers or data buyers will not sell or publicly publish data that can be traced back to the data supplier. If this data concerns personal data, the legal regulations for the processing of personal data apply.

[204] BO Akkerbouw's code of conduct (2019), p. 1.

It has to be noted that the Data Act provides basic principles with a horizontal framework for all sectors. This means sectoral codes cannot contradict this framework, but they can provide progressive principles tailored to specific sectoral needs as long as they are compatible with the main provisions of the Data Act. The following evaluation will both consider how to update the BO Akkerbouw code in line with the Data Act principles and how to address the remaining issues after the Data Act with some tailored complementary principles for arable farming – where necessary.

4.3.1 Comparing the entitlement (data right) holders

In the BO Akkerbouw code of conduct, the entitlements (data rights) are clearly attached to the one (data supplier) whose actions generate the data. In the arable farming practice, this is likely to be the farmers. So, farmers can decide to share data with data buyers, service providers or third parties. Compared to the Data Act, where the entitlements (data rights) are linked to the device ownership, rent or lease, this design in the BO Akkerbouw code indeed, is more comprehensive to cover most of the smart farming practices in arable farming because data rights are linked with the data suppliers' (farmers) own actions. Therefore, it may be better to keep the entitlement design as is instead of copying the Data Act entitlement model. However, farming operations are beyond individual farmers' presence as individuals may disconnect from the specific farming operation at some point, but historical data sets of the fields may be necessary for the new operators. In this regard, inalienable data rights can be linked with 'farm units' that may be defined and registered based on geographical location. An active operator of the farm, thus, can always access and share the data sets collected from this particular farm unit.[205]

Beyond the entitlement design, it would be necessary to reconsider the aforementioned 'comply or explain' mechanism in the BO Akkerbouw code.[206] The code is already voluntary for participation. If a party decides to be a part of these already very basic principles, it may be more functional to expect them to comply. This could mitigate the inherent limitations of the voluntary soft laws, the BO Akkerbouw code, in this particular case. This can also help the participants to update their terms and conditions during the upcoming period till Data Act apply

[205] See more detail regarding this data entitlement design suggestion in Atik (2022a).

[206] It has to be noted that it is not clearly explained who would then evaluate the argumentation/reason for not complying. One can assume that BO Akkerbouw plays a role for this. If there is no mechanism for controlling compliance, then it does not make sense to allow providing reasons for non-compliance.

- as an opportunity for them to a smooth transition. Thus, they may be more prepared for Data Act compliance in future.

It is important to note here that data rights in Chapter 2 of the Data Act only cover some of the ag-data collection and storage methods in the arable farming practice.[207] Also, locked-in data sets under the control of SMEs are exempted from the provisions in Chapter 2 of the Data Act. It means farmers cannot use their already restricted data access and sharing rights vis-à-vis SME data holders. Therefore, BO Akkerbouw may prefer a progressive position to update their code in such a way that any data holder – regardless of whether they are SMEs or not – shall abide by the data access and sharing rights of the farmers.

4.3.2 Comparing the data re-use conditions

With regards to the data re-use conditions, BO Akkerbouw code provides that re-use is only possible with the explicit consent of the data supplier (farmer), who should be informed about the purpose of the re-use. Also, companies, which hold the data, are responsible for not selling or disclosing the data to the public if the supplier (farmer) can be identifiable with data access. This is not completely different from the mechanism that the Data Act brings. The user-centric approach in the Data Act is emphasised several times in the discussion above.

However, the conditions for the re-use of data are not entirely clear in the Data Act. It is certain that data re-use (transfer) is possible upon users' requests (Article 5), but there is an ambiguity about whether the data holder companies can share data with third parties without the users' requests. There are contradicting statements in the Recitals. Recital 31 states that "*[d]ata generated by the use of a product or related service should only be made available to a third party at the request of the user."*[208] However, Recital 38 seems to deny this: *"[v]oluntary data sharing remains unaffected by these rules."* Article 4(6) states that *"The data holder shall only use any non-personal data generated by the use of a product or related service on the basis of a contractual agreement with the user."* One can interpret that this also covers data sharing with third parties, but when evaluating the entire Regulation, data sharing without users' individual requests can be possible with a nuance: if this is stated in the contracts

[207] See more on section 3.2.3 above.

[208] This is in line with the restrictive first sentence of Article 4(6). See a detailed discussion regarding this provision in section 3.3 below in the context of farmers' trust.

with users, and if this sharing would not be detrimental for the commercial position of users.[209] However, it is not clear whether data-reuse conditions need to be defined in detail or whether a general term to let data holders share data with third parties can be considered valid. This is a confusing design and highly restrictive in terms of third-party access possibilities.

In this regard, ***the BO Akkerbouw may need to update its code regarding data re-use in line with Article 4(6) which mandates contractual clauses to do so. It may also specify the requirements of the contractual clause for data sharing to be more clear than the Data Act in this regard.***

Preventing 'gatekeepers' to benefit from the right to data sharing (Article 5)

Another difference that the Data Act brings for data sharing is Article 5(2) which excludes 'gatekeepers' defined in the Digital Markets Act[210] (DMA) from eligible third parties, who can access data under the right to share the data with third parties (Article 5(1)). It also prohibits 'gatekeepers' from incentivising users in order to accumulate data. The aim is to prevent powerful players from hoovering up all the data. The same concern is valid for agricultural data as vertically integrated agricultural giants have more incentives and abilities to accumulate data.[211] However, the notion of 'gatekeepers' refers to core platform services listed in Article 2.2 of the DMA, and technology providers or machine producers in arable farming seem not to fall under any of these definitions.[212]

In particular, ***BO Akkerbouw may update its code in line with the legislators' aim to prevent data accumulation in the hands of a few giants by, for instance, inserting some provisions to prevent vertically integrated giants from hoovering up all the ag-data sets in the sector.***

[209] See the second sentence of Article 4(6): *"…The data holder shall not use such data generated by the use of the product or related service to derive insights about the economic situation, assets and production methods of or the use by the user that could undermine the commercial position of the user in the markets in which the user is active."*

[210] COM(2020) 842 final.

[211] See a detailed discussion on the matter in the context of possible implications of ownership right design in the sector in Atik and Martens (2021), pp. 382-384.

[212] See similar considerations in this regard in Atik and Martens (2021), p. 394 and Atik (2022b). See also section 3.2.2 above.

Purpose limitation and data deletion

Article 6 of the Data Act regulates that third parties, which access data as a result of the users' right to transfer (Article 5), can only use the data with the specific purpose of access and they are responsible to delete the data when the purpose disappears. This is a clear purpose limitation obligation for third parties. The purpose limitation focus is similar to the BO Akkerbouw code, but the main difference here is the data deletion obligation for third parties as a further restriction for data re-use. ***The BO Akkerbouw may consider updating its code in this regard.*** However, it is advisable that the third party should always take clear confirmation from the 'user' (farmer) before deleting the data sets so as to prevent data loss situations that may harm users.[213]

Also, Article 11(2) provides that in case of unauthorised data access, the data recipient shall destroy the data sets and stop all related business activities developed based on this unauthorised access. The latter shall not apply if such data use did not generate significant harm to the data holder or if such a strict imposition on data recipients would be disproportionate compared to the data holder's interests.[214] ***The BO Akkerbouw may consider updating its code to insert similar obligations in case of unauthorised data access*** although it is not crystal clear what the unauthorised data access really is, how to determine whether such unauthorised access caused 'significant harm' to data holders, or whether the destruction of business built on the unauthorised access is 'proportionate' or not in the Data Act.[215]

Non-competing obligations

Article 4(4) (that prevents users from developing a competitive product by using the accessed data) and Article 6(2)(e) (that prevents third parties from using the *data to develop a product that competes with the product from which the accessed data originate or share the data with another third party for that purpose*") are another important development with the Data Act.[216] ***The BO Akkerbouw may consider updating its code to cover these non-compete clauses for the ones who access data from data holders (IoT device manufacturers).***

[213] See more discussion about this suggestion in section 3.2.4 above.

[214] Article 11(3).

[215] See section 3.3.4 above for more detail.

[216] It is noteworthy to mention the wording of these clauses. The forbidden action is developing a competing 'product'. This may entail that developing 'related service' is out of the scope of these restrictions. See also Recital

Data sharing under FRAND terms

Another novelty in the Data Act that the BO Akkerbouw may take into consideration is Article 8 on *"[c]onditions under which data holders make data available to data recipients".* Article 8(1) mainly obliges data holders[217] to be fair, reasonable and non-discriminatory as well as transparent when making data available to data recipients[218] under the right to data sharing (Article 5). Article 8(3) forbids data holders discriminatory actions between their own enterprises[219] and other data recipients when making data available: *"…it shall be for the data holder to demonstrate that there has been no discrimination."*[220] Article 8(4) states that *"[a] data holder shall not make data available to a data recipient on an exclusive basis unless requested by the user under Chapter II."* ***These provisions could be used as a reference point to insert fair data access conditions tailored to the sectoral needs in the BO Akkerbouw code***.

Compensation to be paid by the data recipient to the data holder

Article 9 states that data recipients shall pay a 'reasonable' compensation to data holders for reaching data under Article 5. It is unclear what the 'reasonable' really is. If the data recipient is an SME, then the compensation shall not exceed the cost of data sharing. ***BO Akkerbouw may update the code with an appropriate rule for the sector in this regard.***

35. It is not clear whether this is only an omission or an intentional choice. If the latter is the case, there is no hint regarding the reason behind this distinction.

[217] defined as *"legal or natural person who has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation implementing Union law, or in the case of non-personal data and through control of the technical design of the product and related services, the ability, to make available certain data"* See Article 2(6).

[218] defined as "*a legal or natural person, acting for purposes which are related to that person's trade, business, craft or profession, other than the user of a product or related service, to whom the data holder makes data available, including a third party following a request by the user to the data holder or in accordance with a legal obligation under Union law or national legislation implementing Union law"* See Article 2(7).

[219] *"'enterprise' means a natural or legal person which in relation to contracts and practices covered by this Regulation is acting for purposes which are related to that person's trade, business, craft or profession"* See Article 2(8)

[220] Recital 41 states that *"[i]t is not unlawful discrimination, where a data holder uses different contractual terms for making data available or different compensation, if those differences are justified by objective reasons."* This is very close to the abuse of dominance defence model. It seems that the data holders are considered a dominant player in terms of exclusively controlling the necessary data sets.

Also, in case of a dispute between the data holder and data recipient on the compensation amount, Member States shall create a dispute settlement body that will deal with these disputes within 90 days.[221] This may prevent smooth data flows as waiting 90 days may ruin the data operation of users (farmers). Therefore, ***a complementary obligation can be inserted in the BO Akkerbouw code to ensure that data access will always be granted immediately upon users' request*** to prevent delays and any connected harms to users, and compensation can be paid retrospectively after dispute settlement ends.[222] This may remove the mentioned risks to the benefit of farmers.

4.3.3 Other provisions

Unfair Contractual Terms

Chapter IV of the Data Act provides rules for the invalidity of unfair terms in the contracts if they are imposed on SMEs.[223] However, there is an unclarity in the relevant provisions regarding whether they are applicable to any data or 'data generated by the use of a product or related service' as in the previous chapters.[224]. ***BO Akkerbouw may consider updating its code by inserting similar rules in its code after the Data Act. It is particularly suggested that the scope can be determined broader when doing so: the rules can be valid for all 'unfair terms' imposed on farms regardless of whether they are SMEs or not.*** When updating the code, the broader interpretation can be preferred to apply the unfair terms provisions i) to any farm data sets regardless of whether they are produced by the use of a product or not, ii) to any unfair terms regardless of whether they are unilaterally imposed on farmers and iii) to any contractual clause regardless of they are related to data and subject matter of the contract or not. Also, clarification of, at least, the most prominent unfair terms in the arable farming setting can be a prerequisite to updating the code. Thus, farmers can be protected from any contractual obligations that are 'unfair'.

[221] See section 3.3.3 above.

[222] See original suggestion in Atik (2022b).

[223] See the details in section 3.4 above.

[224] Ibid.

Public sector access to data

Chapter V regulates the exceptional situations where public bodies can access to data such as a public emergency.[225] Although this is not likely to significantly affect the sectoral dynamics, ***BO Akkerbouw may consider updating its code by inserting some general obligations to share data with the public bodies to prevent or recover from emergencies and it may encourage its participants to share data to realise broader policy aims such as environment or public health.***

Interoperability obligations for operators of data spaces

Chapter VIII regulates interoperability obligations for operators of data spaces, but these obligations do not go beyond the description of the technical standards that will be used in the sectoral data spaces.[226] In other words, there is no any obligation for the sectoral players such as agricultural machine manufacturers, digital service providers or data intermediaries. However, ***BO Akkerbouw may also encourage the sectoral players to develop and stick to a common data standard and interoperability protocols.***

Model Contracts

Article 34 provides that the Commission will release sectoral model contracts that are compliant with the Data Act. In order to contribute to the Commission as a stakeholder in arable farming in the Netherlands, ***BO Akkerbouw may consider starting a project on developing sectoral model contractual terms when it comes to data collection and use in arable farming. For different arrangements (for instance, farmers' contracts with technology providers, machine manufacturers or data intermediaries), there may be some nuances to ensure fair and compliant terms.*** This would also be very helpful for farmers when they choose a company to work with. Also, this may nudge the companies to more quickly comply with the Data Act and the updated BO Akkerbouw code.

4.3.4 General Evaluations

It has to be noted first that BO Akkerbouw's code of conduct will not become superfluous once the Data Act has been implemented. BO Akkerbouw's code of conduct can

[225] See more in section 3.5 above.

[226] See Section 3.8 above.

stay on the website with its existing form. However, it is preferable to update the document in line with the horizontal framework provided by the recent Data Act. Also, it is advisable to be more proactive to provide supplementary provisions in the updated version of the code given that the new Data Act provide limited coverage for the ag-data access issues in the sector and relatively limited protection for farmers ex explained in detail above. Also, it is advisable that BO Akkerbouw may i) enlighten farmers about what is covered by the Data Act and what is not, ii) advise farmers to organise their data collection as much as covered by Articles 4 and 5 of the Data Act, for instance, by asking suppliers that rent out farm machinery to farmers about the way in which they handle the data they collect from the farms, and iii) warn the farmers about the risks such as in the case of common ownership of an IoT device, the data sets are accessible by all owners, renters or leasers.

4.4 How will the Data Act be implemented at a national level and what actions are needed from the Dutch government?

Chapter 3 of the Data Act obliges the Member States to create dispute settlement bodies and a mechanism regarding "*the determination of fair, reasonable and non-discriminatory terms for … making data available in accordance with Articles 8 and 9.*"[227] These dispute settlement bodies shall be impartial, they need to have the required expertise about FRAND terms, and they need to reach cost-efficient decisions.[228] In this regard, the first required action for the Netherlands with the Data Act will be the creation of a dispute settlement body to deal with issues regarding the compensations to be paid by the data recipients to data holders.[229] Also, as explained in section 3.9 about Chapter IX of the Data Act, the Member States including the Netherlands will also have to assign, at least, one competent authority to supervise compliance with the Data Act. These competent authorities can impose penalties in case of a breach. The details of the penalties will be determined by the Member States including the Netherlands.

[227] Article 10(1).

[228] See Article 10(2).

[229] See section 3.3.3 above.

4.5 How Data Act is related to the Commission's plans to create Common European Agricultural Data Space (CEADS) and how it may affect the existing initiatives of data infrastructures in arable farming?

On 23 February 2022, the Commission released the Data Act and Staff Working Document on (SWD(2022) 45 final) on Common European Data Spaces at the same time. Data Act and sectoral data spaces are highly related to each other. The former aims to provide the horizontal regulatory framework when it comes to data access and re-use and the latter is more about the technical design of data access hubs at the sectoral level. In both of the documents, there are signals towards the follow-up sectoral regulations including in agriculture.

Explanatory Memorandum of the Data Act states that *"[t]his proposal leaves room for vertical legislation to set more detailed rules for the achievement of sector-specific regulatory objectives."*[230] Thus, *"[t]he initiative leaves a significant amount of flexibility for application at sector-specific level."*[231] There is also a particular signal for a follow-up agricultural data regulation as Recital 25: *"[t]his Regulation should therefore build on recent developments in specific sectors, such as the Code of Conduct on agricultural data sharing by contractual agreement. Sectoral legislation may be brought forward to address sector-specific needs and objectives."* This follow-up sectoral regulation may provide specific ag-data access rights and obligations and it may also serve to regulate the Common Agricultural Data Space (CEADS).

By regulating the general obligations of the operators of data spaces in Chapter VIII in detail, the Data Act is an important starting point for the creation of sectoral European data spaces. The European Commission has had plans to create sectoral data spaces since 2018.[232] The European strategy for data (COM(2020) 66 final) was announced on 19 February 2020 to foster the European data economy by clearly declaring the aim of creating common European data spaces in strategic sectors including agriculture to eventually reach a European data space – a genuine single market for data.[233] The Staff Working Document (SWD(2022) 45 final) on Common European Data Spaces provides more details regarding this plan by mentioning the concept of common European data spaces (Section 2), data governance aspects and legislative measures (Section 3), data IT infrastructures, including EU support programmes for funding in

[230] Explanatory Memorandum of the Data Act, p. 5.

[231] Ibid., p. 8.

[232] COM(2020) 66 final, pp. 12-13 and 21-23, in general, and 31-32, in particular; See also earlier documents of COM(2018) 232 final and SWD(2018) 125 final.

[233] SWD(2022) 45 final.

this field (Section 4). Also, it expresses the recent developments in sectoral common European data spaces (Section 5).

SWD(2022) 45 final document states the Commission's vision for the agricultural data space. The aim is to create a trustworthy agricultural data pooling and sharing infrastructure for private stakeholders (farmers, machinery companies, data service providers) and public authorities to serve to reach a competitive and sustainable sector in line with the Common Agricultural Policy and the Farm-to-Fork Strategy. It is planned to initiate a coordination and support action (CSA) in the third quarter of 2022 to contribute to developing a governance and business model for the agricultural data space.[234] Also, several Horizon Europe projects will help to generate relevant insights on economic aspects of ag-data, the potential of big data and data infrastructures to develop a business model for the agricultural data space. It is particularly expected that these projects will shed more light on privately and publicly held agricultural data, data interoperability issues, general design principles for data spaces or the potential of digital platforms to support digital innovation in agriculture.

For now, the Data Act does not provide any obligation for the existing data initiatives or data infrastructures in the sector as explained in section 3.8.1 above. However, it imposed certain obligations on the operators of the data spaces. So, it will be the main framework when designing the agricultural data space even though sectoral regulation(s) can provide further specifications within these boundaries. Although there is no declared official design for the agricultural data space, the preliminary idea is integrating the existing data infrastructures in the sector instead of creating a central data infrastructure from scratch that would require public-private cooperation.[235] In this regard, sectoral stakeholders (especially, existing data infrastructures in the sector) should actively contribute to the developments of the CEADS and connected regulatory design.

5.0 Conclusion

The Data Act proposal includes a number of different layers that tackle the issues with the data economy from different perspectives. From the standpoint of smart farming practices in arable farming, this is a step forward to have, at least, clear rights to access and share data despite the fact that the definitions of the fundamental concepts and the scope of the provisions exclude some important practices in the sector.

[234] See SWD(2022) 45 final, pp. 27-28.

[235] European Commission (2020), pp. 22-23.

Data access (Article 4) and data sharing (Article 5) rights are crucial for the farmers' data lock-in, but they are only applicable to *"data created by the use of a product or a connected service."* The implementation of these provisions in the ag-data access setting is severely constrained by the definitions of "user", "product" and "related service". Also, SME data holders are excluded from the provisions in Chapter II including rights under Articles 4 and 5.[236] This means locked-in farm data sets in the hands of small start-ups are outside the scope of these rights. More importantly, it is not clear whether these data rights are inalienable or un-waivable. Therefore, one should note that data rights may be accumulated in the hands of a few powerful giants.[237] This is particularly a concern for farm data control because vertically integrated agricultural companies have significant powers to dominate the markets for Smart Farming solutions.[238]

There are also other provisions that may affect the farmers' lock-in situations indirectly. For instance, Article 9 regulates compensation for making data available on 'reasonable' terms, which might not be easily identified in practice without a clear test,[239] and this may prevent smooth switching in some situations. Regarding the technical reasons for the farm data lock-ins, there are no direct provisions, but Chapter VIII obliges operators of (sectoral) data spaces to determine essential horizontal requirements for interoperability.[240] This will affect the Common European Agricultural Data Space, but interoperability problems amongst the services of technology providers and agricultural machines will not be affected. Another important development that may affect the lock-in problem in the sector is related to the provisions regarding the invalidity of unfair terms unilaterally imposed on SMEs. Small farms may benefit from this additional protection. However, it should not be overlooked that adoption rates of digital technologies are higher among bigger farms.[241] As soon as they exceed the turnover determined for SMEs definition,[242] they will not be able to benefit from these rules.

[236] Article 7(1)

[237] See similar concerns in the context of an ag-data ownership design, and suggestions for an alternative entitlement design for the DAS in Atik and Martens (2021), pp. 382-383 and Atik (2022a).

[238] See more in Atik (2021) and Atik and Martens (2021).

[239] If the data recipient is an SME, then the framing is relatively clearer: *"compensation shall not exceed the costs directly related to making the data available"* See Article 9(2).

[240] See Article 28.

[241] Shang et al. (2021), p. 12.

[242] as defined in Article 2 of the Annex to Recommendation 2003/361/EC: *"... (SMEs) is made up of enterprises which employ fewer than 250 persons and which have an annual turnover not exceeding EUR 50 million, and/or*

In addition to these specific limitations, it may not be easy to determine what 'unfair' is, and this may result in ambiguities in practice.[243]

In brief, the horizontal Data Act is an important development to mitigate the legal reasons for the farm data lock-in problem in the sector, but it is important to note that it may not be sufficient alone to eradicate this issue completely due to the explained limitations in the design of the rights and rules and the silence in the Regulation when it comes to data standards and interoperability obligations for the manufacturers of IoT devices.[244]

Before the Regulation enters into force, it may be possible to revise the relevant statements and definitions to ensure their wider applicability to the ag-data access problems if this would not have negative effects on other industries. However, it may not be realistic to anticipate a significant shift in the design of this horizontal intervention. Several statements in the Data Act signal that follow-up sector-specific regulations will complement the remaining issues in different sectors.[245] So, it may be more effective to provide insights for the policy makers, who will design the follow-up sectoral rules at this stage to ensure that the possible future ag-data regulation will be designed tailored to the sectoral needs.

To conclude, IoT implementations and smart farming practices in arable farming also be positively affected by the horizontal Data Act intervention. However, it is not able to remove all the sectoral problems alone. Especially, when considering the fact that the Data Act will apply 12 months later than its entry into force[246] and possible sectoral regulatory interventions will come much later on, first-movers powerful players in the sector may use this time to reinforce their positions with more aggressive actions by considering that some really strict rules are coming to regulate the market failures that they benefit from. To take action against this risk, a) updating the BO Akkerbouw's code of conduct in line with the prominent principles of the Data Act and having more proactive positioning to include provisions to address the remaining issues from the sectoral perspective, b) changing the 'comply or explain' principle with stricter obligations for the participants to the code, and c) adding compliance check

an annual balance sheet total not exceeding EUR 43 million." In the context of the agriculture sector, these actors could appear in the form of family farms.

[243] The certainty can be more easily achieved for *per se* unfair terms provisions (Article 13(3)) though. For the remaining issues, the Commission may need to release guidelines to increase clarity.

[244] This may be left to the sectoral regulations as each sector may have peculiarities that requires tailored regulations for standards and interoperability.

[245] See section 3.11 regarding the Chapter XI of the Data Act above.

[246] See Article 42.

mechanisms to disclose non-compliant companies for the farmers' enlightenment would be helpful.

References

Atik, C. (2021). Understanding the Role of Agricultural Data on Market Power in the Emerging Digital Agriculture Sector: A Critical Analysis of the *Bayer/Monsanto* Decision. in Michal Gal and David Bosco (eds), *Challenges to Assumptions in Competition Law* (Edward Elgar) https://doi.org/10.4337/9781839109072.00009

Atik, C. and Martens, B. (2021). Competition Problems and Governance of Non-personal Agricultural Machine Data: Comparing Voluntary Initiatives in the US and EU Journal of Intellectual Property, Information Technology and E-Commerce Law 12(3)

Atik, C. (2022a). Towards a Comprehensive European Agricultural Data Governance: Moving Beyond the 'Data Ownership' Debate. IIC - International Review of Intellectual Property and Competition Law (53)(5) https://doi.org/10.1007/s40319-022-01191-w

Atik, C. (2022b). Data Act: Legal Implications for the Digital Agriculture Sector. TILEC Discussion Papers Series DP2022-013

Atzberger, C. (2013). Advances in remote sensing of agriculture: Context description, existing operational monitoring systems and major information needs. Remote sensing, 5(2) https://doi.org/10.3390/rs5020949

Balducci, F., Impedovo, D., Informatica, D., & Moro, A. (2018). Machine learning applications on agricultural datasets for smart farm enhancement. Machines, 6(38). https://doi.org/10.3390/machines6030038.

Barbero, M. et al. (2016). Study on emerging issues of data ownership, interoperability, (re-) usability and access to data, and liability. Deloitte Report for the European Commission https://op.europa.eu/en/publication-detail/-/publication/74cca30c-4833-11e8-be1d-01aa75ed71a1/language-en

Blackburn G.A. (2006). Hyperspectral remote sensing of plant pigments. Journal of Experimental Botany 58(4) https://doi.org/10.1093/jxb/erl123

BO Akkerbouw (2019). Code of Conduct on Arable Data Use (Gedragscode Datagebruik Akkerbouw)

Caporaso, N., Whitworth, M.B., and Fisk, I.D. (2018). Near-Infrared spectroscopy and hyperspectral imaging for non-destructive quality assessment of cereal grains. Applied Spectroscopy Reviews. 53(8). 667-687. https://doi.org/10.1080/05704928.2018.1425214.

Case No COMP/M.8084 – *Bayer/Monsanto*, European Commission Decision (29 May 2018)

Coble, K. et al. (2016). Advancing U.S. Agricultural Competitiveness With Big Data And Agricultural Economic Market Information, Analysis, And Research. Report for the Council on Food, Agricultural and Resource Economics https://fabe.osu.edu/sites/fabe/files/imce/images/10-7-2016BigData_v1.pdf

Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (Text with EEA relevance) (notified under document number C(2003) 1422)

Commission Staff Working Document on the free flow of data and emerging issues of the European data economy Accompanying the document Communication Building a European data economy – SWD(2017) 2 final

Commission Staff Working Document on Guidance on sharing private sector data in the European data economy accompanying the document communication "Towards a common European data space" – SWD(2018) 125 final

Commission Staff Working Document on Common European Data Spaces – SWD(2022) 45 final

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Towards a common European data space – COM(2018) 232 final

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A European Strategy for Data – COM(2020) 66 final

Copa-Cogeca. (2016). Main Principles Underpinning the Collection, Use and Exchange of Agricultural Data - https://ec.europa.eu/futurium/en/system/files/ged/main_principles_underpinning_the_collection_use_and_exchange_of_agricultural_data_.pdf

Corentin, L. et al. (2018) GeoFIS: an open source, decision-support tool for precision agriculture data. Agriculture 8(6)73 https://doi.org/10.3390/agriculture8060073.

De Baerdemaeker, J. and Saeys, W. (2013). Advanced control of combine harvesters. IFAC Proceedings Volumes. 46(18) https://doi.org/10.3182/20130828-2-SF-3019.00069

Du, M. and Noguchi, N. (2017). Monitoring of wheat growth status and mapping of wheat yield's within-field spatial variations using color images acquired from UAV-camera system. Remote Sensing. 9(3):289, https://doi.org/10.3390/rs9030289.

EU Code of conduct on agricultural data sharing by contractual agreement (2018)

European Commission (2019). EU Member States Join Forces on Digitalisation for European Agriculture and Rural Areas. Shaping Europe's digital future https://digital-strategy.ec.europa.eu/en/news/eu-member-states-join-forces-digitalisation-european-agriculture-and-rural-areas

European Commission (2020). Expert Workshop on a Common European Agricultural Data Space https://digital-strategy.ec.europa.eu/en/library/expert-workshop-common-european-agricultural-data-space

Eurostat (2016). Agriculture statistics - family farming in the EU https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Agriculture_statistics_-_family_farming_in_the_EU#Structural_profile_of_farms_-_analysis_for_the_EU

EIP-AGRI. (2016). Data revolution: emerging new data driven business models in the agri-food sector. https://ec.europa.eu/eip/agriculture/sites/agri-eip/files/eip-agri_seminar_data_revolution_final_report_2016_en.pdf

Esmeijer, J. et al. (2015). Data-driven innovation in agriculture: Case study for the OECD KBC2-programme. TNO Report - R10154

Foley, J. A. et al. (2011). Solutions for a cultivated planet. Nature, 478(7369) https://doi.org/10.1038/nature10452

Godfray, H. C. J. et al. (2010). Food Security: The challenge of feeding 9 billion people. Science, 327(5967) https://doi.org/10.1126/science.1185383

Graef, I. and Husovec, M. (2022). Seven Things to Improve in the Data Act. SSRN https://dx.doi.org/10.2139/ssrn.4051793

Grasso, S. et al (2020). Arable farming: Top 5 technologies. Explore How Farmers Produce Food Sustainably - Online Course Material of the University of Reading https://www.futurelearn.com/info/courses/explore-how-farmers-produce-food-sustainably/0/steps/60781

Härtel, I. (2020). Report on the topic of "European Guidance and Rules for Agricultural Data" (European Agricultural Data Governance). Report for the German Ministry of Agriculture

Hermann, D. (2018). Optimisation of Combine Harvesters using Model-based Control. DTU Elektro PhD Thesis. https://orbit.dtu.dk/en/publications/optimisation-of-combine-harvesters-using-model-based-control

Jouanjean, M. et al. (2020). Issues Around Data Governance in the Digital Transformation of Agriculture: The Farmers' Perspective. OECD Food, Agriculture and Fisheries Papers No. 146 https://doi.org/10.1787/53ecf2ab-en

Khanal, S., Fulton J. and Shearer, S. (2017). An overview of current and potential applications of thermal remote sensing in precision agriculture. Computers and Electronics in Agriculture 139 https://doi.org/10.1016/j.compag.2017.05.001

Kritikos, M. (2017). Precision Agriculture in Europe – Legal, Social and Ethical Considerations. EPRS Report for the European Parliament

Leduc, G., Kubler, S. and Georges, J. (2021). Innovative blockchain-based farming marketplace and smart contract performance evaluation. Journal of Cleaner Production 306 https://doi.org/10.1016/j.jclepro.2021.127055

Lianos I and Katalevsky D, (2017). Merger Activity in the Factors of Production Segments of the Food Value Chain: - A Critical Assessment of the Bayer/Monsanto merger. CLES Policy Paper Series 2017/1 https://www.ucl.ac.uk/cles/sites/cles/files/cles-policy-paper-1-2017.pdf

Lieder, S., and Schröter-Schlaack, C. (2021). Smart Farming Technologies in Arable Farming: Towards a Holistic Assessment of Opportunities and Risks. Sustainability 13(12) https://doi.org/10.3390/su13126783

Martens, B. (2022). A mutual exhaustion rule on data rights to overcome the paradox of pro- and anti-competitive provisions in the EU Data Act. Discussion Paper.

Martínez, R., Pastor, J. Á., Alvarez, B. and Iborra, A. (2016). A Testbed to Evaluate the FIWARE-Based IoT Platform in the Domain of Precision Agriculture. Sensors (Switzerland), 16(11). https://doi.org/10.3390/s16111979

Michihisa I., Ikemura Y., Suguri M. and Masuda R. (2010). Cut-edge and Stubble Detection for Auto-Steering System of Combine Harvester using Machine Vision. IFAC Proceedings Volumes. 43(26) https://doi.org/10.3182/20101206-3-JP-3009.00025

Midtiby, H. S., Steen, K. A., and Green, O. (2018). In row cultivation controlled by plant patterns. Computers and Electronics in Agriculture, 153 https://doi.org/10.1016/j.compag.2018.07.037

Mutschler, P., Ulicny, U. and Reuters, T. (2018). Threats to Precision Agriculture. Public-Private Analytic Exchange Program. Public-Private Analytic Exchange Program Report for the Department of Homeland Security-USA http://dx.doi.org/10.13140/RG.2.2.20693.37600

Nasi, R. et al. (2018). Estimating biomass and nitrogen amount of barley and grass using UAV and aircraft based spectral and photogrammetric features. Remote Sensing, 10(7) https://doi.org/10.3390/rs10071082

Oksanen, T., Linkolehto R. and Seilonen, I. (2016). Adapting an industrial automation protocol to remote monitoring of mobile agricultural machinery: A combine harvester with IoT. IFAC-PapersOnLine 49(16) https://doi.org/10.1016/j.ifacol.2016.10.024

Peets, S., Mouazen, A. M., Blackburn, K., Kuang, B., and Wiebensohn, J. (2012). Methods and procedures for automatic collection and management of data acquired from on-the-go sensors with application to on-the-go soil sensors. Computers and Electronics in Agriculture, 81 https://doi.org/10.1016/j.compag.2011.11.011

Pinter Jr, P. J et al. (2003) Remote sensing for crop management. Photogrammetric Engineering & Remote Sensing 69(6)

Posada, J. C. (2014) Rights of farmers for data, information and knowledge. GFAR Report http://www.gfar.net/sites/default/files/rights_of_farmers_for_data_information_and_knowledge.pdf

Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), COM(2020) 842 final, 15.12.2020

Proposal for a Regulation (COM/2022/68 final) of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), 23.2.2022

Rasmussen, N. (2016). From precision agriculture to market manipulation: a new frontier in the legal community. Minnesota Journal of Law, Science and Technology 17

Regulation (EU) No. 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ('GDPR') [2016] OJ L 119/1

Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, OJ L 303, 59–68

Shang, L. et al. (2021) Adoption and diffusion of digital farming technologies - integrating farm-level evidence and system interaction. Agricultural Systems 190 https://doi.org/10.1016/j.agsy.2021.103074

Steen, K. A., Villa-Henriksen, A., Therkildsen, O. R., and Green, O. (2012). Automatic detection of animals in mowing operations using Thermal cameras. Sensors, 12(6) https://doi.org/10.3390/s120607587

Sundmaeker, H. et al. (2016). Internet of food and farm 2020' in Ovidiu Vermesan and Peter Friess (eds), *Digitising the Industry - Internet of Things Connecting the Physical, Digital and Virtual Worlds* (River Publishers)

Sykuta, M. E. (2016) Big Data in Agriculture: Property Rights, Privacy and Competition in Ag Data Services. International Food and Agribusiness Management Review 19

The Economist (2014). Digital disruption on the farm https://www.economist.com/business/2014/05/24/digital-disruption-on-the-farm

Thiessen, E. and Heege, H. J. (2013). Site-Specific Sensing for Fungicide Spraying. *Precision in Crop Farming* (Springer)

Tilman, D., Balzer, C., Hill, J., and Befort, B. L. (2011). Global food demand and the sustainable intensification of agriculture. In Proceedings of the national academy of sciences of the United States of America 108 https://doi.org/10.1073/pnas.1116437108

van der Burg, S. et al (2019). Ethics of smart farming: current questions and directions for responsible innovation towards the future. NJAS Wagening J Life Sci 90–91 https://doi.org/10.1016/j.njas.2019.01.001

van der Burg, S., Wiseman, L. and Krkeljas, J. (2021) Trust in farm data sharing: reflections on the EU code of conduct for agricultural data sharing. Ethics and Information Technology 23 https://doi.org/10.1007/s10676-020-09543-1

Verdonk, T. (2019). Planting the Seeds of Market Power: Digital Agriculture, Farmers' Autonomy, and the Role of Competition Policy in Leonie Reins (ed), *Regulating New Technologies in Uncertain Times* (Springer)

Villa-Henriksen, A., Edwards, G.T.C., Pesonen. L. A., Green O., and Sørensen C.A.G. (2020). Internet of Things in arable farming: Implementation, applications, challenges and potential. Biosystems Engineering, 191 https://doi.org/10.1016/j.biosystemseng.2019.12.013

Wiseman, L., Sanderson, J. and Robb, L. (2018). Rethinking Ag Data Ownership. Farm Policy Journal 15(1)

Wiseman, L et al. (2019). Farmers and their data: An examination of farmers' reluctance to share their data through the lens of the laws impacting smart farming. NJAS Wageningen Journal of Life Sciences 90–91(1) https://doi.org/10.1016/j.njas.2019.04.007

Wolfert, S., Ge, L., Verdouw, C., and Bogaardt, M. J. (2017). Big data in smart farming e a review. Agricultural Systems, 153 https://doi.org/10.1016/j.agsy.2017.01.023

Yanbo H., Lee M. A., Thomson S. J., and Reddy K. N. (2016). Ground-based hyperspectral remote sensing for weed management in crop production. International Journal of Agricultural and Biological Engineering, 9(2) https://ijabe.org/index.php/ijabe/article/view/2137

Zagórda, M. and Walczykova, M. (2018). The application of various software programs for mapping yields in precision agriculture. BIO Web of Conferences 10 https://doi.org/10.1051/bioconf/20181001018

Zude-Sasse, M., Fountas, S., Gemtos, T. A., and Abu-Khalaf, N. (2016). Applications of precision agriculture in horticultural crops. European Journal of Horticultural Science 81(2) https://doi.org/10.17660/eJHS.2016/81.2.2