EU Code of conduct on agricultural data sharing by contractual agreement.

The agri-food sector is moving into an era of digitally enhanced farming, where data is generated during the various stages of agricultural production and all related operations. This data is collected, transferred, processed and analysed. **The farmer remains at the heart of the collection, processing and management of agricultural data.** Collaborative agri-business models, including agri-cooperatives, collective shared services and other agri-businesses play a key role in ensuring that datadriven strategies add value to the agri-food chain. They can also facilitate collective services, be helpful in negotiating fair contracts and facilitate the implementation of the contracts. Data has become valuable and many experts consider BIG DATA to be the next major driver for productivity gains in agriculture. However, data analytics involve much more than simply putting information into expert hands; they are about enhancing knowledge in close collaboration with data originators and generating benefits within the value chain.

Digital farming represents an unprecedented opportunity to create value and business opportunities by applying data-driven solutions:

1. To improve resource efficiency, productivity, environmental processes, animal health and welfare and provide tools to mitigate climate change.
2. To adapt business plans, respond to dynamic markets and consumer expectations.
3. To decrease administrative and bureaucratic costs and enable science- based policies.
4. To provide better and more prosperous living conditions for rural communities.

Digital farming makes the collection and exchange of data possible at an unprecedented level. In order to tap into all of the potential benefits, data sharing between different stakeholders must be conducted under fair and transparent rules. The increasing exchange of data poses a major challenge for the EU agri-food sector. It raises questions about privacy, data protection, intellectual property, data attribution (sometimes referred to as ownership), relationships of trust/ power, storage, conservation, usability and security.

The nature of agricultural data is highly specific but very diverse. The collection of agricultural data includes, among others, livestock and fish data, land and agronomic data, climate data, machine data, financial data and compliance data. Some of this data may be considered to be personal data, sensitive data or be seen as confidential information from the point of view of many agro-businesses providing services/ equipment for farm activities. Agricultural data is therefore of economic importance for both farmers and the entire value chain and it is essential that the necessary safeguards are built in.

Theoretically, usage rights can be granted to an infinite number of parties, which reflects the non-physical nature of data. Due to this non- physical nature, it is difficult to monitor who is authorised to share data and what data is shared. Unintentional and uninformed sharing of data can disadvantage the data originators and the value chain (e.g. misuse of sensitive data, unfair

trading practices, breach of the legitimate IP right). This makes data originators, for instance, farmers, breeding companies, contractors, etc., cautious about sharing their data.

There is a common political view that assumes that increasing data sharing is only possible by making it mandatory, due to the originators' unwillingness to share data. The opposite is true: farmers and agri-businesses are more than willing to share data with each other and engage in a more open data mind-set. However, they will only do so if the potential benefits and risks are made clear and when they can trust that these are settled in a proper and fair way through contractual agreements. It is therefore crucial to define key principles on data rights, be they proprietary or similar rights, access rights and/or data re-use rights. Transparency and responsibility are key to gaining trust. If such principles are established and followed, then it will be possible to construct business models that benefit all stakeholders involved.

Given that technology and digital tools will continue to evolve, it is fundamental for all parties involved to engage in dialogue on the opportunities and challenges of data sharing.

This code predominantly focusses on non- personal data. Nevertheless, if data is linked to a person who is identifiable through a contract, land register, coordinates, etc., it is considered as personal data and falls under the General Data Protection Regulation.

We hope that this explanation will advise stakeholders on the main principles related to the rights and obligations of using and sharing data. This will ensure that stakeholders are confident that data is secure and handled in an appropriate manner as well as facilitate data-driven business models. Compliance with the code of conduct is voluntary. The signatories therefore encourage all parties involved in the agri-food chain to conform according to these jointly agreed principles.

Definitions

For the purpose of the Code of Conduct (Code), the following definitions apply:

1. Software Application: processing of data (input) by transforming it into different data (output). Often presented as a graph, on a dashboard or in some other manner to allow for interpretation to be used as new decision support information for value creation.
2. Pseudonymization: a procedure in which the most revealing fields within a data record are replaced by one or more artificial identifiers, or pseudonyms. The pseudonym allows the data to be traced back to its origins, which distinguishes pseudonymization from anonymization. The purpose of pseudonymization is to render the data record less identifiable and therefore lower the risks involved in its use. (See definition in GDPR1).
3. Data: All forms of information that are transferred between the data originator, data provider, data users or third parties during the course of a business operation.
4. Personal data1: Any information relating to an identified or identifiable natural person (‘data subject'). An identifiable natural person is someone who can be identified, directly or

indirectly, notably by referring to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

5. Anonymised Data: Data that has been rendered anonymous, and is thus no longer personal, by irreversibly stripping it of any identifiable information. This makes it impossible to gain insights into a discreet individual, even by the party that is responsible for the anonymization. Privacy laws, including GDPR2, do not apply to anonymized data since it is not personal.
6. Publicly available Data: Data that can be freely used, reused and redistributed by anyone with no existing local, national or international legal restrictions on access or usage3 (e.g. Copernicus, weather data, Eurostat, etc.)
7. Raw Data: Data that is generated and collected without editing or any other form of processing.
8. Metadata: Data that provides information on other data (e.g. author, units).
9. Primary Data: Raw Data transformed into values that are identifiable by people (primary processing). For example, field data (e.g. parcel, geological data, soil data, water data, cultivation, production- related data of a specific farm).
10. Aggregated Data: A combined dataset made up of a few or a wide range of sources (e.g. sensors, systems, farmers or data platform). The aggregation of data can provide information (e.g. benchmarking and analytics) that can provide the data originator with additional value when compared to data from a single source. Moreover, if revealing information is stripped away, aggregating can be done anonymously.
11. Agricultural data: Data related to agricultural production, including farm data and all types of data generated within the farming processes (refer to annex).
12. Big Data: Vast volumes of highly diverse data that can be captured, analysed and used for decision-making.
13. Data originator (sometimes referred as “owner”): In this code the originator (owner) is generally defined as “the person or entity that can claim the exclusive right to license access to the data and control its downstream use or re-use”, i.e. the party that the data is attributed to. The data originator of all the data generated during the operation is the one who has created/collected this data either by technical means (e.g. agricultural machinery, electronic data processing programs), by themselves or who has commissioned data providers for this purpose.
14. Data provider: A natural or legal person that under an agreement delivers data to the Data user and/or Data originator.
15. Data sharing: The practice of making data available to data users or third parties.
16. Data originator (sometimes referred as “owner”): In this code the originator (owner) is generally defined as “the person or entity that can claim the exclusive right to license access

to the data and control its downstream use or re-use", i.e. the party that the data is attributed to. The data originator of all the data generated during the operation is the one who has created/collected this data either by technical means (e.g. agricultural machinery, electronic data processing programs), by themselves or who has commissioned data providers for this purpose.

17. Data provider: A natural or legal person that under an agreement delivers data to the Data user and/or Data originator.
18. Data sharing: The practice of making data available to data users or third parties.

Data user: A natural or legal person that receives data from the data originator or data provider under an agreement with the data originator.

Controller: The natural or legal person, public authority, agency or other such body that, alone or in hand with others, determines the purposes and means of the processing of personal data. Where the purposes and means of such processing are determined by European Union or Member State law, the controller or the specific criteria for their nomination may be provided for by European Union or Member State law.

Processor: A natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller.

Processing: Any operation or set of operations that is performed on data or on datasets, whether by automated means or not, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or other methods of making the data available, alignment or combination, restriction, erasing or destruction4.

Data storage: The recording (storing) of information (Data) in a storage medium. The data originator can store data in a primary location, in a data platform or in cloud-based storage platforms. The location in which data is stored is referred to as the "data storage location" or "storage location" or "storage site".

Data portal: A list of datasets with pointers facilitating access to those datasets.

Through portals, the data user is able to operate the applications (as an interface or for a functionality) developed in the data platform5.

Data Platform: Software where applications are made available for data processing. Data platforms may be closed (just for members or open for Application Programming Interfaces - APIs), or may be open source hardware platforms and software libraries.

Decision Support Information: outcome of an application, usually information that supports decision making.

EU Code of conduct on agricultural data sharing by contractual agreement

Attribution of the underlying rights to derive data (Also referenced as data ownership)

As a basic principle, when data is produced by an agri-chain operator due to their activity or is commissioned by this operator, the operator is considered the data originator. The right to determine who can access and use the data is attributed to this operator. This does not cover data/information generated by processing this data from multiple originators (e.g. aggregating), but the provision of data for such purposes should be part of an agreement. For instance, the rights regarding data produced on the farm or during farming operations are granted to ("owned by") the farmer and may be used extensively by them.

The nature and means of collecting different agricultural data leads to different levels of attribution of data rights ("ownership"). Data cannot be owned in the same way as physical assets. It is therefore crucial to set some key principles for agricultural data access and usage rights.

The parties (originator, provider, user, third party) should establish a contract clearly setting the data collection and data sharing conditions according to the needs of the contracting parties.

Details referring to data sharing must feature in a dedicated and exclusive section of the contract, where possible.

The contract should acknowledge the right of all parties to protect sensitive information (e.g. IP) via restrictions on further use or processing. Parties may not use, process or share data without the consent of the data originator.

This Code recognises the data originator's right, whether they are a farmer or another party, to benefit from and/or be compensated for the use of data created as part of their activity. It also recognises the need to grant the data originator a leading role in controlling the access to and use of data from their business and to benefit from sharing the data with any partner that wishes to use their data. Therefore, the contract should clearly establish the benefits for the data originator. The originator could be compensated for the value created either financially or by agreed exchange of services, better products, or any other form agreed by both parties.

All contracts shall use simple and understandable language in order to explain the content or be accompanied by an informal document that explains data-related aspects. This contractual agreement should clearly specify:

1. the most important terms and definitions
2. the purpose of collecting, sharing and processing the Data.
3. rights and obligations that the parties have related to Data, rules and processes for data sharing, data security and the legal framework in which the data is kept and in which back-ups are stored.
4. the software or the relevant application and information on the storage and use of the agricultural data

5. verification mechanisms for the data originator
6. transparent mechanisms for adding new and/or future uses.

Data access, control and portability

The collection, access, storage and usage of the collected agricultural data can only occur once the data originator has granted their explicit, express and informed permission via contractual arrangement. The data originator must be informed in a clear and unambiguous manner if someone intends to collect and store their data. If both parties are in agreement, the contract should specify the conditions according to which the identification of the data originator may be possible. Otherwise, the data should be subject to pseudonymisation.6

The data originator must give permission for their data to be used and shared with third parties, including circumstances in which decisions are made based on the data. Information should only be given to third parties as aggregated, pseudonymized or anonymized data, unless it is required to deliver the requested service and/or the conditions specified in the contract. Unless specified in the contract, the data user must take all precautions to avoid re-identification.

Data must be collected and used for the specific purpose agreed in the contract. The datasets should only be kept for as long as is strictly necessary for the relevant analyses to be carried out. In addition, data should only be accessed by those with the required authorization.

Access to data, be it in read-only or fully editable modes, should be strictly audited and any transfer or change to the data (e.g. input, modification, removal) should be fully traceable, e.g. accompanied by metadata about the author and modification.

Data originators should be granted appropriate and easy access and be able to retrieve their attributed ("own") data further down the line, unless the aggregated data is not linked to the attribution as it is not only based on the data of the data originator. It is essential to make the data provider ("collector") responsible for making the data easily available to the data originator in a format that they will find accessible and readable, where technically feasible. If not technically feasible, the data provider should provide justification.

The data originator shall have the right to receive the data concerning their operation as specified in the contract, in a structured, frequently used and machine-readable format.

Unless otherwise agreed in the contract, the data originator has the right to transmit this data to another data user. If agreed between the parties, the data originator shall have the right to have the data transmitted directly from one data user to another, where technically feasible.

Furthermore, originators should be in no way restricted should they wish to use their data in other systems/platforms/ data storage facilities (portability of data), unless stated in the contract. Therefore, the data user shall disclose the means (e.g. if and how) through which a data originator may view, correct, retrieve or extract data. The means through which they may migrate data pertaining to their farming operations to another service and the electronic data interchange standards and formats which are supported shall also be made clear.

This should be done without compromising restricted access to machine data or sensitive data (only relevant to the correct functioning of the machinery). This should be clearly specified in the contract, e.g. between farmers/contractors and device manufacturers.

Data protection and transparency

It is essential for data users who control the database to have a protocol on data protection safeguards for individual originators, one that does not allow unauthorised sharing with third parties. Furthermore, personal data in databases must be both stored under a pseudonym and encrypted or protected with similar methods. This is to render the data less identifiable and mitigate risks both during the course of normal operations and in the event of a data breach.

Data users should provide contact details that the data originator can use to get support, clarifications or to voice complaints.

Contracts must not be amended without the prior consent of the data originator. If data is to be sold or shared with a third party that is not initially mentioned in the contract, the data originator must be able to agree on or refuse this, without financial or other repercussions. The data user can only sell or disclose data to a third party if he/she has secured the same terms and conditions as specified in the contract between data user and originator.

Data originators must be given the possibility to opt out of the contract and terminate or suspend the collection and usage of their data, provided that the contractual obligations have been met. This must be clearly stated in the contract and data originators should be informed of the consequences of these decisions. Either this should be done upon their first request and is of immediate effect or it should be done after a previously defined notice period of a reasonable duration. This clause must grant the data originator permanent access to their data during the notice period.

If several different services are on offer, data originators must be able to opt for none, one or some. In order to make an informed decision, a data user that offers services should explain all of the services and features involved in the different options.

In order to facilitate data sharing, this Code encourages partners in the agro-food chain to set up tools to support decision-making systems for data originators as well as for data users that would allow them to integrate a vast array of data. This should involve different partners of the food chain, in particular data originators, in order to effectively contribute to their development and better respond to their needs.

Privacy and security

The contract should clearly define the data user's/provider's security and confidentiality responsibilities. The data user should keep track of the data as much as possible throughout the value chain and share the gathered information with the data originator. Collectors and users of farm data must therefore not use this data for unlawful purposes or take advantage of it to speculate or for other such purposes.

If the data is being used to make decisions about the data originator “as a natural person” the GDPR applies. Therefore, the data user, now the controller, shall provide the data originator, now the data subject (directly or indirectly, identified or identifiable natural person) with the information necessary to ensure fair and transparent processing. If automated decision-making is used on personal data, the data subject shall be briefed about its existence, including profiling7, and at least in those cases, meaningful information about the logic and/or the nature of the algorithm shall be provided, as well as the significance and the envisaged consequences of such processing for the data subject. Data must not be used to assess the originator's ability to pay for a service or machine.

In general, the data user commits to protecting the data received from the data originator, against loss, theft, unauthorized access and alteration by non-authorized persons.

In addition, sensitive agricultural Data must be able to benefit from a special regime regarding the rights of access, use or sharing as well as any

security enhancements (e.g. masking, encryption, authentication, secure internet flow, etc.) as defined in the contract between the farmer and the data provider or user. As good practice, Data users could appoint a data protection officer, who could play an important role in assuring that data originators' rights are respected, as stated in the GDPR.

There must be the option to remove, destroy (e.g. right to be forgotten) or return all original data (e.g. farm data) upon the data originator's request. If hacking, seizure, confiscation, insolvency or settlement proceedings are detected, the data originator should be immediately informed by the data user about the non-personal data being compromised and the measures taken. For personal data the obligations under the GDPR apply9.

Data users who control databases commit to regularly implementing backup and recovery protocols to prevent data loss in the event of a crisis. It is vital to provide the necessary security safeguards against disclosure, modification, destruction, loss or unauthorised access, at an affordable cost. There must also be protocols to implement in the event of a breach and records of any potential breaches or unauthorised attempts to access the data must be kept.

The Data originator and data user are responsible for login data and will handle this with care. Users must ensure that login information remains secret.

Liability and intellectual property rights

The terms of liability should be clearly laid out in the contract.

The data originator guarantees the accuracy and/or completeness of the raw data to the best of their knowledge. However, they are not liable for damage arising from and/or connected with the generation, receipt and/or use of this data by machines, devices, data users and/or third parties.

Protecting trade secrets, intellectual property rights and protecting against tampering are the main reasons as to why information is not shared and why even business partners in joint projects are not permitted to receive data.

One main issue is being able to guarantee that these two interests, expressed as licensing conditions in the contracts, are respected. Protecting the intellectual property rights of the different stakeholders in the value chain is fundamental.

“Protecting trade secrets, intellectual property rights and protecting against tampering are the main reasons as to why information is not shared and why even business partners in joint projects are not permitted to receive data.”

Different types of data in the agro-food sector*

1. Agricultural data
   Farm data – data referring to farms and farm operations, including farm management.

   Agronomic data – related to plant production (e.g. yield planning, soil data, input data)

   Compliance data – data required for control and enforcement in relation to competent authorities.

   Livestock data - related to the herd (e.g. age, sex, performance indicators such as milk yield and live weight, animal welfare and health indicators, input data).

   Machine data - used for machine operations (e.g. data flowing between system controllers and machine sensors), often encrypted and not made available to prevent “reverse engineering” or modifications on the on-board system communication which could result in the malfunctioning of controls in place to protect the operator and the machine.

   Service data – data used for vehicle maintenance and repair.

   Agri-supply data (input) - related to the nature, composition and use of inputs such as fertilizers, feedstuffs, plant protection products, etc.

   Agri-service provider data - data originating from an agricultural services provider operating to benefit a client (e.g. farmers). Of sole interest to the management of the service-providing company (e.g. working time of an employee, machine performance) and not related to the farm or farm operations.

   According to the Personal Data Regulation (EU) 2016/679, personal data means any information relating to an identified or identifiable natural person (‘data subject'); an identifiable natural person is one who can be identified, directly or indirectly.

CASE STUDIES

Case study 1: Precision feeding programme

A compound feed manufacturer is proposing a service designed to optimise feed conversion rate to pig farmers. To this end, the feed producer asks a service provider to implement sensors to

measure the amount of feed consumed by a (group of) pig and to collect information on the weight of the animals, the amount of water they drink, other parameters related to the breed, age and sex of the animals the housing (temperature and hygrometry), etc.

The compound feed manufacturer processes and aggregates the data to evaluate the performance of different types of feed formulation (ingredients, nutritional values) across the different farms and to compare the differences to the different parameters collected. Based on that, he is able to provide the pig farmer with advice on how to best use the feed, including which parameters to change.

In such cases, the pig farmer is the data originator, the service provider is the data provider and the feed manufacturer is the data user.

The nature of the processes that the feed manufacturer intends to perform and to whom the data will be accessible should be defined in the contract.

The contract should also specify to which other data users the farmer may provide the data, for example a dairy cooperative, and under which conditions, considering that the set of data may contain not only the data from the use of the feed on the farm but also on the composition of the feed (in which case the feed manufacturer is the data originator for that type of data and for which the feed manufacturer can claim IP rights.).If specified in the contract the data of the data provider can be provided directly to this cooperative. This data exchange can be bundled in one contract with multiple parties signing.

If the service provider like to contract an IT company for data assessment, the service provider is also a data user and the IT company a third party. The terms for providing the data to the third party will be specified in the contract.

Similar business models and data relationships are present in the animal breeding sector.

Case study 2: Pest alert system

The provider of the service offers crop-based agricultural holding owners extensive support in setting up a pest alert system. It is based on the use of sensors, placed in various positions across the field of a given farmer, weather stations and mathematical models created by scientists that allow for the probability of plant disease or increased pest activity to be calculated. Models have been created by taking into account a set of factors that may increase disease development. Sensors and weather stations monitor field conditions, focussing mainly on humidity, wind speed and direction, as well as temperature. The system also takes into account the topography of the area (e.g. natural barriers) thanks to the use of GIS (geographical information system) data.

Monitoring services are connected to the IoT infrastructure, which sends information to the central database for further processing. As a result, the farmer receives valid pieces of information on what illnesses and pests may attack plants, what substances should be used to prevent such diseases, as well as when they should be used in order to have an optimum effect. Through using machine learning, the service provider aims to increase the number of sensors in the network.

With this system, two types of data can be identified: the data provided automatically by sensors (weather data, soil humidity, etc.), as well as that provided by farmers (such as treatment history). It can be, therefore, be assumed that the data originators are the farmers (if in the farm of during farm operations), also from data of sensors that are owned by the farmer. If sensors are not owned by the farmers, the sensor owners are seen as data providers.

Publicly available data (Satellite, meteorological data) will also be used in the data processing by the scientist (data user) and the service provider acts as the data provider.

The farmer should be informed about the fact that their Data is processed, as well as about their benefits and responsibilities (including the possibility of data modification or deletion, data transfer, and the right to be forgotten), and the purpose of the data processing. The service provider should keep a processing register, assess processing efficiency, as well as provide a proper technical and organisational means to ensure that the data processing is fully secure. A greater contribution (for example – more sensors, weather stations or a longer presence within the network) must also generate more benefits for the data originator.

Case study 3: Illness forecasting system for dairy-cows

In this case, the parties involved are: farmers, milking system producers, dairy cooperative, vets, scientists and the service provider.

This service would be based on collecting data on the milking capacity of cows and comparing this with Data on milk collection in order to assess illness likelihood and the factors contributing to it. Thanks to extensive Data collection, it would be possible to specify factors contributing to various illnesses, identify illnesses more rapidly and even carry out preventive actions. Aggregating milk production data, collected for the most part on a daily basis, would allow farmers to react in a swift manner.

Farmers, milking system producers, and dairy cooperatives would provide data on the milking capacity of individual cows, whereas vets, based on animal treatment records, would provide information on the occurrence of particular illnesses. The role of scientists would be to draw conclusions by comparing milking capacity and illness record data. The service provider would ensure a user-friendly interface and a satisfactory data flow.

The farmer is the data originator of all the data related to the farm of farm operations.

Data users: service provider (veterinary, advisor) and milking cooperatives (providing e.g. aggregated data for comparison reasons), Data scientists, milking system provider or in some cases agri-cooperatives when collecting data from several farmers and processing it in order to produce information (e.g. benchmarking) etc.

Case study 4: producing potatoes using an agricultural contractor.

A farmer wants to grow potatoes and asks an agricultural contractor with high-tech machinery to do the operations from seeding, crop maintenance and harvesting. As agreed, the agricultural contractor will provide the farmer with the agronomic data from the fields measured with the

machinery/sensors. This could be location specific yield-, soil-, crop- or input data or general data for that field, such as amounts of fuel, seed, pesticide and fertiliser used.

This is specified in a contract between the farmer (data originator) and the agricultural contractor (data provider).

At the same time, the agricultural contractor has a contract with the different suppliers (machinery, pesticides, fertiliser etc.). Here the agricultural contractor acts as the data originator and the supplier as the data user. The contract with the farmer will specify the agronomic data that is passed onto the supplier and its purpose.

For operation-specific data such as machine operation (including machine data related to the functionality of the machine or working time of the driver), and not related to the farmer or farm operation, this is not necessary, this is not necessary.

The agricultural contractor could also act as a data user by processing the agronomic data collected and providing additional services to the farmer to help them make the right decisions (e.g. pesticide spraying time, fertiliser use etc). The same contract can specify these both services provided as Data provider and Data user. Providing any agronomic data on software platforms must be specified. In the contract between the agricultural contractor and the platform, the agricultural contractor is the data user and the platform is the third party.

There is the possibility to have a contract that bundles multiple actors in a chain.

The farmer as the data originator can agree with other advisor and platform services, (all considered data users).

The farmer (data originator) can provide data to land owners, potato processors, the government, paying authorities (data users) etc. These organisations can use that data further in the chain for specific purposes as agreed in the contract between data originator and data user.

Regulatory framework

This document contains non-binding guidelines and is not to be used as a legal document. Legal documents fall solely under the jurisdiction of the EU and national decision makers. That said, it will make reference to relevant EU legislation. Furthermore, these recommendations shall not apply to the performance of a task carried out in the public interest or to exercising a request to supply information based on an obligation foreseen by law. Therefore, please find the references to the most relevant regulatory frameworks on the sharing of agricultural data below.

Regulation (EU) 2016/679 of the European Parliament and of the Council from 27th April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/ EC (General Data Protection Regulation)10

Please be aware that for non-personal data, each Member States may apply its own legislation. Please take note of the proposal for a regulation on a framework for the free flow of non-personal data in the European Union COM/2017/049511.

Regulation (EC) No 593/2008 of the European Parliament and of the Council from 17th June 2008 on the law applicable to contractual obligations (Rome I)12.

Directive 96/9/EC of the European Parliament and of the Council from 11th March 1996 on the Legal Protection of Databases13.

Directive (EU) 2016/943 of the European Parliament and of the Council from 8th June 2016 on the protection of un- disclosed know-how and business (trade secrets) against their unlawful acquisition, use and disclosure14.

Proposal for an EP and Council regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on privacy and Electronic Communications) COM/2017/010 final – 2017/03 (COD)15.

Directive 2004/48 enforcement of IPR Corrigendum to Directive 2004/48/ EC of the European Parliament and of the Council from 29th April 2004 on the enforcement of intellectual property rights (OJ L 157, 30.4.2004)16.

Please be aware that several sectorial regulations may apply, such as:

- Council Regulation 2100/94 on Community plant variety rights17 and Commission Regulation 1768/95 implementing rules on the agricultural exemption provided for in Article 14(3) pf Council Regulation 2100/9418.
- The Animal Breeding Regulation is regulation 2016/1012 on zootechnical and genealogical conditions for the breeding, trade an and entry into the Union of purebred breeding animals and, hybrid breeding pigs and the germinal products thereof.

Main legal principles in order to have a balanced contract - Contract check list for agricultural data.

When using a product or service that captures or uses agricultural data, answer the following questions:

Is there an agreement/contract in place?

What obligations are there? What warranties and indemnities are there for each party?

What data is collected?

Who owns/controls access to the data? What services are delivered?

Will my data be used for purposes other than providing me, the data originator (e.g. farmer), a service? Is it clear what these are? Can I agree/disagree? What are/is the benefits/value for me (as data originator)?

Is the data shared with other parties? What rules do the external parties adhere to? Can I agree/disagree with sharing data with other parties?

Can the service provider change the agreements unilaterally? What happens when the service provider changes ownership? Can I retrieve my dataset from the system in a usable format? Will I be updated on security breaches?

Can I opt out of the service and have my data deleted from the system? Is there a contact point to assist me with any questions that I may have? Do I need insurance?

What are the confidentiality terms?