



Regenerating soils for climate and farmers

Ethical and legal requirements

An identification of the relevant ethical and legal frameworks related to the AgriCapture project and platform.



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 101004282.

The content of this publication exclusively reflects the author's view and the Research Executive Agency and the Commission are not responsible for any use that may be made of the information it contains.



Document control page

Project	AgriCaptureCO2
Project, full title	Developing EO-powered services to promote soil carbon sequestration through regenerative agriculture
Project number	101004282
Project start	1 January 2021
Deliverable	D1.2
Work Package	WP1 MANAGE: project management
Document title	Ethical and legal requirements
Version	V11
Responsible author	ARL
Contributors	Arthur van der Wees, Anna Ida Hudig, Dunja Madunic, Prakriti Pathania, Dimitra Stefanatou, (ALBV)
Date of delivery	31.08.2021
Due date of deliverable	31.08.2021
Type	Report
Language	English
Rights	Copyright "AgriCapture consortium"
Dissemination level	Public

Version history			
Version	Implemented by	Date	Description
V1	ALBV	15.07.2021	Table of Contents
V2	ALBV	26.07.2021	Initial input under chapters 1, 2 and 3.
V3	ALBV	28.07.2021	Additional input under chapter 2 and 3.
V4	ALBV	03.08.2021	Initial input under chapters 4,5,6 and 7.



V5	ALBV	6.08.2021	Initial input under chapters 8 and 9.
V6	ALBV	09.09.2021	Initial input under chapters 10.
V7	ALBV	12.08.2021	Additional input under all chapters.
V8	ALBV	20.08.2021	Consolidation of input and editing across the entire document.
V9	ALBV	23.08.2021	Refinements across all chapters.
V10	ALBV	27.08.2021	Version submitted for internal review.
V11	ALBV	31.08.2021	Integration of internal review comments and final submission.



Table of contents

Executive summary	6
List of abbreviations	7
Table of figures.....	10
1 Introduction	11
1.1. Aim	11
1.2 Scope	12
1.3 Methodology	13
1.4 Target audience	15
1.5 Structure.....	16
2 Market-Centric Perspective.....	17
2.1 Intellectual Property & Contract Law	17
3 Sustainability Perspective	20
4 Data-centric perspective	22
4.1 The Free Flow of Non-Personal Data Regulation	23
4.2 The Data Governance Act	24
4.3 Trade Secrets Directive.....	26
4.4 Other relevant instruments	27
5 Economic Perspective.....	29
5.2 Revised Payment Services Directive.....	29
6 Human-Centric Perspective	31
6.1 General Data Protection Regulation.....	31
6.2 Regulation on electronic identification and trust services for electronic transactions.....	33
7 System-Centric Perspective.....	35



7.1 The Artificial Intelligence Act.....	35
7.2 The Cybersecurity Act.....	39
8 Ethics in practice	42
8.1 Accountability by design.....	42
8.2 Other built-in values	43
9 Conclusion.....	44
References.....	45
Annexes.....	48
Annex I	48



Executive summary

The overarching objective of the AgriCapture H2020 project is “to promote regenerative agriculture as a solution in the fight against climate change while providing agronomic and economic benefits for farmers”. AgriCapture revolves around the fixation of carbon in the soil by means of regenerative agriculture to reduce atmospheric carbon emissions and strengthen the position of farmers from a business point of view. To this end, sensory devices, including satellites, are deployed to collect and process soil and climate-related data. Processing of such digital data entails a series of benefits, for instance, by increasing transparency and facilitating auditability, while being, also, subject to specific requirements applicable to the organizations with a role in the respective operations.

In this context, the project provides for a dedicated task, Task 1.3 on Legal and Ethical Issues that identifies the most relevant ethical and legal requirements related to AgriCapture project and platform. The present deliverable, therefore, elaborates on several EU regulations selected from different perspectives and looks into the applicability of those to regulations (e.g. Product Liability Directive, Free Flow of Non- Personal Data Regulation) to AgriCapture project, aiming to give answers to key questions, such as:

- a) *Who has insight to the data?*
- b) *Who controls the data?*
- c) *What happens with the data after collection?*
- d) *How can business interests, including IP, be protected, whilst encouraging knowledge exchange?*

To this end, the deliverable introduces a customised methodology. To give an extensive and holistic overview of the legal landscape in the context of which AgriCapture’s stakeholders interact – or may interact in the foreseeable future – with a wide range of regulatory frameworks is discussed through different lenses. These lenses, roughly ordered by relevance to the subject matter, include (1) the market-centric perspective; (2) the sustainability perspective; (3) the data-centric perspective; (4) the economic perspective; (5) the human-centric perspective; and (6) the system-centric perspective. The regulations selected that are considered as mostly relevant for AGRICAPTURE are discussed in the light of the above-mentioned perspectives.

Note that deliverable provides for additional considerations and tools to build in the principle of *accountability* and the other ethical principles by design aiming, thus, to render, in reality, AgriCapture outcomes not only compliant with the applicable legal requirements, but, also, future-proof and risk-resistant.



List of abbreviations

AI	Artificial Intelligence
AISP	Account Information Service Providers
CADA	Continuous Appropriate Dynamic Accountability
CDM	Clean Development Mechanism
COVID	Corona Virus Disease
CSA	Cybersecurity Act
CSRD	Corporate Sustainability Reporting Directive
DGA	Data Governance Act
DG Trade	Directorate General for Trade of the European Commission
DPIA	Data Protection Impact Assessment
eID	Electronic Identification
eIDAS	Regulation on Electronic Identification
EIONET	European Environment Information and Observation Network
EIP AGRI	Agricultural European Innovation Partnership
ENISA	European Union Agency for Cybersecurity
ESG	Environmental, Social and Governance
EU	European Union
EUIPO	EU Observatory on Infringements of Intellectual Property Rights



GDPR	General Data Protection Regulation
GHG	Greenhouse Gas
ICT	Information Communications Technology
IIA	Initial Impact Assessment
IP	Intellectual Property
IPAP	Intellectual Property Action Plan
IPR	Intellectual Property Rights
IT	Information Technology
LUCAS	Land Use Cover Area Frame Survey
PIN	Personal Identification Number
PISP	Payment Initiation Service Providers
PSD2	Revised Payment Services Directive
SCA	Strong Customer Authentication
SFDR	Sustainable Finance Disclosure Regulation
TSD	Trade Secrets Directive
UAV	Unmanned Aerial Vehicles
UK	United Kingdom
UN	United Nations
UNCBD	United Nations Convention on Biological Diversity



UNCCD	United Nations Convention to Combat Desertification
UNFCC	United Nations Framework Convention on Climate Change



Table of figures

Figure 1: Ecosystem for the Rule of law in the Digital Age	11
Figure 2: AGRICPATURE subject matter from different perspectives.....	13
Figure 3: Applicable EU regulations and technology domain of interest.....	15
Figure 4: PSD2 – A new level playing field for the financial services industry and third-party organisations.....	30
Figure 5: The four risk levels of AI as indicated by the proposed Artificial Intelligence Act.	36
Figure 6: Prohibited uses of AI, according to Article 5 of the proposed Artificial Intelligence Act.	39
Figure 7: Multi-angled stakeholders & influencers.....	48



1 Introduction

On April 20th, 2020, European Commission President, Ursula Von der Leyen, stated that “we now need to build a resilient, green, and digital Europe”. The activities within AgriCapture Horizon2020 project correspond directly to this objective set by European Commission in particular, by utilising regenerative agriculture to fixate carbon in the soil. The endorsement of such an approach could reduce the CO₂ concentration in the air, while increasing the agro-economic benefits for farmers.

1.1. Aim

The overarching objective of AgriCapture is to promote regenerative agriculture as a solution in the fight against climate change while providing agronomic and economic benefits for farmers. Given that the agricultural sector is responsible for 18.4% of the global GHG emissions¹, reforming agriculture is key in solving the climate crisis. In this respect, AgriCapture is developing an innovative, robust, and scalable solution to measure carbon capture in soil.



Figure 1: Ecosystem for the Rule of Law in the Digital Age

¹ Hannah Ritchie and Max Roser (2020) - CO₂ and Greenhouse Gas Emissions. Published online at OurWorldInData.org [Online Resource]. Available at: <https://ourworldindata.org/co2-and-other-greenhouse-gas-emissions>.



1.2 Scope

This project is conducted in a market context, where farmers in their capacity as independent market entrepreneurs could strengthen their business models by means of the innovations provided for by AgriCapture project.

The project's focus is mainly on soil from a sustainability perspective, which could be considered as forming the first layer; the second layer could be considered agriculture, including CO₂ fixation in the soil. The third layer could be considered data, which could play -amongst other- a role in relation to transparency and to the creation of a trusted environment. Data are also a useful tool to verify whether the envisioned additional carbon reduction is realised, and to audit the carbon credit attribution. Furthermore, the project includes, but is not limited to, different elements of productivity, public good, carbon credits and ecotourism.

In light of the project's overarching objectives, Task 1.3 on Legal and Ethical Issues that surfaces the most relevant ethical and legal requirements related to AgriCapture project and platform. The AgriCapture platform includes all products, services and stakeholders that are involved in quantifying, verifying, and promoting soil organic carbon capture, allowing (i) farmers and other landowners to become "carbon farmers", (ii) food companies to offset their carbon footprint and offer "zero carbon" products, and (iii) certifying organisations to scale up and automatise their processes.²

The present deliverable, therefore, elaborates on several EU regulations selected from different perspectives and looks into the applicability of those to regulations (e.g. Product Liability Directive, Free Flow of Non-Personal Data Regulation) to AgriCapture project, aiming to give answers to key questions, such as **who has insight to the data, who controls the data, what happens with the data after they are collected and how can business interests, including IP, be protected, whilst encouraging knowledge exchange**. The regulations discussed may require certain project partners, depending, also, on their role in the project, to comply with or they could serve an inspiration for them to take the extra mile and take the respective requirements into account, although they are not formally bound by them.

The emphasis of this deliverable is on data, including, exercise of control on data and personal data protection; the discussion, however, elaborates on a wide range of issues, including IP, sustainability and payment services. Certain topics are considered, however, out of scope. These include food and food safety issues, producing, space, water, and financial institutions. Furthermore, D7.2: NEC (Non-EU Countries) – Requirement No.2,



already submitted to European Commission has elaborated separately on the participation of 3rd countries in AgriCapture consortium.

1.3 Methodology

This deliverable adopts a multi-angled approach, meaning that the legal and ethical aspects of the subject matter of AgriCapture will be analysed from different perspectives, as captured in Figure 2 below.

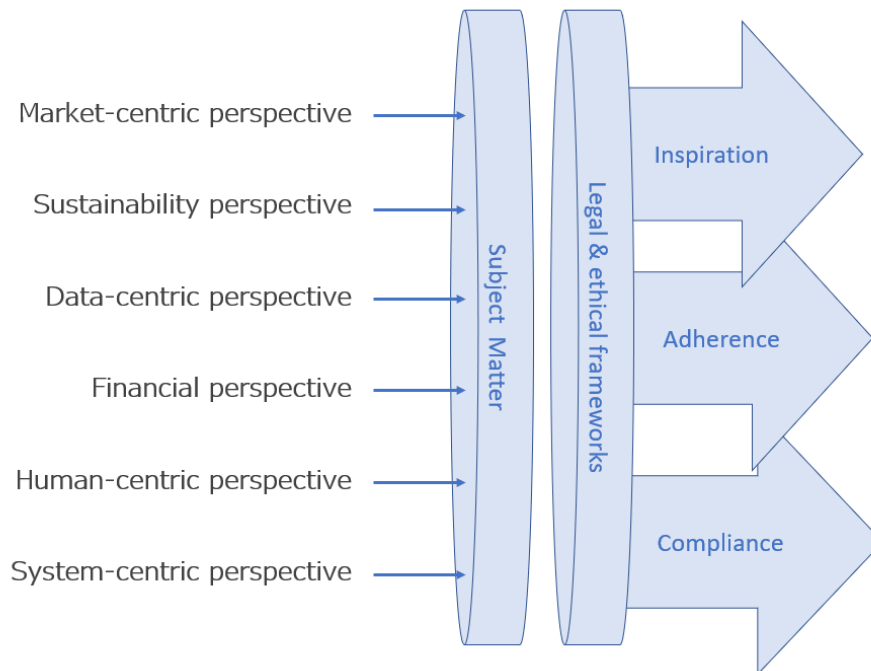


Figure 2: AGRICPATURE subject matter from different perspectives

In the figure above, the subject matter represents the contextual circumstances as a lens through which the different perspectives are projected. These perspectives further elaborated in this deliverable are: market-centric, sustainability, data-centric, financial/economic, human-centric and system-centric (Table 1). It is considered that regulations are not necessarily bound to one or two perspectives; the perspectives rather resemble a spectrum or lens through which light can be shined on the specific subject matter, in this case the AgriCapture project. The subject matter can be further approached on the basis of three separate scales: small scale, medium scale or large scale. As a follow from this analysis, the applicability of regulatory frameworks could depend on the scale on which the project is performed.



Market-centric	Involves the transactions between different stakeholders, as well as sector-specific regulations, and business and IP law.
Sustainability	The environmental sustainability aspects of the project, mostly associated with climate and soil.
Data-centric	Focused on the flow of digital data.
Financial/economic	Focused on mostly the financial economic regulations, such as payment services but also IP.
Human-centric	The human-centric frameworks focus on protection of human rights such as privacy.
System-centric	System-centric frameworks position a technology, such as software or a certain device, central in a regulation.

Table 1: description of the six different perspectives

Legal and ethical frameworks

There are three sorts of outcomes within each perspective, that will be relevant for the pilots: *inspiration*, *adherence* and *compliance*. For the purpose of the present discussion, laws that are not strictly applicable but might be beneficial for stakeholders to bring up new ideas or make policies future-proof are considered to be inspiring. The second group refers to law that stakeholders may want to adhere to without having a regulatory obligation to do so. Laws that require compliance are those for which stakeholders can be held accountable if they do not comply with the framework. Whether one need to comply, adhere or can simply be inspired can depend on the different regulation, but within a regulation the particular clauses that require compliance may, also, vary in terms of levels of compliance anticipated.

Based on their nature, perspective and scope, the identified regulatory frameworks that are either already applicable or currently proposed could be grouped into different categories. In this respect, deliverable introduces two variables that help classifying the frameworks: the *direction* and the *perspective*. The direction could be horizontal, vertical, or a converged ecosystem. Horizontals focus on 'non-functionals' such as safety and security, that can reoccur as an issue across different sectors. Verticals, however, are market or sector specific. Driven by the increased complexity and pervasiveness of digital infrastructure and networks, the converged ecosystems, as a third category, is taken increasingly often as an approach. Applied to the AgriCapture pilots, this would mean that the 'farmer' can be a producer, and/or a consumer and/or a carbon capture provider. To



stay up to date, regulations will need to adapt to this reality of stakeholders taking different roles.

The figure below attempts to map the currently applicable regulations at EU level with the focus areas identified, namely networks, systems, data, applications and people. To this end, the mapping was based on the articles providing for the subject matter and scope under the respective regulations discussed. It should be made explicit that the focus area 'people' identified does not only cover end-users, but also people, in general, acting in their other capacities.

REGULATORY FRAMEWORKS IN THE TWINERGY ERA	PEOPLE	SYSTEMS	DATA	APPLICATION	NETWORK
General Data Protection Regulation	✓	✓	✓	✓	✓
Free Flow of Non-Personal Data Regulation	✓	✓	✓	✓	
Open (& Re-Use of) Data Directive, Data Governance Act* & Data Act*			✓	✓	
PSD2 & Regulatory Technical Standard	✓	✓	✓	✓	
ePrivacy Regulation *	✓	✓	✓	✓	✓
eIDAS Regulation *	✓	✓	✓	✓	✓
Cybersecurity Act	?	✓	✓	✓	✓
Digital Services Act *	?	✓	✓	✓	✓
Product Liability Directive *	✓	?	?	?	?
Contract Law, IPR Law & Tort Law	✓	✓	✓	✓	✓
NIS Directive 2.0 *		✓		Impact-Based?	✓

Figure 3: Applicable EU regulations and technology domain of interest³

1.4 Target audience

The present document is -primarily- addressed to AgriCapture pilot partners. Nevertheless, this document being a public deliverable it is not only addressed to the AgriCapture consortium and to the European Commission services, but it will be -also- made available to the wider public through the project's website. In a wider context, this deliverable is, thus, targeted towards a much broader audience, including farmers, meaning, to all those interested in promoting regenerative agriculture as well as to those interested in supporting the fight against climate change.

³ The (*) is added next to the title of regulations which are either under development or under update reviews, but either expected this year or in a few years from now.



1.5 Structure

This document is composed of nine (9) chapters. Following the current introductory Chapter 1, Chapter 2 focuses on the market-centric perspective, followed by Chapter 3 which focuses on sustainability. Chapter 4 addresses data-centric frameworks, while Chapter 5 expands on the economic perspective. Moreover, Chapter 6 elaborates on the human-centric regulations and Chapter 7 does so in relation to the system-centric perspective. Finally, Chapter 8 expands on an advanced way of designing systems in order to 'make them' work. Chapter 9 provides for the concluding remarks. This document, also, incorporates an Annex with an initial stakeholder analysis that preceded the work presented in the main body.



2 Market-Centric Perspective

Keeping in mind the stakeholders of AgriCapture, it is pertinent to stress the role of contract law, especially, in governing the Business to Business (B2B) relationships that are particularly relevant for AgriCapture. More specifically, in the context of AgriCapture, the nature of the contractual relationships will vary from situation to situation and would include contractual relationships that may only require minimal interaction, and which may last for a short period. On the other hand, AgriCapture may also involve complex multi-party contractual relationships that may span for several years. Either way, it is important to take cognizance of the contractual relationship in order to better understand how the existing regulations impact the stakeholders involved. In this spirit, the discussion below focuses on certain aspects of Intellectual Property and contract law.

2.1 Intellectual Property & Contract Law

Data collecting and analyses has become indispensable in modern agricultural businesses. It goes without saying that data sharing can bring great opportunities for further agricultural improvement and innovation and - if used in a fair, transparent and responsible way - also major improvement of the environment including the soil.

The main principles as it comes to any data, are control, access, use, transparency, management, accountability, dynamic assurance and affordable enforcement. Intellectual Property and Intellectual Property Rights (IP/IPR) are, together with state-of-the-art licensing and rights management through contract law, excellent means to organise and manage these principles, and at the same time indispensable drivers for sustainable economic growth. Other effective means are contractual and other measures that can be taken to protect trade secrets and confidentiality, and digital means to securely monitor and manage digital assets.

Attention needs to be given to the upstream side (companies, corporates and the like) and downstream side (individuals, society, taxpayers and the like) in order to create an ecosystem for controlled sharing, based on trust and what we call CADA: *Continuous Appropriate Dynamic Accountability*. CADA aims for achieving continuous improvement of the ecosystems, products, systems and services to ensure up-to-date levels of protection by requiring the levels of control, protection, management and accountability to continuously meet the respective appropriate levels. The GDPR has the exact same basis and requirements as set above (reference is made to the Articles 25 respectively 32 of the GDPR).

As in many other industries, in agriculture too, big corporates are fast to collect, combine and exploit data, related data, meta-data and the like. By controlling it, they manage to



increase their market dominance day by day, reducing competition and smothering innovation. The European Commissioner for the Internal Market, Thierry Breton, rightfully noted: 'About 80% of all the generated data in the world is in the hands of 4, 5, 6 international players. They have created a sort of monopoly based on their and our data.' Not only do they not share the data for the greater good, but what is worse, it is used to set off products that may at first produce more crop and bring more profit for farmers, but are detrimental to the soil and the environment on the longer run.

Another matter of continuous concern with similar detrimental effects on innovation and competition is the status of IP/IPR protection and enforcement in third countries. It is the watchlist of the Directorate General for Trade of the European Commission (DG Trade), and the EU Observatory on Infringements of Intellectual Property Rights (EUIPO). The main objective of the Commission's strategy here is to identify third countries in which the state of IPR protection and enforcement gives the highest level of concern, aiming to improve IPR protection and enforcement worldwide and enable holders of IPR, especially SME's, to better assess their risks and take appropriate actions when engaging in international business⁴.

As traditional IP/IPR systems did not keep up with these societal transformations of the digital revolution, the Commission adopted the Intellectual Property Action Plan (IPAP) in November 2020, as part of the new European Industrial Policy⁵. The IPAP aims amongst others to upgrade the existing IP system, promote its faster, smarter and more affordable use, ensure better enforcement & promote fair play globally for IP & IPR, enabling more growth and innovation, allocated more equally to a wider range of stakeholders, including SME's and start-ups.

The Commission also promotes industry dialogue to address the impact of new technologies (such as AI and block chain) on the IP system. To ensure that companies, including SME's, have access to fast, effective and affordable protection tools and reduce the persisting fragmentation and complexity in the current system, the Action Plan calls Member States for a rapid rollout of the unitary patent system to create a one-stop-shop for patent protection and enforcement across the EU. The Commission proposes measures to facilitate the sharing of critical IP in times of crisis, whilst ensuring return on investment. The Commission will also work on an improved copyright infrastructure, take action to better mobilise IP-protected data, and propose ways to improve transparency

⁴ European Commission (April 2021). Report on the protection and enforcement of intellectual property rights in third countries [working document]. Available at: https://trade.ec.europa.eu/doclib/docs/2021/april/tradoc_159553.pdf.

⁵ COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Making the most of the EU's innovative potential An intellectual property action plan to support the EU's recovery and resilience COM/2020/760 final. Available at: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52020DC0760>.



and predictability in the licensing of standard-essential patents (SEPs) as these are key element for the digital transformation of Europe's industry. While IP rights-intensive industries account for 93% of EU goods exports, EU businesses still face great challenges when operating in third countries. To address these challenges, the Commission aims to strengthen the EU's position as a global standard-setter in IP. It will also step up the EU response to unfair practices committed by third country players, such as industrial espionage or attempts to misappropriate IP in the context of R&D cooperation.

The AgriCapture Plan fits right into the goals of IPAP, but it will probably take too much time wait for the implementation of laws and regulations that have the envisaged effects. It is imperative to start enabling carbon sequestration and regenerative farming as soon as possible in an accessible and comprehensible manner. This can be done using codes of conduct, e.g. for agricultural data sharing, codes of engagement for stakeholders on e.g. data control/data management, and participation of stakeholders third countries, and continuous development of best practices, which can eventually – if required – be integrated into laws.

Note that when it comes to data, contractual arrangements may, also, play an essential role in determining how an individual's data is collected and processed by businesses and organisations. As will be discussed under section 6.1, EU data protection law allows for processing of data by an organisation if the said processing is being undertaken to perform a contract or to enter into a contract.⁶ On similar lines, contractual arrangements also provide a basis to share and transfer data with other individuals, businesses and organisations. Furthermore, section 4.4 touches upon certain Codes of Conduct (CoCs) that have been adopted in order to facilitate data sharing amongst signatories and provide guidance on contractual relations entered into pursuant to the said CoCs.

⁶ Regulation (EU) 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, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119. Available at: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.



3 Sustainability Perspective

Sustainability has been high on the agenda of the European Union for several years and the EU has been a front-runner in this regard. The European Commission underscored this with its announcement of a European Green Deal as one of its main priorities for the period 2019-2024. The EU Green Deal aims at turning climate and environmental challenges into opportunities across all policy areas and making the transition just and inclusive for all. Moreover, it aims to boost the efficient use of resources by moving to a clean, circular economy. More relevant for AgriCapture, the Green Deal aims at working with Member States to ensure that their respective national strategic plans support sustainable practices, such as precision agriculture, organic farming, agro-ecology, agro-forestry and the like. As per the Green Deal, shifting the focus from compliance to performance, measures such as eco-schemes should reward farmers for improved environmental and climate performance, including managing and storing carbon in the soil, and improved nutrient management to improve water quality and reduce emissions.⁷

Commissioner for the Environment, Oceans and Fisheries Virginijus Sinkevičius said:

"A quarter of our planet's biodiversity is present in soil. This is literally a treasure under our feet, and our food and our future depend on it. We must equip the European Union with a robust soil policy that will allow us to reach our ambitious climate, biodiversity and food security goals, and step up our efforts to manage soil in a way that it can deliver for people, biodiversity and climate."

When it comes to soil, land degradation - one of the key targets of the UN Social Development Goals, is a serious global problem. It is often caused by a combination of factors such as poor land management, unsustainable agricultural practices, pollution and deforestation. It can contribute to natural disasters such as flooding, bushfires, hurricanes, and have serious impact on climate change and social consequences such as poverty and mass migration.

Regenerative farming through improved agricultural practices enables carbon to be stored in plant biomass and soils (Soil Carbon Sequestration), whilst restoring and revitalising the soil and wider environment. Regenerative farming thus holds a major potential to reduce the detrimental impact on climate change. It is estimated that soils can sequester around 20 Pg C in 25 years, more than 10 % of the anthropogenic emissions.⁸

⁷ Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, The European Green Deal, COM/2019/640 final. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1576150542719&uri=COM%3A2019%3A640%3AFIN>.

⁸ FAO (no date). What is Soil Carbon Sequestration? [online resource] Available at: <http://www.fao.org/soils-portal/soil-management/soil-carbon-sequestration/en/>.



As Carbon sequestration requires an international approach, it has been supported under 3 UN Conventions (UNFCCC, UNCCD and UNCBD), the Kyoto Protocol (Clean Development Mechanism⁹) and the European Commission also aims to improve - besides carbon sequestration - biodiversity, healthy soils, crop and environmental quality, prevention of land erosion and other important sustainability benefits.

As part of the EU Biodiversity Strategy for 2030 ('Bringing nature back into our lives')¹⁰ the Commission aims, amongst many other sustainable initiatives, to help farmers to shift to regenerative farming practices in such a manner that their business will be competitive, e.g. through trade and industry policies, international biodiversity coalitions and neighborhood and community policies.

Part of the Biodiversity strategy is the development of methods, criteria, standards and tools to describe essential biodiversity features, values and use and measure the environmental footprint of products and organisations and the establishment of an international natural capital accounting initiative. Setting up a neutral, trusted system for measuring and collecting soil carbon sequestration data, can enable farmers to be financially rewarded for good sequestration results and thus support the transition to regenerative farming.

One of the initiatives worth mentioning are the LUCAS (Land Use Cover Area Frame Survey) Topsoil surveys¹¹ that are being held by Eurostat every 3 years in 28 member states, covering land use, land cover, soil biodiversity and bulk density. The statistics can be used to analyse and contribute to several EU policy areas on soil, biodiversity, climate, agriculture¹², nature conservation but also land monitoring, spatial planning and resource management as carried out by the Copernicus earth observation program¹³.

Another is the 'Mission in the area of Soil Health and Food'¹⁴, together with the agricultural European Innovation Partnership (EIP AGRI), promoting the wide-spread uptake of practices for pesticide and nutrient reduction by promoting innovations and exchange of

⁹ UNFCCC. Clean Development Mechanism (CDM). Available at: <https://cdm.unfccc.int/>. Focus was first on afforestation and reforestation, in post Kyoto negotiations rangelands are added due to huge carbon sequestration potentials.

¹⁰ COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS EU Biodiversity Strategy for 2030 Bringing nature back into our lives COM/2020/380 final. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0380>.

¹¹ Eurostat (no date). LUCAS – Land use and land cover survey[online resource] . Available at: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=LUCAS_-_Land_use_and_land_cover_survey.

¹² On agriculture, relevant is the CAP (Common Agricultural Policy) program: https://ec.europa.eu/info/food-farming-fisheries/key-policies/common-agricultural-policy/cap-glance_en.

¹³ See for instance: <https://www.copernicus.eu/en/use-cases/farm-sustainability-tool-fast-space-data-sustainable-farming>.

¹⁴ European Commission (2020). Mission area: Soil health and food [online resource]. Available at: https://ec.europa.eu/info/research-and-innovation/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe/missions-horizon-europe/soil-health-and-food_en.



knowledge, while also supporting the Global Soil Partnership to prevent further pollution and reduce the legacy pollution risks in soils. Its objective on reducing soil pollution and enhancing restoration is at least 75% of EU soils to be healthy for food, people, nature and climate by 2030¹⁵.

Many of the regenerative initiatives related to farmland face impediments, from the ongoing reluctance of the financial services industry to finance regenerative farming, impediments in farmers contracts regarding the lease of land or machines and related software¹⁶, to the ever increasing influence of large corporates such as Monsanto and Google controlling commercial data collections linked to related sponsored services and products for crop or livestock improvement, generally preferring the short-term interests of shareholders over long term effects on the environment. Many of the current carbon related initiatives, such as carbon banks, trade in carbon credits, and ongoing discussions about true value and true pricing, are mainly driven by large enterprises and the financial services industry that use carbon emissions trading for purposes that often have very little to do with decreasing CO₂ emissions. This will not work.

Most farmers cannot afford to make the switch all by themselves. It is therefore imperative for AgriCapture, that farmers are convincingly enabled to make a living while practicing sequestration and regenerative farming. In order to make a truly accessible system for SME's and farmers, an independent trusted framework is required, built on knowledge sharing, transparency, and good governance principles. The framework should provide a sustainable system with measurable credits for farmers who practice sequestration and regenerative farming, in order to provide them with a healthy revenue model, enabling them to remain independent of restrictive contractual clauses, dominant market players and/or conservative financiers, and to compete internationally with farmers who do not (yet) practice sequestration and regenerative farming.

4 Data-centric perspective

Data plays an essential role in economic growth, innovation, competitiveness and creating benefits for society as a whole. Keeping that in mind, the EU has taken great strides to ensure that governmental agencies, organisations and individuals are able to leverage the potential of data in a sustainable and holistic manner. Several European leaders have also

¹⁵ Directorate-General for Research and Innovation (European Commission) (September 2020). Caring for Soil is Caring for Life [publication]. Available at: <https://op.europa.eu/en/publication-detail/-/publication/4ebd2586-fc85-11ea-b44f-01aa75ed71a1/language-en/format-PDF/source-search>.

¹⁶ e.g. impediments on sharing or re-using collected data, financial impediments related to crop or livestock returns, restrictions as to the use of land.



reiterated the need to ensure that European data is used for European countries in order to create value in Europe.

In February 2020, the EU also published its communication on “A European Strategy for Data” which aims at making the EU a leader in a data-driven society. The Strategy is expected to create a single market for data where data flows across the various sectors in the EU and where the rules for access and use of data are fair, practical and clear. More relevant for AgriCapture is the proposal under the Strategy to create a Common European agriculture data space so as to enhance the sustainability performance and competitiveness of the agricultural sector.¹⁷ As per the Strategy, a common data space for agricultural data based on existing approaches towards data sharing could result in the creation of a neutral platform for sharing and pooling agricultural data, including both private and public data.¹⁸

4.1 The Free Flow of Non-Personal Data Regulation

The free flow of data is the “fifth freedom” within the European Union, among the free movement of goods, services, persons and capital. The Regulation on the Free Flow of Non-Personal Data is applicable since 28 May 2019 and aims at fostering the data economy by facilitating the exchange and storage of electronic, non-personal data across EU borders by removing certain obstacles to the free movement. The overarching objective is to facilitate and encourage businesses to share data and thereby potentially improve and extend their business services as well as the exchange of data in the market in general.¹⁹ Thereby, the framework also aims at mitigating the risk for a ‘vendor lock-in’: the situation where a user is stuck with a digital service provider because it is unable to avoid moving its data from one provider to another.

The Regulation applies to processing of electronic data, other than personal data, within the EU zone, thereby complementing the GDPR. Whereas in 2018, the GDPR has provided for measures to avoid this from happening with regards to personal data, the Regulation on the Free Flow of Non-Personal Data promotes portability of non-personal data.²⁰ In addition to data exchanged or stored within the EU, the Regulation is also applicable when

¹⁷ European Commission (2020). Open Public Consultation on the European Strategy for Data, Summary Report on the open public consultation on the European strategy for data [public consultation]. Available at: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=68611.

¹⁸ European Commission (2020). Open Public Consultation on the European Strategy for Data, Summary Report on the open public consultation on the European strategy for data [public consultation]. Available at: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=68611.

¹⁹ European Commission (8 July 2019). Regulation on the free flow of non-personal data [publication]. Available at: https://knowledge4policy.ec.europa.eu/publication/regulation-free-flow-non-personal-data_en.

²⁰ 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. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1807>.



the users of the service are located in the EU, or when the services are carried out by an entity in the EU.²¹

Following from what is discussed previously, the Regulation will first and foremost foster the exchange of non-personal data among different stakeholder involved with the collection, analysis and further processing of personal data, within and across different regions in the EU. This will be relevant in the context of AgriCapture, in which it may be desirable to share knowledge and insights among different farms in order to strengthen the business case and measure impact. Furthermore, the Regulation facilitates businesses to switch of cloud service providers without losing their data. Under the framework, the Commission stimulates providers to write codes of conducts that allow users to transfer data between cloud providers or local IT environments.²² This could be relevant for storage and further processing of soil and satellite data in the context of AgriCapture. Moreover, With the introduction of this Regulation, data localisation requirements are prohibited, unless they serve public security objectives.²³ Finally, the Regulation ensures that security requirements following from the cybersecurity package that apply to processing of data by businesses within the EU, will apply likewise to processing data across EU borders or in the cloud.²⁴

4.2 The Data Governance Act

Digital technologies have transformed the economy and society in the last few years and data has played a pivotal role in this transformation. As touched upon in the introduction of this section, the European Commission published the European Strategy for Data where it reiterated the importance of data for economic growth, competitiveness, job creation, innovation etc. In response to a public consultation that was conducted on the Strategy, the first deliverable i.e. a proposal for new rules on data governance (DGA) was published in November 2020.²⁵ The public consultation which had received contributions from almost 806 respondents revealed that 97.2% of the said respondents confirmed the need for an overarching data strategy to enable the digital transformation of society, and 91.5% agreed that 'More data should be available for the common good, for example for

²¹ Framework for the free flow of non-personal data in the European Union, art. 2.

²² Framework for the free flow of non-personal data in the European Union, art. 6(2).

²³ Framework for the free flow of non-personal data in the European Union, art. 4.

²⁴ European Commission (8 July 2019). Regulation on the free flow of non-personal data [publication]. Available at: https://knowledge4policy.ec.europa.eu/publication/regulation-free-flow-non-personal-data_en.

²⁵ Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act) COM/2020/767 final. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767>.



improving mobility, delivering personalised medicine, reducing energy consumption and making our society greener.²⁶

The DGA aims at tackling of the issue of low availability of data for research and innovative uses resulting from transaction costs that prevent seamless data exchange between organisations.²⁷ It also aims at diving into the issue of insufficient resourcing in public sector organisations when it comes to ascertaining requests for use of data that is in principle not accessible and the use of which is subject to the respect of rights of others (personal data, copyrighted material, commercially confidential information).²⁸ Moreover, given that the amount of data generated by public bodies, businesses and citizens is expected to multiply by five times between 2018 and 2025, the DGA aims at creating European data spaces for the benefit of society, citizens and companies. The DGA also proposes measures to increase trust in data sharing.

At the very outset, the DGA clarifies that it does not create any obligation on public sector bodies to facilitate the re-use of data nor do they release them from their confidentiality obligations.²⁹ Moreover, the DGA also prohibits agreements and other practices that grant exclusive rights to certain categories of data held by public sector bodies or which restrict the availability of data re-use by other organisations.³⁰ Public sectors bodies that are competent under national law to allow or refuse access for the re-use of one or more of the categories of their data are required to publicly make available the conditions for allowing such re-use, however, such conditions must be non-discriminatory, proportionate and objectively justified with regard to categories of data and purposes of re-use and the nature of the data for which re-use is allowed.³¹ These conditions shall also not be used to restrict competition. In the same context, for allowing re-use of data, public sector bodies are entitled to charge a fee as long as the fee is non-discriminatory, proportionate and objectively justified.³²

Interestingly, the DGA also introduces the concept of “data altruism” which the Regulation defines as consent by data subjects to process personal data pertaining to them, or permissions of other data holders to allow the use of their non-personal data without

²⁶ European Commission (2020). Open Public Consultation on the European Strategy for Data, Summary Report on the open public consultation on the European strategy for data [public consultation]. Available at: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=68611.

²⁷ European Commission (2020). Inception Impact Assessment, Legislative framework for the governance of common European data spaces [impact assessment]. Available at: [https://eur-lex.europa.eu/legal-content/EN/TXT/DOC/?uri=PI_COM:Ares\(2020\)3480073&from=EN](https://eur-lex.europa.eu/legal-content/EN/TXT/DOC/?uri=PI_COM:Ares(2020)3480073&from=EN).

²⁸ European Commission (2020). Inception Impact Assessment, Legislative framework for the governance of common European data spaces [impact assessment]. Available at: [https://eur-lex.europa.eu/legal-content/EN/TXT/DOC/?uri=PI_COM:Ares\(2020\)3480073&from=EN](https://eur-lex.europa.eu/legal-content/EN/TXT/DOC/?uri=PI_COM:Ares(2020)3480073&from=EN).

²⁹ Proposal for Data Governance Act, art 3.

³⁰ Proposal for Data Governance Act, art 4.

³¹ Proposal for Data Governance Act, art 5.

³² Proposal for Data Governance Act, art 5.



seeking a reward, for purposes of general interest, such as scientific research purposes or improving public services.³³ Chapter IV of the DGS deals with data altruism and sets out certain general requirements for an organisation to be registered as a data altruism organisation. On a different note, the DGA also emphasizes on the key role of providers of data sharing services, which act as data intermediaries, in the data economy. As per the DGA, data intermediaries which offer services that can connect the different actors have the potential to contribute to the efficient pooling of data as well as to the facilitation of bilateral data sharing.³⁴ The DGA also lays down the conditions for providing data sharing services such as putting in place procedures to prevent fraudulent practice in relation to access of data, taking adequate technical, organisational and legal measures to prevent transfer or access to non-personal data that is unlawful and a high level of security for the storage and transmission of non-personal data.³⁵

4.3 Trade Secrets Directive

Advanced solutions, including such as those being created by AgriCapture, often rely on detailed innovations and technological advances which can be legally protected via a variety of intellectual property rights, such as patents or trade secrets. This aspect is critical because an organisation's intellectual property gives it a competitive advantage in the market and are also a source of steady revenue. In the EU, trade secrets are governed by the Trade Secrets Directive (TSD) which was adopted in June 2016 with the objective of standardizing national laws in EU countries in relation to unlawful acquisition, disclosure and use of trade secrets.

The TSD acknowledges the need for incentives for Europe's businesses to invest in innovation by offering a unified level of protection for acquiring, developing and applying know-how and information which is the currency of the knowledge economy and provides a competitive advantage.³⁶ Therefore, to reduce fragmentation among Member States, the TSD harmonises the definition of trade secret in line with existing internationally binding standards and provides useful common definition for its application. Under the TSD, in order to be granted protection, information is considered a 'trade secret' if (1) it is secret, i.e. not generally known or readily accessible to people in a wider community than the ones who typically deal with that information, (2) it has an actual or potential commercial

³³ Proposal for Data Governance Act, art 2(10).

³⁴ Proposal for Data Governance Act, recital 22.

³⁵ Proposal for Data Governance Act, art 11.

³⁶ Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure OJ L 157 (Trade Secrets Directive), recital 1. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0943>.



value because it is secret, and (3) it has been subject to reasonable steps under the circumstances to keep it secret.³⁷

The TSD requires Member States to ensure that trade secret holders are entitled to apply for the measures, procedures and remedies provided for to prevent or obtain redress for the unlawful acquisition, use or disclosure of their trade secret.³⁸ Moreover, during legal proceedings relating to the unlawful acquisition, use or disclosure of a trade secret, Member States are required to ensure that the parties, their lawyers, court officials and other parties involved do not disclose the trade secret.³⁹ This obligation remains in force even after the legal meetings have ended except under certain exceptional circumstances as listed in the TSD.⁴⁰

TSD provides for a wide range of remedies to enforce trade secret rights against infringers, while ensuring proportionality between the violation and the sanction.⁴¹ Remedies under the TSD include provisional and precautionary measure, wherein judicial authorities order the cessation or prohibition of the use or disclosure of the trade secret on a provisional basis by the alleged infringer or to order the seizure of suspected infringing goods, including imported goods, so as to prevent their entry into, or circulation on, the market.⁴² The TSD also provides for final injunctions as well as corrective measures.⁴³

4.4 Other relevant instruments

Besides the legislations discussed above, there are several other methods/instruments that have been implemented at different levels to facilitate data transfers in a structured, transparent and seamless manner. In the AgriCapture architecture, data is the foundation that can catapult the project to achieve its envisioned objectives, hence, some of the takeaways and suggestions mentioned in the instruments below could be beneficial for AgriCapture as well.

The United Nation's Global Partnership for Sustainable Development Data is a global network of almost 300 partners that working towards ensuring that opportunities and avenues presented by the data revolution are used to achieve the Sustainable Development Goals.⁴⁴ More pertinent to AgriCapture, the organization launched the tool Africa Regional Data cube which assisted governments in Ghana, Kenya and other countries to access earth observation data and satellite imagery analysis. Similarly, the

³⁷ Trade Secrets Directive, art 2 (1).

³⁸ Trade Secrets Directive, art 4.

³⁹ Trade Secrets Directive, art 9 (1).

⁴⁰ Trade Secrets Directive, art 9 (1).

⁴¹ Trade Secrets Directive, art 7.

⁴² Trade Secrets Directive, art 10.

⁴³ Trade Secrets Directive, art 12.

⁴⁴ Global Partnership for Sustainable Development Data (no date). Better data [online resource]. Better decisions. Better Lives. Available at: <https://www.data4sdgs.org/>.



organization also helped the Government of Senegal to use satellite data to allocate drought-resistant crops to farmers thereby improving the effectiveness of their climate adaptation policy.⁴⁵ From time to time, the organization also publishes resources which include use cases that may be useful for AgriCapture.⁴⁶

The Code of Conduct on Agricultural Data Sharing (CoC) is another relevant instrument that was published in 2018 to provide guidance on contractual relations and governance when re-using and sharing agricultural data.⁴⁷ The CoC lays out principles pertaining to 5 overarching categories:

- 1) Attribution of the underlying rights to derive data (Also referenced as data ownership);
- 2) Data access, control and portability;
- 3) Data protection and transparency
- 4) Privacy and security; and
- 5) Liability and intellectual property right.

In addition to providing cases studies, the Annexes of the CoC provide a contract checklist that highlights some of the main legal principles that need to be accounted for in order to give a well-balanced contract.

The Farm Data Code published in Australia was adopted with a similar intention and to enable farmers to have confidence in how their data is being collected, processed and shared.⁴⁸ The code requires commitment to certain fundamental principles such as:

- Transparent, clear and honest collection, use and sharing of farm data.
- Fair and equitable use of farm data.
- Ability to control and access Farm Data.
- Documentation and Record Keeping.
- Portability of Farm Data.
- Keeping Farm Data Secure.

⁴⁵ Global Partnership for Sustainable Development Data (no date). Our Impact [online resource]. Available at: <https://www.data4sdgs.org/about-gpsdd/our-impact>.

⁴⁶ Global Partnership for Sustainable Development Data (no date). Resources [online resource]. Available at: <https://www.data4sdgs.org/resource-listing>.

⁴⁷ EU Code of conduct on agricultural data sharing by contractual agreement. Available at: http://fefac.eu/wp-content/uploads/2020/07/EU_COD1.pdf.

⁴⁸ Farm Data Code, National Farmers Federation. Available at: <https://nff.org.au/programs/australian-farm-data-code/>.



- Compliance with National and International Laws.

To ensure the continuous effectiveness of the Code, it is expected to be subject to two 6-monthly reviews. Another similar example is of the Farm Data Code of Practice published in New Zealand that also provides a baseline to ensure that farmers are able to trust organizations that hold, manage and move their data. ⁴⁹

5 Economic Perspective

Sustainable finance has gained traction in the last few years and refers to the process of taking into account environmental, social and governance (ESG) considerations when making any form of investments in the financial sector which ultimately result in more long-term investments in sustainable economic activities and projects.⁵⁰ Sustainable finance plays a crucial part in translating the policy objectives under the European Green Deal into tangible results and to also meet the EU's international commitments on sustainability and climate. The recently applicable Sustainable Finance Disclosure Regulation (SFDR), which recently became applicable in March 2021, was enacted in the same spirit with the objective of encourage responsible and sustainable investments, triggering changes in behavioral patterns in the financial sector and discouraging greenwashing.⁵¹ Complementing the objectives of the SFDR is the European Commission's proposal for a Corporate Sustainability Reporting Directive (CSRD), which aims to ensure companies provide consistent and comparable sustainability information.

5.2 Revised Payment Services Directive

Prior to enacting the Revised Payment Services Directive (PSD2), EU lawmakers acknowledged that solutions developed by third party organisations fell outside the scope of existing payment regulations which subsequently resulted in the environment of card payments and new means of payments (such as internet and mobile payments) becoming fragmented, inconsistent and under-regulated.⁵² The enactment of the revised Payment Services Directive, at a time when the payments industry was booming, helped address

⁴⁹ New Zealand Farm Data Code of Practice. Available at: <https://www.farmdatacode.org.nz/>.

⁵⁰ European Commission, Overview of sustainable finance, available at: https://ec.europa.eu/info/business-economy-euro/banking-and-finance/sustainable-finance/overview-sustainable-finance_en.

⁵¹ Regulation (EU) 2019/2088 of the European Parliament and of the Council of 27 November 2019 on sustainability - related disclosures in the financial services sector OJ L 317/1. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019R2088>.

⁵² European Commission (24 July 2013). Impact Assessment accompanying the document Proposal for a directive of the European parliament and of the Council on payment services in the internal market and amending Directive 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC and Proposal for a Regulation of the European Parliament and of the Council on interchange fees for card-based payment transactions [Commission Staff Working Document]. Available at: https://eur-lex.europa.eu/resource.html?uri=cellar:906ed6d3-f509-11e2-a22e-01aa75ed71a1.0001.04/DOC_1&format=PDF.



these challenges and to make electronic payments safer, cost-effective and more innovative.

The PSD2 opened the EU payments market to third party service providers (TPPs) by allowing them to gain access to information about payment accounts provided that the organisation has been granted authorisation as a payment institution under the Directive. TPPs discussed under the PSD2 include Payment initiation service providers (PISPs) and Account information service providers (AISPs). While both PISPs and AISPs constitute TPPs, their roles differ. In a typical transaction, a person making a payment not only shares their security credentials with the bank but also their data which is transmitted through one or more third party software providers that provide the “bridging” interface through which the payer is able to access his/her online account and to then transmit the payment. In this case, the PISP acts as a “facilitator” enabling transfer of funds by populating the transaction details and subsequently verifying that the customer has adequate funds in their account to complete the transaction. AISPs on the other hand act as an “aggregator” by providing the payer with aggregated online information on one or more payment accounts held with one or more other payment service providers and accessed via online interfaces of the account servicing payment service provider.⁵³ Therefore, by bring new players within its scope and creating a framework for all the relevant stakeholders in the payments ecosystem in line with the risk that they introduce, the PSD2 strikes a good balance between the stakeholders involved, as illustrated in the figure below.

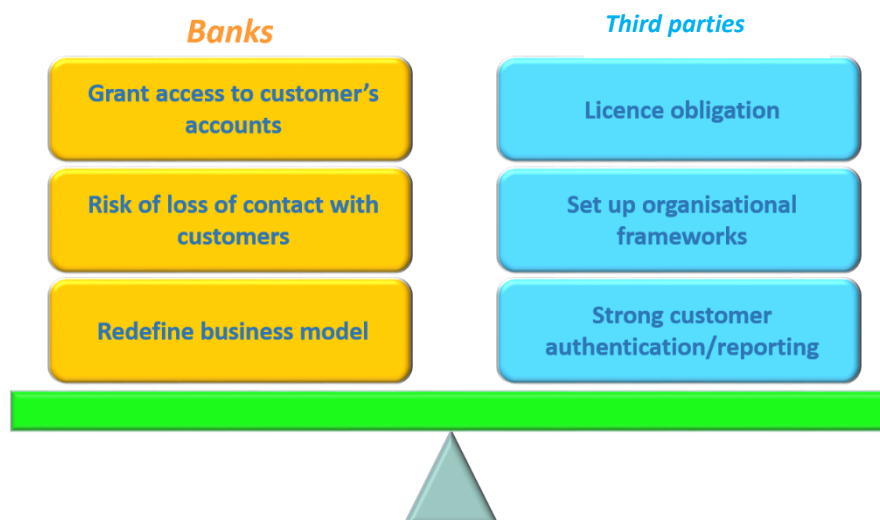


Figure 4: PSD2 – A new level playing field for the financial services industry and third-party organisations

⁵³ Revised Payment Services Directive, recital 28.



The PSD 2 imposed measures to manage operation and security risks. Under the PSD 2, payment service providers are required to prove that they have implemented security measures to ensure that payments are secure and safe. In addition, they are also required to establish and maintain effective incident management procedures including detection and classification of major operational and security incidents.⁵⁴ In the event of a major incident, payment service providers are required to notify competent authority in the home Member State of the payment service provider without any undue delay.⁵⁵

In particular, as a general rule the PSD 2 requires payment service providers to implement strong customer authentication (SCA) where the payer accesses its payments account online, initiates an electronic payment transaction or carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.⁵⁶ In September 2019, the SCA officially went into effect with the aim to reduce instances relating to fraud and to make online payments more secure. SCA requires proper identification or authentication to be undertaken for instances where payments exceed €30 and takes place via an authentication process based on two specific factors supplied by the user, e.g., a password, PIN code, a mobile phone or a fingerprint.

6 Human-Centric Perspective

The Treaty of Lisbon, which along with the Treaty on European Union constitute the Treaties on which the Union is founded, mandates shared competence between the Union and the Member States in certain areas including agriculture. More pertinent to AgriCapture, the Treaty of Lisbon requires the EU to define a common agricultural policy with the objective of enhancing agricultural productivity by encouraging technical progress and by ensuring the rational development of agricultural production and the optimum utilisation of the factors of production, in particular labour.⁵⁷ To safeguard and strengthen the position of farmers in the supply chain, the EU has implemented a legislation that bans 16 unfair trading practices that have been putting farmers at a disadvantage.⁵⁸

6.1 General Data Protection Regulation

The General Data Protection Regulation (GDPR) is a watershed regulation that was implemented to address fragmentation and inconsistencies resulting its predecessor, the

⁵⁴ Revised Payment Services Directive, art 95.

⁵⁵ Revised Payment Services Directive, art 96.

⁵⁶ Revised Payment Services Directive, art 97.

⁵⁷ Consolidated version of the Treaty on the Functioning of the European Union OJ C 326, 26.10.2012, art 39. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT>.

⁵⁸ Directive (EU) 2019/633 of the European Parliament and of the Council of 17 April 2019 on unfair trading practices in business-to-business relationships in the agricultural and food supply chain OJ L111/59. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019L0633>.



Data Protection Directive.⁵⁹ The GDPR pertains to processing of personal data at EU level and is horizontally applicable across all EU Member States. The GDPR, which came into force in May 2018, has empowered citizens in the EU to be in more control of what happens with their data in today's digital age and to enforce new rights provided to them.

In terms of scope, the GDPR applies to processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.⁶⁰ The GDPR has extra-territorial scope meaning that it not only applies to organisation established in the EU but also organisations outside the EU where the processing activities of the said organisation are related to offering of goods and services to individuals in the EU or the monitoring of their behaviour as far as their behaviour takes place within the Union.⁶¹ The individuals whose data is being processed under the GDPR are referred to as "data subjects" under the Regulation. The definition of 'personal data' is rather broad and is defined under the GDPR as *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, in particular by reference 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, psychological, genetic, mental, economic, cultural or social identity of that natural person.*⁶²

The GDPR also carves out certain roles which translate into a certain level of legal responsibilities for each role. A 'controller' is defined as *the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.*⁶³ There GDPR also caters for instances where there are two or more controllers that jointly determine the purposes and means of processing in which case they will be joint controllers.⁶⁴ In the same context, a 'processor' is *a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.*⁶⁵

⁵⁹ Regulation (EU) 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, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119, art 6(b). Available at: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.

⁶⁰ General Data Protection Regulation, art 2.

⁶¹ General Data Protection Regulation, art 3.

⁶² General Data Protection Regulation, art 4(1).

⁶³ General Data Protection Regulation, art 4(7).

⁶⁴ General Data Protection Regulation, art 26.

⁶⁵ General Data Protection Regulation, art 4(8).



One of the most important aspects under the GDPR is the lawfulness of processing wherein processing is only permissible in the following instances:

- a) The data subject has given specific and unambiguous **consent** to the processing of his or her personal data.
- b) Processing is necessary for the **performance of a contract** or to enter into a contract to which the data subject is a party.
- c) Processing is necessary for **compliance with a legal obligation** to which the controller is subject.
- d) Processing is necessary in order **to protect the vital interests** of the data subject or of another natural person.
- e) Processing is necessary for the **performance of a task carried out in the public interest** or in the exercise of official authority vested in the controller.
- f) Processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party.⁶⁶

The risk-based approach taken in the GDPR gives organisations room to approach security in line with the dynamics of their organisation and to implement technical and organisational measures accordingly. The GDPR does, however, provide for some parameters that organisations that can take into account when implementing technical and organisational measures such as the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.⁶⁷ The GDPR also recommends pseudonymisation and encryption of personal data for ensuring security of processing. The GDPR vests the data subjects with certain rights including the right of access to their personal data, the right to be forgotten, right to rectification and the right to object to processing of personal data for certain purposes. In certain circumstances, organisations may also have to conduct a data protection impact assessment (DPIA) in the event the processing is likely to result in a high risk to an individual's rights.⁶⁸ The process may also require pre-consultation with the relevant supervisory authority.

6.2 Regulation on electronic identification and trust services for electronic transactions

The implementation of the Regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS) is one of the first and most modern legal frameworks for cross-border electronic identification and authentication in the EU.

⁶⁶ General Data Protection Regulation, art 6.

⁶⁷ General Data Protection Regulation, art 32.

⁶⁸ General Data Protection Regulation, art 35.



The Regulation, in force since September 2018, creates a harmonized framework allowing people and businesses of a Member State to make use of their national electronic identification schemes (eIDs) to gain access to public services of other Member States where eIDs is available. The eIDAS Regulation also creates an internal market for trust services which will be discussed further in this section. The significance of the eIDAS was further highlighted during the COVID-19 pandemic wherein more and more governments and organisations move their services and operations online.

The Regulation also aims at establishing a framework for the use for electronic Trust Services (eTS) namely electronic signatures, website authentication, electronic seals, time stamps etc., thereby giving them the same legal status to processes that may be paper based. To enable their cross-border use, the eIDAS suggests that national law should define the legal effect of the said trust services. Similar to the GDPR, the eIDAS requires providers of trust services to take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide.⁶⁹ On similar lines, electronic identification offers several benefits to organisations by allowing them to verify the identity of their customers and other businesses in order to establish contractual relationships with them in a quick, efficient and secure manner. By providing such methods of identification, the eIDAS also enables organisations to grow their clientele.

In July 2020, a public consultation was launched by the European Commission to identify the drivers and barriers to the uptake of electronic identification and trust services for electronic transactions in the EU. The Inception Impact Assessment (IIA) deliverable of eIDAS highlighted various problem areas that needed to be tackled. For instance, when the IIA deliverable was published, only 15 of 27 Member States were offering cross-border electronic ID under eIDAS to their citizens.⁷⁰ Moreover, due to the fact that the eIDAS only “encourages” Member States to make eIDs available to the private sector including for online banking or online shopping, very few Member States have implemented this possibility.⁷¹

Building on the eIDAS Regulation, the European Commission recently proposed a framework for a European Digital Identity for the benefit of EU citizens, residents and businesses in the EU. Once adopted, EU citizen will be able to easily access services using their European Digital Identity without having to use private identification methods or

⁶⁹ eIDAS Regulation, art 19.

⁷⁰ European Commission (2020). Inception Impact Assessment, Revision of the eIDAS Regulation – European Digital Identity (EUid) [impact assessment]. Available at: <https://www.gleif.org/content/1-about/8-gleif-engagement/2-consultation-responses/inception-impact-assessment.pdf>.

⁷¹ European Commission (2020). Inception Impact Assessment, Revision of the eIDAS Regulation – European Digital Identity (EUid) [impact assessment]. Available at: <https://www.gleif.org/content/1-about/8-gleif-engagement/2-consultation-responses/inception-impact-assessment.pdf>.



unnecessarily sharing personal data. The proposal is also expected to boost competitiveness in the EU by making it easier and seamless for businesses to verify the identity of citizens. The use of the European Digital Identity is voluntary, and the proposal aims at empowering people by allowing them to choose which aspects of their identity and data they wish to share with third parties. To expedite the process, the European Commission has provided a set of recommendations along with the proposal for the framework for a European Digital Identity and will also work in tandem with Member States to agree on the way forward.

7 System-Centric Perspective

Digital technologies and digitisation have transformed everyday life, how organisations do business and also how governments interact with their citizens. While these technologies have brought with them substantial benefits in different domains, they have also presented concomitant risks. While several regulations have been implemented/proposed to safeguard individuals from damage resulting from the use of such technologies or from misuse of data by such technologies there is also a need for regulations that look at the lifecycle of such technologies. Manufacturers of digital technologies need to move away from the “Sell Now, Fix Later” approach and ensure that different aspects such as privacy, security, safety, cyber resilience, transparency and accountability are taken into account right from the design phase of such technologies. This section touches upon proposed and existing EU laws that aim at doing so by ensuring that manufacturers ensure that their technologies meet certain standards before being placed on the market and lays down responsibilities that continue even after the technologies have been put in use individuals or organisations.

7.1 The Artificial Intelligence Act

On April 21st, 2021, the European Commission published the proposal for a Regulation laying down harmonized rules on artificial intelligence (‘Artificial Intelligence Act’).⁷² It is intended that the proposed Regulation forms the first legal framework in the EU regulating the use of AI following a proportionate, risk-based approach.⁷³ Overall, the Artificial Intelligence Act aims at strengthening the uptake of AI in Europe, by building trust in AI systems addressing ‘human and societal risks associated with specific uses of AI’.⁷⁴

⁷² Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts COM/2021/206 final. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206>.

⁷³ Proposal for the Artificial Intelligence Act, Explanatory Memorandum, under 1.1.

⁷⁴ Speech by Executive Vice-President Vestager at the press conference on fostering a European approach to Artificial Intelligence, Brussels, 21 April 2021 [transcript], available at: https://ec.europa.eu/commission/presscorner/detail/en/speech_21_1866.



Under the Regulation, *Artificial Intelligence* is defined as:

- *Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;*
- *Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems;*
- *Statistical approaches, Bayesian estimation, search and optimization methods.*⁷⁵

The Artificial Intelligence Act does not regulate AI technology per se, but, instead, it provides for what AI is used for and how it is used. As mentioned earlier, the Artificial Intelligence Act is a risk-based regulation; the higher the risk that the use of AI may involve, the stricter it is regulated. To this end, the uses of AI systems are classified in four categories: low or minimal risk, limited risk, high risk, and unacceptable risk uses (Figure 3).⁷⁶ The qualifications of each risk level as well as the obligations that follow from this classification will be discussed in the next section.

Four risk levels of AI



Figure 5: The four risk levels of AI as indicated by the proposed Artificial Intelligence Act.

Low or minimal risk uses

It is expected that the majority of AI systems such as, for instance, email spam filters or AI in video games, entails minimal to no risk.⁷⁷ According to Article 1 of the proposed Artificial Intelligence Act, low or minimal risk uses are outside of its scope.⁷⁸ The

⁷⁵ Proposal for the Artificial Intelligence Act, Annex I.

⁷⁶ Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence, Brussels, 21 April 2021 [press release], available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1682.

⁷⁷ Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence, Brussels, 21 April 2021 [press release], available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1682.

⁷⁸ Proposal for the Artificial Intelligence Act, art. 1.



Regulation therefore allows the use of such applications, without any restrictions. Nevertheless, the use of such applications will, certainly, remain to be regulated on the basis of other already applicable regulations.

Limited risk uses

The second category consists of AI uses that are intended to interact with people, such as chatbots or self-checkout services in shops.⁷⁹ Furthermore, other applications that are considered 'limited risk' include emotion recognition systems, biometric categorisation systems and AI used for media content manipulation, such as image, audio or video.⁸⁰ Based on the rationale that users should be aware that they are interacting with a machine, these limited risk uses are subject to transparency obligations.⁸¹

High-risk uses

As Vestager points out, high-risk uses, that is, uses that 'interfere with important aspects of our lives', are the main focus of the Artificial Intelligence Act.⁸² The European Commission has drafted a list of such uses in Annex III of the proposal, which serves as a reference for indicating high-risk. Prioritisation in access to jobs, education or eligibility for public assistance benefits and services form examples of such high-risk AI systems. Other examples include systems deciding on the creditworthiness of individuals, emotion detection or assistance of judges in court.⁸³ There are two necessary conditions for classifying other AI systems as high-risk. Firstly, it the system should be used in any of the areas listed in Annex III. Secondly, the system constitutes 'a risk of harm the health or safety' of humans, or 'a risk of adverse impact on fundamental rights'. The 'severity and probability of occurrence' of the risk should be equal to or higher than that of the systems already listed in Annex III.⁸⁴

According to the proposed Regulation, providers of certain high-risk AI systems are obliged to:

- (a) provide their system with high-quality data, that does not contain biases and inaccuracies, and are adapted to the setting where the system is intended to be used, so that the system will not be biased or discriminating.⁸⁵

⁷⁹ Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence, Brussels, 21 April 2021 [press release], available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1682.

⁸⁰ Proposal for the Artificial Intelligence Act, art. 1.

⁸¹ Proposal for the Artificial Intelligence Act, art. 52.

⁸² Speech by Executive Vice-President Vestager at the press conference on fostering a European approach to Artificial Intelligence, Brussels, 21 April 2021 [transcript], available at: https://ec.europa.eu/commission/presscorner/detail/en/speech_21_1866.

⁸³ Proposal for the Artificial Intelligence Act, Annex III.

⁸⁴ Proposal for the Artificial Intelligence Act, art. 7.

⁸⁵ Proposal for the Artificial Intelligence Act, art. 10.



- (b) maintain detailed technical documentation to demonstrate and assess compliance with applicable requirements set under the Artificial Intelligence Act.⁸⁶
- (c) ensure that the functioning of the AI system remains traceable throughout its lifecycle (record-keeping), so that it can be explained.⁸⁷
- (d) share substantial information with users to help them understand the output and how to properly use AI systems (transparency).⁸⁸
- (e) ensure a proper level of human oversight, both in the design as well as in the implementation stage of AI.⁸⁹
- (f) respect the highest standards of accuracy, robustness, and cybersecurity.⁹⁰

Unacceptable risk

The last category covers the uses of AI systems that are strictly prohibited, based on the type of AI technology and the intended use. There are four sub-categories of such uses (Figure 4). Firstly, the prohibition applies to AI systems that use subliminal techniques that can cause physical or psychological harm to someone. Secondly, AI systems that manipulate behaviour of vulnerable people on the basis of age or physical or mental disability, to make them cause harm, are strictly prohibited; for example, the use of AI in a toy that involves voice assistance to manipulate a child into doing something dangerous is prohibited. Thirdly, the proposed Regulation provides for a ban on AI systems that are used by public authorities to examine the trustworthiness of people for the benefit of a social scoring system. Finally, according to the proposal, the use of biometric identification systems in publicly accessible spaces for law enforcement purposes will be, in principle, prohibited. There are certain exceptions provided in this respect, such as a search of a missing child or threat of terrorist attacks.⁹¹

⁸⁶ Proposal for the Artificial Intelligence Act, art. 11.

⁸⁷ Proposal for the Artificial Intelligence Act, art. 12.

⁸⁸ Proposal for the Artificial Intelligence Act, art. 13.

⁸⁹ Proposal for the Artificial Intelligence Act, art. 14.

⁹⁰ Proposal for the Artificial Intelligence Act, art. 15.

⁹¹ Proposal for the Artificial Intelligence Act, art. 5.



Unacceptable risk (prohibited uses)

<p><u>1.</u> AI systems that use subliminal techniques that can cause physical or psychological harm to someone</p>	<p><u>2.</u> AI systems that manipulate behaviour of vulnerable people on the basis of age or physical or mental disability, to make them cause harm</p>
<p><u>3.</u> AI systems that are used by public authorities to examine the trustworthiness of people for the benefit of a social scoring system</p>	<p><u>4.</u> Biometric identification systems in publicly accessible spaces for law enforcement purposes</p>

Figure 6: Prohibited uses of AI, according to Article 5 of the proposed Artificial Intelligence Act.

Even though the Proposed AI Act is not yet applicable, it is recommended for each of the technologies used in AgriCapture, including software and data analytics, to assess whether they qualify to be AI under the definition above. If they do, a second step will be to determine of which risk category they are part of, and if and how it is feasible to take the appropriate measures associated with each risk category.

7.2 The Cybersecurity Act

Keeping in mind the rampant use of network and information systems by citizens, organisations and businesses in the EU and the increasing cybersecurity risks, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented the EU Cybersecurity Strategy. To allow citizens and organisations to leverage the benefits of trustworthy and reliable services and digital tools, the Strategy aimed at fortifying the EU’s resilience against cyberthreats. The Strategy also supports the EU to step up leadership on international norms and to bolster collaborations across the globe to promote an open, stable and secure cyberspace, grounded in the rule of law, democratic values, fundamental freedoms and human rights.

With that objective and pursuant to the Strategy, the European Commission also implemented the Cybersecurity Act (CSA) to establish a cybersecurity certification framework for products, services and processes across the EU in a holistic manner.⁹² In the very first article of the CSA, it is clarified that with a view to facilitate proper functioning of the internal market while aiming to achieve a high level of cybersecurity, cyber resilience

⁹² Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) OJ L 151. Available at: <https://eur-lex.europa.eu/eli/reg/2019/881/oj>.



and trust within the Union, the CSA focuses on two main objectives.⁹³ Firstly, to lay down the objectives, tasks and organisational matters relating to ENISA (the European Union Agency for Cybersecurity). Secondly, to create a framework for establishing European cybersecurity certification schemes that ensure an adequate level of cybersecurity for ICT products, ICT services and ICT processes in the EU and to avoid the fragmentation of the internal market with regard to cybersecurity certification schemes.⁹⁴

As mentioned above, the CSA reinforces the mandate of ENISA making the agency responsible for carrying out all tasks assigned to it pursuant to the CSA and to act as the reference point for advice and expertise on cybersecurity. ENISA is also required to assist Union institutions, bodies, agencies as well as Member States in creating and implementing Union policies relating to cybersecurity. In the context of capacity building, ENISA is required to assist Member States in their efforts to improve the prevention, detection and analysis of, and the capability to respond to cyber threats and incidents by providing them with knowledge and expertise.⁹⁵ The agency is also required to encourage the use of European cybersecurity certification and contribute to the establishment and maintenance of a European cybersecurity certification framework in accordance with the CSA.⁹⁶

Besides giving the ENISA a bigger role in the cybersecurity domain, the CSA provides for the establishment of a European cybersecurity certification framework to enhance the conditions for the functioning of the internal market by bolstering the level of cybersecurity within the EU. In addition, the European cybersecurity certification framework is to provide for a mechanism to create European cybersecurity certification schemes as well as to attest that the ICT products, services and processes that have been assessed in line with such schemes maintain the security requirements to protecting the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the functions or services offered by those products, services and processes throughout their life cycle.⁹⁷

Pursuant to the CSA, the European Commission is required to publish a Union-wide rolling work programme that will include a list of ICT products, services and processes or categories thereof that could potentially benefit from being included within the scope of a European cybersecurity certification scheme.⁹⁸ Inclusion of products, services and processes to be included in the rolling work programme would have to be justified based on certain grounds including market demand, developments in cyberthreat landscape and/or relevant union or member state law. The CSA also requires European cybersecurity

⁹³ Cybersecurity Act, art 1.

⁹⁴ Cybersecurity Act, art 1(b).

⁹⁵ Cybersecurity Act, art 6.

⁹⁶ Cybersecurity Act, art 4(6).

⁹⁷ Cybersecurity Act, art 46.

⁹⁸ Cybersecurity Act, art 47.



certification scheme to be designed to achieve certain objectives including: (a) to safeguard stored or otherwise processed (e.g. collected, analysed, exchanged) data against accidental or unauthorised storage, processing, access or disclosure during the life cycle of the ICT product, service or process (b) to ensure that authorised persons and machines can only access information to which their access rights refer, (c) to identify and document any vulnerabilities (d) to ensure that the ICT products, services and processes are secure by design and by default.⁹⁹

Interestingly, the CSA also introduces assurance levels wherein European cybersecurity certification scheme may specify one or more assurance levels for ICT products, services and processes namely basic, substantial or high.¹⁰⁰ These levels are to be proportionate with the level of the risk associated with the intended use of the said for ICT products, services or processes. For instance:

- A European cybersecurity certificate or EU statement of conformity for the assurance level '**basic**' that is given for ICT products, services or processes would mean that the said products, services or processes meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level intended to minimise the known basic risks of incidents and cyberattacks.¹⁰¹
- Similarly, A European cybersecurity certificate that refers to assurance level '**substantial**' would mean that the ICT products, services or processes meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level intended to minimise the known cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with limited skills and resources.¹⁰²
- Lastly, a European cybersecurity certificate that refers to assurance level '**high**' would translate to the ICT products, services or processes meeting the corresponding security requirements, including security functionalities, and having been evaluated at a level intended to minimise the risk of state-of-the-art cyberattacks carried out by actors with significant skills and resources.¹⁰³

⁹⁹ Cybersecurity Act, art 51.

¹⁰⁰ Cybersecurity Act, art 52.

¹⁰¹ Cybersecurity Act, art 52(5).

¹⁰² Cybersecurity Act, art 52(6).

¹⁰³ Cybersecurity Act, art 52(7).



8 Ethics in practice

Making it work does not simply mean putting effort into making technology function. Instead, it implies that the technology should be equipped by design with embedded non-functionals. These non-functionals are principles that prepare for potential risk the technology may encounter or cause. Including these non-functionals by design is therefore essential to make the technology work.

8.1 Accountability by design

Accountability is one of the key principles that flows from ethics. In moral interactions, it is essential that someone can be held *responsible* for their own actions. *Accountability* is a slightly stricter form of responsibility. There are three, non-exhaustive, examples of when it can become a pressing issue: in the energy exchange, in the data exchange, and in the interaction with machine interfaces.

Firstly, within the context of the AgriCapture pilots, where community members will consume, generate, store and exchange energy, accountability will be of considerable importance. Participants should in certain cases, for example, be able to hold someone accountable for not being able to deliver the required amount of electricity, if this is not due to their own in actions.

Secondly, in the data exchange market, this issue could become even more complex. Can residents hold the vendor of their smart meter accountable when their data processing activities do not comply with the terms of conditions in the contract? Who can be held accountable when the data on energy generation, consumption or storage, fall in the hands of the insurance company, who will then use insights derived from the data to tailor their insurance package to the energy behavior of individual households, thereby disadvantaging certain families?

Finally, accountability could become an even more pressing issue when considering that participants are not only interacting with each other, but also with machine interfaces. In a questionnaire distributed by the Commission among more than 200 stakeholders in the consumer IoT sector, of which 70% consists of large multinational organizations, the sector has expressed their concern that voice assistants and smart device operating system providers will have a more direct relationship with the user than they have. They fear that this close relationship between the technology interfaces and the user will could weaken their role as intermediaries between user and technology.¹⁰⁴ As a result, the accountability of these intermediaries for actions caused by IoT devices towards users

¹⁰⁴ European Commission (9 June 2021). Commission Staff Working Document: Preliminary Deliverable– Sector Inquiry into Consumer Internet of Things. Brussels: SWD(2021) 144 final. Available at: https://ec.europa.eu/competition-policy/system/files/2021-06/internet_of_things_preliminary_report.pdf



could be undermined. It is therefore recommended to prioritise keeping a human in the loop to be able to hold someone accountable for their actions or inactions.

In any of these scenarios, or in combined cases, the participants need a leg to stand on, that is, they need to be able to hold someone accountable for the harm, and, if appropriate, get a compensation. Generally speaking, participants and other stakeholders should be able to hold each other accountable for their actions or inactions. This also implies that people and participating organisations need to be aware that they can be held accountable for their actions, as an incentive for them to act more responsibly. Accountability is not only a theoretical moral principle, but it will also cater for becoming or being compliant to relevant standards and other applicable policy and legal frameworks.

Accountability is about owning and co-owning roles and responsibilities, finding solutions, making things happen, and helping out if things may go wrong once in a while. In this respect, accountability is not an afterthought dealt with after something goes wrong.

8.2 Other built-in values

Apart from accountability, there are more values and qualitative attributes that need to be embedded in the system in order to make it work, and to make them resilient to prepare for risks. These attributes, sometimes called 'non-functionals' in computer science jargon, are an integral part of any and every functionality. These principles, such as trust, security, safety, privacy, et cetera – will harness the system to prevent it from failing.

A thorough and holistic risk mapping approach allows for selecting the right principles, and giving each principle appropriate weight in comparison to the others. In the context of AgriCapture, risks could, for example, arise from the exchange of data between connected devices. The constant interactions between devices make the system more vulnerable for potential risk. It is therefore required to build in trust, privacy protection and security mechanisms, among others. Without taking care of the risks and mitigating them with these principles, the technological systems – devices, networks, algorithms – will eventually fail, possibly leading to unintended consequences.



9 Conclusion

This deliverable provided a holistic and extensive overview of the legal landscape that is relevant for AgriCapture currently and, possibly for the foreseeable future.

All legal requirements deemed mostly relevant, ranging from those requiring strict compliance to those that could serve as an inspiration to stakeholders to be 'more' ethical are presented under six (6) different perspectives. Given that mostly businesses are involved in the processing of data relating to AgriCapture, the market-centric perspective played naturally a key role in the discussion justifying the primer focus on the Trade-Secrets Directive; the significance of sustainability and of the respective perspective in relation to climate change was highlighted as well. The data-centric perspective was further addressed, including in relation to the free flow of non-personal data and data governance. Moreover, the economic perspective, mainly, revolving around financial economics, provided for some valuable insights both with respect to intellectual property and contract law, as well as payment services. Furthermore, protection of personal data linked to the human-centric perspective was taken into account to an extent, although non-personal data are those that are of direct relevance for the scope of AgriCapture. Finally, the AI Act and the Cybersecurity Act, also, relevant for AgriCapture platform were captured under the earlier discussion.

In addition to compliance, adherence and inspiration as considered in this document, what, essentially, matters is to 'make everything work'. In order to achieve this, solutions have to be made future-proof and, therefore, risk-resistant. To this end, it is of critical importance to embed fundamental ethical principles, such as accountability, in the design phase, meaning, from the early stages of the development process; this would allow the designer to deploy more responsible solutions, which could work for a longer period, therefore, further rendering the technological outcomes sustainable in the long run.



References

AgriCapture Grant Agreement - 101004282 - AgriCapture, October 2020 [Grant Agreement].

Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, The European Green Deal, COM/2019/640 final. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1576150542719&uri=COM%3A2019%3A640%3AFIN>.

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, available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066>.

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS EU Biodiversity Strategy for 2030 Bringing nature back into our lives COM/2020/380 final. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0380>.

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Making the most of the EU's innovative potential An intellectual property action plan to support the EU's recovery and resilience COM/2020/760 final. Available at: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52020DC0760>.

Consolidated version of the Treaty on the Functioning of the European Union OJ C 326, 26.10.2012, art 39. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT>.

CORDIS (April 2021). Reaping the benefits of healthy soils, for food, people, nature and the climate [article]. Available at: <https://cordis.europa.eu/article/id/429351-soil-health-reaping-the-benefits-of-healthy-soils-for-food-people-nature-and-the-climate> (see especially: <https://cordis.europa.eu/article/id/429361-sharing-expertise-to-increase-soil-carbon-sequestration-and-healthy-soil-practices>).

Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (Text with EEA relevance) OJ L 157. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0943>.

Directive (EU) 2019/633 of the European Parliament and of the Council of 17 April 2019 on unfair trading practices in business-to-business relationships in the agricultural and food supply chain OJ L111/59. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019L0633>.

Directorate-General for Research and Innovation (European Commission) (September 2020). Caring for Soil is Caring for Life [publication]. Available at: <https://op.europa.eu/en/publication-detail/-/publication/4ebd2586-fc85-11ea-b44f-01aa75ed71a1/language-en/format-PDF/source-search>.

EU Code of conduct on agricultural data sharing by contractual agreement. Available at: http://fefac.eu/wp-content/uploads/2020/07/EU_COD1.pdf.



Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence, Brussels, 21 April 2021 [press release], available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1682.

European Commission (2020). Inception Impact Assessment, Revision of the eIDAS Regulation – European Digital Identity (EUid) [impact assessment]. Available at: <https://www.gleif.org/content/1-about/8-gleif-engagement/2-consultation-responses/inception-impact-assessment.pdf>.

European Commission (2020). Mission area: Soil health and food [online resource]. Available at: https://ec.europa.eu/info/research-and-innovation/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe/missions-horizon-europe/soil-health-and-food_en.

European Commission (2020). Open Public Consultation on the European Strategy for Data, Summary Report on the open public consultation on the European strategy for data [public consultation]. Available at: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=68611.

European Commission (2020). Inception Impact Assessment, Legislative framework for the governance of common European data spaces [impact assessment]. Available at: [https://eur-lex.europa.eu/legal-content/EN/TXT/DOC/?uri=PI_COM:Ares\(2020\)3480073&from=EN](https://eur-lex.europa.eu/legal-content/EN/TXT/DOC/?uri=PI_COM:Ares(2020)3480073&from=EN).

European Commission (24 July 2013). Impact Assessment accompanying the document Proposal for a directive of the European parliament and of the Council on payment services in the internal market and amending Directive 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC and Proposal for a Regulation of the European Parliament and of the Council on interchange fees for card-based payment transactions [Commission Staff Working Document]. Available at: https://eur-lex.europa.eu/resource.html?uri=cellar:906ed6d3-f509-11e2-a22e-01aa75ed71a1.0001.04/DOC_1&format=PDF.

European Commission (8 July 2019). Regulation on the free flow of non-personal data [publication]. Available at: https://knowledge4policy.ec.europa.eu/publication/regulation-free-flow-non-personal-data_en.

European Commission (8 July 2019). Regulation on the free flow of non-personal data [publication]. Available at: https://knowledge4policy.ec.europa.eu/publication/regulation-free-flow-non-personal-data_en.

European Commission (9 June 2021). Commission Staff Working Document: Preliminary – Sector Inquiry into Consumer Internet of Things. Brussels: SWD(2021) 144 final. Available at: https://ec.europa.eu/competition-policy/system/files/2021-06/internet_of_things_preliminary_report.pdf.

European Commission (April 2021). Report on the protection and enforcement of intellectual property rights in third countries [working document]. Available at: https://trade.ec.europa.eu/doclib/docs/2021/april/tradoc_159553.pdf.

European Commission, Overview of sustainable finance, available at: https://ec.europa.eu/info/business-economy-euro/banking-and-finance/sustainable-finance/overview-sustainable-finance_en.

Eurostat (no date). LUCAS – Land use and land cover survey[online resource] . Available at: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=LUCAS_-_Land_use_and_land_cover_survey.



- FAO (no date). What is Soil Carbon Sequestration? [online resource] Available at: <http://www.fao.org/soils-portal/soil-management/soil-carbon-sequestration/en/>.
- Farm Data Code, National Farmers Federation. Available at: <https://nff.org.au/programs/australian-farm-data-code/>.
- Global Partnership for Sustainable Development Data (no date). Better data [online resource]. Better decisions. Better Lives. Available at: <https://www.data4sdgs.org/>.
- Global Partnership for Sustainable Development Data (no date). Our Impact [online resource]. Available at: <https://www.data4sdgs.org/about-gpsdd/our-impact>.
- Global Partnership for Sustainable Development Data (no date). Resources [online resource]. Available at: <https://www.data4sdgs.org/resource-listing>.
- Hannah Ritchie and Max Roser (2020) - CO₂ and Greenhouse Gas Emissions. Published online at OurWorldInData.org [Online Resource]. Available at: <https://ourworldindata.org/co2-and-other-greenhouse-gas-emissions>.
- New Zealand Farm Data Code of Practice. Available at: <https://www.farmdatacode.org.nz/>.
- Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act) COM/2020/767 final. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767>.
- Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts COM/2021/206 final. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206>.
- Regulation (EU) 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, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119, art 6(b). Available at: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.
- 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. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1807>.
- Regulation (EU) 2019/2088 of the European Parliament and of the Council of 27 November 2019 on sustainability-related disclosures in the financial services sector OJ L 317/1. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019R2088>.
- Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) OJ L 151. Available at: <https://eur-lex.europa.eu/eli/reg/2019/881/oj>.
- Speech by Executive Vice-President Vestager at the press conference on fostering a European approach to Artificial Intelligence, Brussels, 21 April 2021 [transcript], available at: https://ec.europa.eu/commission/presscorner/detail/en/speech_21_1866.
- UNFCCC. Clean Development Mechanism (CDM). Available at: <https://cdm.unfccc.int/>.



Annexes

Annex I

The Annex I below provides for an analysis of the relevant stakeholder groups associated with AgriCapture per use case. The AgriCapture project has a wide array of stakeholders, of which a certain proportion is already known, but a large part of the stakeholders will be identified as the pilots mature. For the stakeholder analysis, a framework is used capturing human-centric technology, thriving ecosystems & multi-angled stakeholders & influencers (figure 7). This stakeholder plotting and analysis preceded the work captured in the main body of the document.

Human-Centric Technology, Thriving Ecosystems & Multi-Angled Stakeholders & Influencers

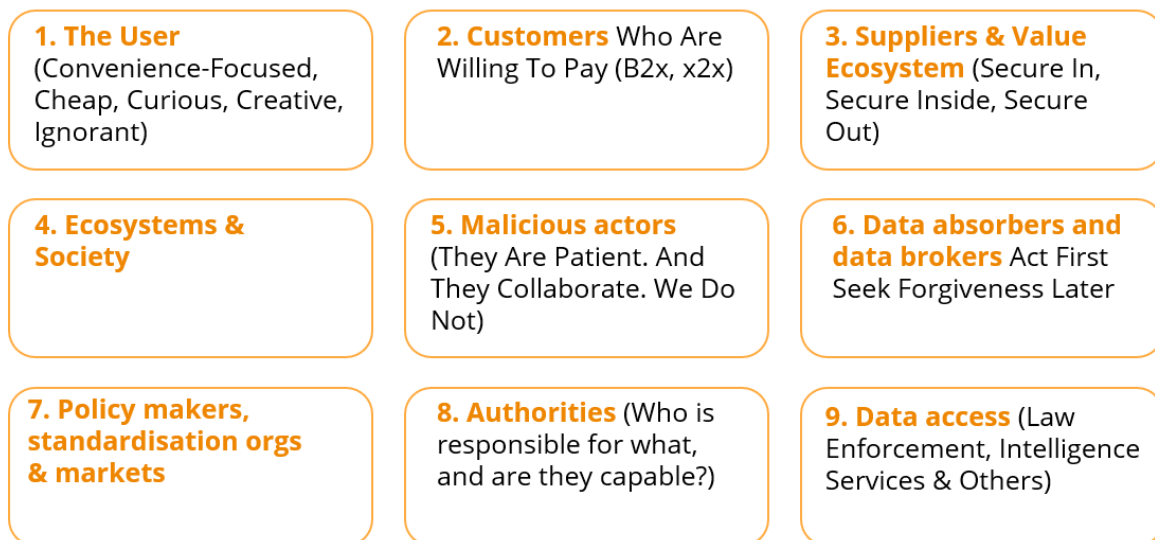


Figure 7: Multi-angled stakeholders & influencers

Use case 1: Sustainable olive oil: Water-efficiency in semi-arid agriculture (ELGO, Greece)

Product: soil sensors, multi-spectral UAV imagery, in-situ meteo station, soil data

The user	Water & data & technologies → farmers, olive oil → customers
Customers	Olive oil → tourists, locals
Suppliers & value ecosystem	Farmers (100), agri-cooperatives, olive mill owned by agri-cooperative, processor (2), retailers (5)



Ecosystems & Society	Natural ecosystem of Crete, local community in Crete
Malicious actors	
Data absorbers and data brokers	
Policy makers, standardisation orgs & markets	
Authorities	Local government, Greek national government, EU
Data access	

GHG

Use case 2: Capturing ecological value: Large-scale sequestration on Europe's large farms (SatAgro, Poland)

Product: soil data (existing farmer data, EIONET datasets & to be collected), socio-economic data

The user	Data → farmers & ?
Customers	Crops → consumers
Suppliers & value ecosystem	Farmers (ca. 215), agrifood corporates
Ecosystems & Society	Local ecosystem, local community
Malicious actors	
Data absorbers and data brokers	
Authorities	Local government, Polish national government, EU
Data access	

Use case 3: Scaling certified Reg Agri businesses: New streams of revenues for Reg Agri farmers (FrOils, UK)



Product: soil data (existing farmer data & to be collected), UK national soil survey, long-term GWCT field trial data

The user	Farmers, agri-processor, Reg Agri certifier
Customers	Crops → consumers
Suppliers & value ecosystem	Farmers (>20), agri-processor, Reg Agri certifier
Ecosystems & Society	
Malicious actors	
Data absorbers and data brokers	
Authorities	Local government, UK national government, EU
Data access	

Use case 4: Meeting public climate commitments: Informing public land management for climate action (GiLab, UK)

Product: soil samples, UK national soil survey data

The user	Lancashire County
Customers	
Suppliers & value ecosystem	UK Environment Agency, Lancashire Environmental Record Network, Local Nature Partnerships
Ecosystems & Society	
Malicious actors	
Data absorbers and data brokers	
Authorities	Local government, UK national government, UK Environment Agency, Lancashire Environmental Record Network, Local Nature Partnerships. EU
Data access	



Use case 5: Overcoming financial barriers to sustainable agriculture: Carbon farming under UN's CDM (Serbia)

Product: soil data (existing and to be collected)

The user Farmers, Government Ministries, Citizens in Ruma

Customers

Suppliers & value ecosystem Farmers (20), Government Ministries, Citizens in Ruma

Ecosystems & Society

Malicious actors

Data absorbers and data brokers

Authorities Local government, national government, EU

Data access



End of document



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 101004282.

The content of this publication exclusively reflects the author's view and the Research Executive Agency and the Commission are not responsible for any use that may be made of the information it contains.

