15

Does Everything Conform to Legal, Ethical, and Data Protection Principles?

Marina Da Bormida in Cugurra

Genoa, Italy
Email: marina.cugurra@eta-one.com

Abstract

In this chapter, the legal and ethical sources relevant to personal data sharing systems, both already applicable and under development, are identified and the main challenges related to personal data sharing operations and practices are sketched, as well as the technology-related opportunities to tackle them, with special attention to what DataVaults[1] technological fixes are going to offer to the data marketplace in this regard towards a trustworthy personal data sharing environment. The chapter also offers an overview of the ethics-related work performed, tools employed, and achievements reached in the DataVaults project: such tools and work could be replicated in other environments, with some adaptations, with the same goal of ensuring the adherence to the relevant legislation, especially GDPR, and to the ethical mandates.

15.1 Introduction

This chapter provides an overview of the legal and ethical framework relevant to personal data sharing systems, focusing on both the existing regulatory sources and on the reforms under development. Such reforms are expected to shape, among other, the future personal data economy, seeking to address the main challenges and barriers related to the operations and practices rotating around personal data. The chapter moves on with a deep-dive on some of

[1] https://www.datavaults.eu/

such challenges and some examples of technology-related opportunities to tackle them with under the current and future European regulatory regime, in particular, underlying what DataVaults technological fixes are going to offer to the private and urban-scale data sharing platforms operating with personal data. Besides these insights on how DataVaults platform in its whole or some of its privacy-preserving technological artefacts could support a trustworthy personal data sharing environment for the benefit of all the involved stakeholders, the chapter also offers an overview of the ethics-related work, tools, and achievements characterising DataVaults itself, from its ethical policy and legal and ethical requirements elicitation, to the ethics and data protection impact assessment methodology used in its piloting activities to assess the legal compliance and ethical soundness of the project's technologies and their use in real-life contexts. These activities and tools can be used in other environments, with some adaptations, with the same goal of ensuring the adherence to the relevant legislation, especially GDPR, and ethical mandates. The chapter ends by drawing conclusions.

This chapter and its findings are mainly based on the legal and ethical surveys conducted within the DataVaults project and take inspiration and extracts from it, combined with insights coming from the recent debates and the literature.[2]

15.2 The Evolving Regulatory Framework Relevant to the Personal Data Sharing Platforms

One of the main barriers to the development and growth of the data economy in relation to personal data is the lack of trusted and secure personal data platforms capable of handing back control over the use of personal data to individuals. This shortcoming hampers personal data sharing practices, despite the wide individuals' willingness to share personal data in return for actual benefits, non-necessarily financial.

There is the need for trusted, secure, and value generating data management and sharing platforms for personal data, allowing stakeholders' collaboration in order to support their own goals and operations, as well

[2] DataVaults Consortium, D2.1 "Security, Privacy and GDPR Compliance for Personal Data Management" (2020).
DataVaults Consortium, D2.3 "Updated DataVaults Security Methods and Market Design" (2021)
DataVaults Consortium, D1.3 "DataVaults MVP and Usage Scenarios", (2021). More information on the DataVaults projects can be retrieved at. https://www.datavaults.eu/

as allowing further stakeholders, such as local communities and local authorities, to offer new socially and environmentally sustainable solutions and business models.

In other words, there is the need for solutions moving forward towards regaining the trust of individuals when it comes to data sharing, letting the control in the hands of the data owners (the individuals) who will be able to decide how, how much, and in which manner they would like to share their personal information, while, at the same time, guaranteeing their privacy and adequate security levels as well as ensuring fair share of the value that their data generate, also in case of secondary use.

This approach is aligned with the European Commission's vision of personal data sharing that should provide benefits for all the actors in the value chain.

Both at European level and in the society, it is emerging the perception that personal data spaces should be promoted, especially on a EU-wide level, ensuring the legal compliance and fostering trust and collaboration. This vision includes addressing the concerns on security, privacy, ethics, and IPR ownership for prioritising human wellbeing and fundamental rights in the data-driven economy.

The recent works "A European Strategy for Data"[3] and the "White Paper on Artificial Intelligence",[4] which represent two pillars of the new digital strategy of the Commission, underline this vision for putting people first in developing technology, defending and promoting European values and rights in any design, development, and deployment of the technology in the real economy.

Any personal data sharing platform should fully embrace this strategy and the promotion of such values, including protection of privacy. In order to do so and foster the creation of a single market for data upholding such values and fully respecting individuals' rights and freedoms, the compliance with the existing legal sources is first of all paramount, and also the adequate consideration of the regulatory reforms under development.

---

[3] COM/2020/66 final, Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions. "A European strategy for data". Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066

[4] COM/2020/65 final, "WHITE PAPER On Artificial Intelligence - A European approach to excellence and trust". Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0065&WT_mc_id=Twitter

15.3 Existing Regulatory Framework

The consideration of the overall regulatory and ethical framework relevant to the personal data sharing, comprising a number of applicable instruments to be addressed in a systematic way, is key to design, develop, deliver, and operate the personal data platforms in an ethical, private, and fairness-friendly way, which is at the same time compliant with the legislation, and where individuals are enabled to take ownership and control of their data and share them at will, while value is properly attributed to all the entities involved in generating the same. This section does not present a comprehensive analysis of the European regulatory framework, which would fall outside the scope of this work. On the contrary, it indicates the main instruments that are functional to the objective mentioned above.

GDPR, "General Regulation on data protection". The first piece of legislation to mention is the GDPR, "general regulation on data protection 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".[5] It repealed the Directive 95/46/EC (General Data Protection Regulation), providing a comprehensive reform of data protection rules in the EU, establishing common European rules to ensure that personal data enjoys a high standard of protection everywhere in the EU.

One of the main objectives of the GDPR is to give back individuals the control over their personal data, thereby acting as key enabler of the Digital Single Market: personal data can only be gathered and handled legally under strict conditions and for a legitimate purpose. The individuals or organisations collecting or managing personal information have to protect it from misuse and have to respect the data subject's rights, whilst the data subject is enabled to complain and obtain redress if his/her data is misused.

The whole legal source might be relevant to the sharing of personal data within a data platform.

Directive 2002/58/EC "ePrivacy Directive". Another instrument relevant to a personal data sharing platform is the "ePrivacy Directive" (Directive 2002/58/EC on privacy and electronic communications[6]), which replaced the

[5] European Commission, "General Regulation on data protection 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". Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj

[6] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l24120&from=EN

Directive 97/66/EC and was partially amended by Directive 2009/136/EC. It pertains to the processing of personal data and the protection of privacy in the sector of electronic communications, telecommunications networks, and internet services, transposing in the telecommunications sector, which is a "sensitive" area from a privacy perspective, the main principles and rules of the GDPR, aiming at particularising and complementing the former (for instance, as regards the consent to the use of cookies and opt-outs) in case electronic communications data are personal data. Several provisions might be relevant in relation to the exchange of personal data, such as Article 2, on the traffic data and location data, Article 4, on the obligation of adopting security measures appropriated to the risk presented, Article 5, dwelling on the protection to confidentiality of the communications among individuals, Article 6, on user's consent, Article 15, on data retention, and others. The ePrivacy Directive is expected to be repealed by the ePrivacy Regulation.

Human rights law: This area of law includes, among other sources, above all, the European Convention on Human Rights[7] and the Charter of Fundamental Rights of the European Union.[8] Both of them acknowledge privacy and data protection as fundamental human rights in Europe.

From an international perspective, the Universal Declaration of Human Rights (1948) is also relevant: it recognises the privacy as a fundamental human right by protecting territorial and communications privacy. Its Article 8 deals with private and family life, home, and correspondence of the citizen. Since then, more enforceable European tools surpassed its application in the field of data privacy. Article 8.2 states the lawfulness criterion, in the meaning of rule of law.

The European Court of Human Rights' jurisprudence has to be taken into account in relation to personal data sharing practices and tools. This case law is an essential factor supporting the application of these legal sources in relation to the technological artefacts supporting the personal data sharing.

Ethics and soft law instruments. The composite regulatory system to be taken into account also comprises the soft law sources (quasi-legal instruments), which may not have any legally binding force but is helpful in so far they serve to fill in gaps, identify safeguards, boundaries, and obligations to ensure the legitimacy and fairness of personal data sharing platforms, and,

[7] The European Convention on Human Rights, adopted in 1950 and entered into force in 1953. The Convention and its Protocols can be retrieved at the following link:https://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/treaty/results/subject/3

[8] Charter of Fundamental Rights of the European Union, 2016/C 202/02. It can be retrieved at the following link: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12016P/TXT&from=EN

at the same time, contributed to find out, on a case-by-case basis, a balance between competing interests. Soft law has an array of possible benefits and usually runs within the boundaries set by its interplay with the traditional legal instruments, in a landscape of increasingly dynamic cross-fertilisation of regulations and technology. It should receive the appropriate consideration when determining personal data sharing technology design and deployment, especially due to the rapidly developing field of data sharing ecosystems: thanks to its flexible nature, that lets it be quickly adapted to future technological progress, soft law could provide useful insights, recommendations, and indications and support in identifying the adequate safeguards and mechanisms in relation to transparency and accountability.

Among the other soft law sources, we can mention, for instance, the European Commission's Communications "AI for Europe" (25 April 2018) and "Building Trust in Human-Centric AI" (8 April 2019), as well as the "Data Protection in the era of Artificial Intelligence. Trends, existing solutions and recommendations for privacy-preserving technologies" (BDVA,[9] October 2019) and "Meeting the challenge of Big Data. A call for transparency, user control, data protection by design and accountability" (Opinion 7/2015, European Data Protection Supervisor, 2015).

Regulation 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS).[10] This source, repealing the Directive 1999/93/EC, is potentially relevant to the personal data sharing platform. It is aimed at ensuring the proper functioning of the internal market, facilitating seamless digital transactions among individuals and businesses across the same, and creating a climate of trust in online and digital transactions. According to Article 2, it applies to electronic identification schemes notified by a Member State and to trust service providers established in the Union.

This regulation consists of two main parts: one concerns electronic identification, whilst the other concerns trust services (electronic signatures and other trust services).

It sets the conditions for the recognition of electronic identification means of natural and legal persons, the rules for trust services (especially for electronic transactions), besides introducing a legal framework for electronic signatures, electronic seals, electronic time stamps, electronic documents,

[9] Big Data Value Association

[10] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31999L0093

electronic registered delivery services, and certificate services for website authentication. Its provisions regarding the electronic registered delivery services might be relevant to the personal data sharing platforms, since their services can fall into such concept. In fact, the electronic registered delivery service is defined by eIDAS a "service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and which protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations" (Art. 3, (36) eIDAS). On the other hand, Article 2 (2) eIDAS states that this regulatory source does not apply to "the provision of trust services that are used exclusively within closed systems resulting from national law or from agreements between a defined set of participants". In any case, the eIDAS Regulation states that the processing of personal data must be carried out in accordance with the GDPR and respecting its principle of confidentiality and security of processing.

Regulation 2018/1807 on a framework for the free flow of non-personal data in the European Union, adopted by the EC, applies to any form of data other than personal data, as defined in Article 4.1 of the GDPR. It is functional to create a comprehensive and coherent approach to the free movement and portability of data in the EU. Notably, its main objectives are to further promote the free movement of data and data processing services (Recital 4), whilst facilitating cross-border availability of data, enhancing legal certainty and creating a level playing field through a single set of rules for all market participants. It supplements and complements the GDPR in issues related to non-personal data within the Digital Single Market, primarily concerning business and public sector users of data storage and processing services. This instrument should be taken into account in relation to the non-personal data (such as insights, other derivatives, data related to the persona, and data completely anonymised) collected, shared, and used in the personal data platform, as well as for mix platform, combining personal and non-personal data sharing.

E-Commerce Directive, Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the internal market. This is another important legislative source that might be relevant for the operation of personal data sharing platform, considering that their services, to the extent that they represent information society services, might be provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of the service and, therefore, fall under the scope of this Directive. Considering the nature of this source, the national provisions implementing it would need to be considered in each country

where the personal data platform is adopted. Section 4 on intermediary liability may be particularly relevant in the case of illicit third-party content.

Platform-to-Business Regulation – P2BR. The Regulation 2019/1150 on promoting fairness and transparency for business users of online intermediation services is a set of rules in the area of business platforms for creating a fair, transparent, and predictable business environment for smaller businesses and traders on online platforms, in order to enable consumers to receive the highest quality goods and services. The P2BR, which is part of the legislative measures promoted by the EC for the Digital Single Market strategy, foresees a list of measures ensuring transparency and fairness with the intent to temper the natural asymmetries that characterise the relationship between the platforms and their suppliers, establishing a fair and trustworthy innovation-driven ecosystem. Its Article 2 describes a set of requirements of the intermediation services (platforms) that fall into the scope of its application. Its definition of intermediaries describes only the services that have a direct relationship with business users and their clients without a clear threshold, applying indistinctively to all types of platforms falling in such criteria. The two main principles set by the P2BR are transparency and fairness. Taking into account who the data platform concerned intends to offer its services to, it could fall within the P2BR scope. Nevertheless, in order to be applicable to such a platform, it should fall under the concept of online intermediation service: whilst it is likely that the data providers are businesses, it is not sure that the data receivers are consumers, as requested by the definition of the online intermediation service, which is, in principle, applicable only for business users.[11]

Directive 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services might also be relevant. Given that contracts are often crucial for the personal data platform, it is paramount to consider the EU framework related to contractual agreements, which may be applicable in the context of the project. From a consumer policy perspective, considering the steps taken by the EC to implement a "digital update" of consumer contract law, it is widely recognised that consumers should enjoy the same level of protection under consumer contract law, whatever the object of consumption is. This Directive aims at the maximum harmonisation

[11] Such services must have the following characteristics: being information society services, i) allowing business users to offer goods or services to consumers for facilitating the initiating of direct transactions between such business users and consumers ii) and provided to business users on the basis of contractual relationships between the provider of those services and business users (which, in turn, offer goods or services to consumers).

and at introducing mandatory contractual liability for the non-conformity of digital content with the contract. It also extends the information duties as well as the right to withdraw from a contract in case of "free digital services" contracts, where consumers provide personal data instead of paying a fee. The Directive is directed to protect the consumer, understood as "any natural person who, in relation to contracts covered by this Directive, is acting for purposes which are outside that person's trade, business, craft, or profession" (Article 2.6).[12] The Directive applies to "contracts of an indefinite or fixed duration which were concluded before the application date and provide for the supply of digital content or digital services over a period of time, either continuously or through a series of individual acts of supply, but only as regards digital content or a digital service that is supplied from the date of application of the national transposition measures", with the exception of the provisions on the modification of the digital content or digital service and the right to redress. In relation to contractual agreements and consumer protection, also the following pieces of legislation can be considered: Directive 93/13/EEC on unfair terms in consumer contracts and Directive 2019/2161 (amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC, and 2011/83/EU) as regards the better enforcement and modernisation of Union consumer protection rules.

Security Law. Despite from a legal point of view the requirements related to security are mainly coming from the GDPR and the ePD, it is useful to take into account the latest legislative developments in this area. Cybersecurity has been identified as one of the highest priorities for the EU: the achievement of a secure and safe environment is a precondition to enhance trust and to boost business opportunities. In this area of law, it is important to mention the following.

- The Directive 2016/1148 on security of network and information systems (NIS), which was part of the 2013 EU cybersecurity strategy, comprising binding and non-binding legal instruments aimed at establishing a high standard of security across the European Union. It applies to operators of essential services and digital service providers.
- The Regulation (EU) 2019/881 (Cybersecurity Act), included in the Cybersecurity Package. It provides rules on the creation of an EU cybersecurity certification scheme for ICT products, ICT services, and ICT

[12] Member states can extend the protection afforded to other persons who are not qualified as consumers.

processes and aims to improve the cross-border coordination, besides promoting EU standards. The cybersecurity certification schemes for ICT products, ICT services, and ICT process might be of interest for a personal data platform, since it can enhance its security and trust.

As regards the EU encryption framework, the following documents are particularly interesting for the personal data market: the ENISA[13] Opinion Paper on encryption (2016) and the European Electronic Communications Code (EECC), established with the Directive 2018/1972. This code, in its security provisions, makes reference to encryption protocols and, explicitly, to the end-to-end encryption.

15.4 The Regulatory Reforms Under Development

Vast reforms are underway and an update of the European regulatory landscape was announced in terms of the Commission's Mission Statement for 2019–2025. Especially some of them are expected to be significant for the deployment and use of personal data platform.

Considering the envisaged role of individuals as data owner, it is opportune to follow the developments in terms of the European consumer protection framework and, more specifically, the developments related to so-called "New Deal for Consumers" initiative, adopted in 2018.[14] This initiative is functional to achieve a stronger and better enforced consumer protection rules in light of a growing risk of EU-wide infringements and at modernising EU consumer protection rules in view of market developments.

Another important regulatory source is the Communication "2030 Digital Compass: the European way for the Digital Decade".[15] Its Vision for 2030 relies on empowered citizens and businesses. The Communication also underlines the need to full respect of EU fundamental rights, including the freedom of expression (including access to diverse, trustworthy, and transparent information), the freedom to set up and conduct a business online, the protection of personal data and privacy and right to be forgotten, and the

[13] European Union Agency for Network and Information Security

[14] Communication of the Commission of 11 April 2018—A New Deal for Consumers, (COM)2018, 183 final. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0183

[15] COM(2021) 118 final. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "2030 Digital Compass: the European way for the Digital Decade". Available at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118

protection of the intellectual creation of individuals in the online space. It is envisaged the definition of a comprehensive set of digital principles allowing to inform users (besides guiding policy makers and digital operators), including, for instance, a secure and trusted online environment, the access to digital systems, and devices that respect the environment, accessible and human-centric digital public services and administration, ethical principles for human-centric algorithms, and access to digital health services. The EC proposed to include these sets of digital principles and rights within an inter-institutional solemn declaration between the European Commission, the European Parliament, and the Council.

The overarching regulatory framework especially relies on the already mentioned new European Data Strategy. It was presented along with the Commission's Communication on "Shaping Europe's digital future": data are embraced as the "lifeblood of economic development". Therefore, the EC aims at renewing its overarching framework to achieve the proper balance between, on the one hand, the wide availability and use of data and, on the other hand, the high preservation of privacy, security, safety, and ethical standards. Aspects related to data ownership and data governance are going to be addressed and/or reframed. The Strategy is motivated by the need to put people first in developing technology and to defend and promote European values and rights in how the technology is designed and deployed in the real economy. The Strategy sets out a programme of policy reforms, already started with the Data Governance Act, the Digital Services Act, the Digital Markets Act, and the Cybersecurity Strategy.

The proposal **Data Governance Act** (DGA) was published in November 25, 2020 and has been conceived to play a vital role in ensuring the EU's leadership in the global data economy, whilst empowering users to stay in control of their data. The DGA sets out policy measures and investments designed to capitalise on European vast quantity of data and, hence, to give the EU businesses a competitive advantage. The envisioned framework is expected to boost data sharing, encouraging a greater reuse of data by increasing trust in data intermediaries and strengthening various data-sharing mechanisms across the EU. In addition, the DGA will support the creation of EU-wide common, interoperable data spaces in strategic sectors relevant to the personal data platform, such as health, energy, and mobility, which, in turn, are meant to bring benefits to citizens. Its broad definition of data includes personal data as defined in the GDPR, which apply simultaneously to the DGA. As remarked by the explanatory memorandum, the DGA and its measures are fully compliant with the data protection legislation and increase, in practice, the control that individuals have over the data that they generate.

This is an important element for the personal data economy and the personal data platforms in particular. Many of its rules are potentially relevant for the private and urban personal data platforms. They include, among others:

- conditions for reuse of public sector data, which are subject to existing protections (such as intellectual property, commercial confidentiality, and data protection);
- obligations on providers of various types of intermediation services within data-sharing services – new European rules on neutrality are defined to allow novel data intermediaries to function as trustworthy organisers of data sharing;
- a set of measures to increase trust in data-sharing, due to the fact that the lack of trust is currently a major obstacle and results in high costs;
- data altruism, providing its concept and the possibility for organisations to register as "Data Altruism Organization recognized in the Union";
- measures to give the individuals the control on the use of the data they generate, in particular by making it easier and safer for companies and natural persons to voluntarily make their data available for the wider common good under clear conditions.

On the other hand, the proposal European Digital Service Act (DSA)[16] is expected to update and reform the framework established by the e-Commerce Directive, addressing the topics of intermediary liability and safety rules for digital platforms, including transparency, information obligations, and accountability for digital services providers. At the same time, there is a strong call for maintaining the core principles of the e-Commerce Directive, its measures having the consumer protection at their core and the protection of fundamental rights in the online environment, as well as online anonymity wherever technically possible. In fact, the DSA builds on the key principles set out in the e-Commerce Directive, which is still applicable, seeking to ensure the best conditions for the provision of innovative digital services in the internal market, to contribute to online safety and the protection of fundamental rights, whilst setting a robust and durable

[16] COM/2020/825 final, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC. Available at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A825%3AFIN

governance structure for the monitoring and supervision of providers of intermediary services.

Since the adoption of the e-Commerce Directive, novel information society (digital) services have emerged, which, on the one hand, have deeply contributed to societal and economic transformations in the European Union and worldwide but, on the other hand, have brought new risks and challenges, both for society as a whole and for individuals using such services. The DSA, which is envisaged to be a standard-setter at global level, addresses the online marketplaces and consumer trust in the digital economy, while respecting users' fundamental rights and advocating for rules to underpin a competitive digital environment in Europe. Clear responsibilities and accountability are defined for providers of intermediary services, and in particular online platforms, including marketplaces. Due-diligence obligations are set for certain intermediary services in order to improve users' safety online across the entire Union and improve the protection of their fundamental rights. Certain online platforms have the obligation to receive, store, partially verify, and publish information on traders using their services in order to ensure a safer and more transparent online environment for consumers. A higher standard of transparency and accountability is set for certain platform as well as obligations to assess the risks their systems pose and to develop appropriate risk management tools to protect the integrity of their services against the use of manipulative techniques. However, the operational threshold for service providers in scope of these obligations includes only online platforms with a significant reach in the European market (currently set to more than 45 million recipients of the service). The DSA is without prejudice to the GDPR.

The proposal Digital Market Act[17] might be relevant to the personal data architectures in the future. Its objective is "to allow platforms to unlock their full potential by addressing at EU level the most salient incidences of unfair practices and weak contestability" in view of allowing end-users and business users alike to reap the full benefits of the platform economy and the digital economy at large, in a contestable and fair environment. Nevertheless, its scope of application concerns "markets characterised by large platforms, with significant network effects acting as gatekeepers".

The **proposal of Regulation on Privacy and Electronic Communications (ePrivacy Regulation)** is another legal instrument under development to

[17] COM/2020/842 final, Proposal for a Regulation of the European Parliament and the Council on contestable and fair markets in the digital sector (Digital Markets Act). Available at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A842%3AFIN

monitor is the ePrivacy Regulation,[18] intended to update European privacy framework, repealing the ePrivacy Directive, for a better alignment of the provisions of such Directive with those of the GDPR, while addressing the new challenges to privacy, brought about by the significant advancement of technology the last two decades. In fact, albeit objectives and principles of the existing framework remaining sound and relevant, the essential technological, economic, and business progresses, together with the ever-increasing penetration of the internet in various aspects of the life and its vital role in the Digital Single Market, call for the modernisation of the Directive. The choice of a Regulation is meant to improve the harmonisation. As clarified in the proposal itself, it will be "*lex specialis*" to the GDPR: it will fine-tune and complement the GDPR as regards electronic communications data that qualify as personal data, whilst all matters concerning the processing of personal data not covered by the proposal remain regulated by the GDPR.

The **proposal for a Directive on measures for a high common level of cybersecurity across the Union**[19] pertains to the area of security and will repeal the Directive (EU) 2016/1148. This proposal is directed to introduce systemic and structural changes to the current NIS Directive for covering a wider set of entities across the Union, with stronger security measures, such as mandatory risk management, minimum standards, and relevant supervision and enforcement provisions. As highlighted by the European Data Protection Supervisor,[20] it is essential to integrate "the privacy and data protection perspective in the cybersecurity measures stemming from the Proposal or from other cybersecurity initiatives of the Strategy in order to ensure a holistic approach and enable synergies when managing cybersecurity and protecting the personal information they process", and that "all cybersecurity systems and services involved in the prevention, detection, and response to cyber threats should be compliant with the current privacy and data protection framework".

---

[18] COM/2017/010 final, Proposal for a Regulation of the European Parliament and the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010

[19] COM/2020/823 final, Proposal for a Directive on measures for a high common level of cybersecurity across the Union , repealing Directive (EU) 2016/1148. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A823%3AFIN

[20] European Data Protection Supervisor, "Opinion 5/2021 on the Cybersecurity Strategy and the NIS 2.0 Directive", 2021. Available at: https://edps.europa.eu/data-protection/our-work/publications/opinions/edps-opinion-cybersecurity-strategy-and-nis-20_en (accessed Jul. 29, 2022)

In parallel, the EC and the High Representative of the Union for Foreign Affairs and Security Policy issued a Joint Communication titled "The EU's Cybersecurity Strategy for the Digital Decade", whose overall objective is to ensure a global and open internet with strong safeguards for the risks to security and the fundamental rights, in a multi-stakeholder model.

15.5 Main Legal and Ethical Challenges and Technology-enabled Opportunities to Tackle with Them

The operation of a personal data platform might imply a number of legal and ethical challenges, for instance, related to personal data management in terms of data collection, data sharing and processing, as well as to the potential trade-off between the need to maximise data utility whilst protecting human rights and preserving meaningful human control or the question if and to what extent the future technological development should allow for automation of (legal) protection in an increasingly digital society.[21]

In the following paragraphs, some important challenges and trends related to the tools and technologies aimed at facilitating secure and trustworthy data sharing in an urban and private environment are provided, taking inspiration and extracts from the work and regulatory surveys conducted within the DataVaults project,[22] also in this case combined with insights from recent debates and the literature.

15.6 The Need to Avoid Consent Fatigue and to Develop and Use User- and Data-Protection-Friendly User Interface

According to the GDPR, the consent has to be given for the processing of personal data for one or more specific purposes. In case of new purposes, it is necessary to either get fresh consent specifically covering such new purpose or find a different legal basis for the new purpose.

---

[21] Big Data Value Association (BDVA), "Data protection in the era of Artificial Intelligence", 2019. Available at: https://www.bdva.eu/data-protection-era-artificial-intelligence-0 (accessed Jul. 29, 2022)

[22] DataVaults Consortium, D2.1 "Security, Privacy and GDPR Compliance for Personal Data Management", 2020 DataVaults Consortium, D2.3 "Updated DataVaults Security Methods and Market Design", 2021 DataVaults Consortium, D1.3 "DataVaults MVP and Usage Scenarios", 2021

Even when expressed through electronic means, the consent of the data subject should be preventive and unambiguous. It requires a statement or clear affirmative action of the data subject. For instance, these actions can consist of ticking a box in an online environment, the choice of technical settings for information society services, and any other statement or conduct clearly indicating the data subject's acceptance of the data processing activities.

In a personal data sharing platform, it is also necessary to ensure that, where consent is obtained through the use of a service-specific user interface (for example, within a given personal data app or the interface of an IoT device), the individual must be able to withdraw consent through the same electronic interface with undue effort and without detriment.

The EDPS Opinion 7/2015[23] outlines challenges relevant to data platforms entailing the sharing of personal data and that need to be addressed. It clarifies that in many big data environments "individuals cannot efficiently exercise control over their data and provide meaningful consent in cases where such consent is required. This is all the more so as the precise future purposes of any secondary use of the data may not be known when data is obtained: in this situation, controllers may be unable or reluctant to tell individuals what is likely to happen to their data and to obtain their consent when required".

The data collection and processing in such data platforms might be intended for multiple purposes and it is necessary to ensure the consent for all of these purposes (Recital 32 GDPR).

Recital 43 GDPR casts doubt on an approach based on one single consent form, broadly formulated as pre-emptively covering different future business models of the data controller.

Globalised, generic consent for multiple vague purposes risk to be assumed as not freely given and the question that arises is whether separate consent and the need for several, broken down consent requests are appropriate. This needs to be explored in the context of DataVaults, but also reflecting on the need to avoid "consent-fatigue" of a data subject.

As acknowledged by the Article 29 Working Party, a layered approach could be a possible solution, still providing all necessary information step by step and providing balancing means of user control, whilst being substantially different by the mere use of pre-ticked boxes: it is not necessary that the first layer of information is completely in-depth about the details of the processing. It should be explored if, for most of the cases (though not

[23] https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf

applicable to the special categories of personal data of Article 9 GDPR), an implicit consent (such as a shade going away after a few seconds and assumes "yes") could work, after the first general consent during the installation of the service. It should be likewise investigating which information needs to be given to the data subject in which layer.

Useful indications can be retrieved in the following GDPR Recitals:

1. Recital 32, which clarifies that it can be a written statement, including by electronic means, or an oral statement, if the data subject's behaviour clearly indicates his/her acceptance of the data processing. It is recommended that if the data subject's consent is to be given following a request by electronic means, such a request must be clear, concise, and not unnecessarily disruptive to the use of the service for which it is provided.

2. Recital 33, which states that, being often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection, data subjects should be allowed to give their consent to certain areas of scientific research (or parts of research projects) when in keeping with recognised ethical standards for scientific research. "Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose".

3. Recital 42, which states that "…For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment".

The data platform consent management policies need to ensure that the consent is:

1. "granular", capable of providing distinct consent options for distinct processing operations;

2. specific to "one or more specific" purposes, ensuring that the data subject has a choice in relation to each of them;

3. freely given, in the sense that the data subject should be able to exercise a real choice, without risk of deception, coercion, intimidation, or significant negative consequences if he/she does not consent;

4. informed, being the provision of information to data subjects prior to obtaining their consent necessary to enable them to understand what they are agreeing to, make informed decisions, and exercise control, and, in general, their rights (including to withdraw their consent). As noted, a layered approach could help in this regard;

5. separate from other terms and conditions;

6. "explicit", in case of processing of special categories of data, profiling activities or cross-border data transfers. Though in many cases, the term "explicit" could be interpreted as given in writing with a hand-written signature, in digital or online context like DataVaults, a data subject may be able to issue the required statement with other modalities (such as by filling in an electronic form, or by using an electronic signature).

These considerations are especially applicable to private data platforms, whilst for urban data platform, the personal data collection and/or use might also relies on other legitimate sources of the processing pursuant to Article 6 GDPR "Lawfulness of processing", in particular points: "(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, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child".

In case of public authorities, there might be a clear imbalance of power in the relationship between the controller and the data subject and other lawful bases for the processing could be, in principle, more appropriate. This has to be taken into consideration for the urban data platform relying on personal data use. Pursuant to the accountability principle, the existence of valid consent must be demonstrable by the data controller (accountability).

In strict correlation with this topic, a personal data platform or application also requires to adopt user and data protection friendly user interface (UI), capable of facilitating as much as possible the user control features and consent management in an easy manner. It should be capable of collecting consent and constraints/restrictions, providing appropriate options for user information and control, thereby enabling the data subject to easily consent and exercise his/her rights set forth under data protection legislation, at national and European level.

An important element to consider is the wide range of data sources and to pay special attention in case where it includes sensitive information in the sense of Article 9 GDPR.

A filter on those data categories could allow the UI to distinguish between consent requests on "normal" personal data and those involving sensitive data. It could be investigating whether introducing functionalities for automatically detecting when sensitive data (or particular subset of sensitive data, for instance, in the healthcare demonstrator) is collected, using machine learning techniques or other techniques and filtering such data.

The following challenges could occur and need to be addressed:

- managing consent in a fine-grained way (including, for instance, partial granting or withdrawal of consent in some circumstances);
- managing the own data and exercise data subject's rights in an easy way, for instance, as regards adding, deleting, and rectifying personal data, and including also the possibility to access additional information in case of a data breach;
- switching back and forth between different consent modalities, such as always requiring explicit consent for personal data sharing in some situations and opting for convenient assumption of implicit consent in other;
- ensuring data portability and exporting the own personal information (for instance, in an RDF format).

15.7 Risk-based Approach and Risk-Exposure Dashboard

Within a data sharing ecosystem, it is advisable, in relation to ethics risks and especially to those related to personal data collection and/or processing, to adopt a risk-based approach, following the current regulatory trend, as provided, for instance, by the GDPR (Recitals 75 and 76) and AI Act proposal.

This approach requires to consider the risk of varying likelihood and severity for the rights and freedoms of natural persons. Following this approach, it is therefore necessary to evaluate the ethics risks related to the data processing activities of the platform, assessing the particular likelihood and severity of each risk to data protection (or other ethical values), taking into account "the nature, scope, context and purposes of the processing and the sources of the risk". The assessment of the risk must be conducted in an objective manner to determine whether there is a "risk" or a "high risk", in order to let the data controller be particularly prudent to carefully consider their obligations when necessary. Such an approach requires consideration of what measures are appropriate in each case, depending on the scope, nature, context, and purposes of the processing concerned, as well as of the risks of varying likelihood and severity for freedoms and rights of individuals.

The more severe and likely the risks from the proposed processing, the more measures will be required to counteract such risks.

According to Recital 75, examples of potentially risky processing relevant to a platform enabling the exchange of personal data include: i) processing that may give rise to discrimination, identity theft, financial loss, reputational damage, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; ii) processing that might deprive data subjects of their rights and freedoms or prevent them from exercising control over their personal data; iii) processing of sensitive personal data; iv) processing for purposes of profiling; v) processing of personal data of vulnerable natural persons; vi) processing involving a large amount of personal data and affecting a large number of data subjects.

For operationalising the risk-based approach, the DataVaults project developed a specific tool and related service: the Risk Exposure Dashboard, displaying an individual's current and projected risk estimations, which are updated whenever a modification to the shared assets occurs. Such estimations and risk exposure metrics are calculated relying on the data assets the data owner has already shared, as well as on the data they intend to share, and taking into account all sharing aspects, such as anonymisation level and discoverability, as well as the information provided by the nature of the data itself. The calculation of the privacy risk exposure, based on previous knowledge and depending on the data already available and shared and specific metrics, will allow also being able to notify individuals of their privacy risk exposure from the DataVaults Cloud Platform through the DataVaults Personal App.

The Risk Management Service might represent a high-value powerful accountability tool for the fulfilment of the GDPR-compliant informed consent requirement and user control, strengthening the positioning on the market of a (urban and/or private) data platform embedding it within its architecture and offering it to the individuals to foster their inclination to share their personal information.

A dedicated "Sharing Risk Information" operation is, indeed, essential for raising the awareness of the individuals on the privacy exposure impact of sharing data assets.

15.8 Personas and Digital Twins

Depending on the defined data sharing configuration and selected user privacy level, different tools and techniques for privacy enhancement will be used, ranging from the integration of traditional obfuscation schemes such as

digital twins and user personas, to the use of trusted computing technologies (i.e., TPMs) as a central element for the provision of privacy-preserving signature schemes based on the use of Direct Anonymous Attestation.

It is interesting here to elaborate on some legal and ethical challenges and opportunities raised by the personas and the digital twins in relation to the personal data platform or, in any case, to urban data platform based on personal data for their operation and service provision.

In DataVaults, the individuals can select the preferred level of anonymisation for the data asset they are going to upload and share in the DataVaults Cloud Platform: their personal data can be shared without applying anonymisation (eponymous) or in anonymised way by implementing the digital twin generator or the persona group generator. More precisely, if the individual selects the anonymised sharing, depending on the individual's preference to upload and share as personal anonymised data (i.e., digital twin) or as grouped anonymised data (i.e., to become part of a persona group).

This is a very useful functionality related to the anonymisation features and level of the personal data sharing that should be available in any personal data platform.

As regards DataVaults, this is provided through the use of the anonymisation bundle, which, as regards personas generation, groups data coming from different individuals and processes them using statistical methods for creating an aggregated representation/model where the individual's data is obfuscated by being included in a large pool of similar data, the so-called persona.

In DataVaults, personas will be partially auto generated and presented to the data scientists prior to his/her analysis, based on certain similar aspects identified by the system (age group, location, interest, compensation requested, etc.). Though the DataVaults Cloud Platform, the data scientist will be provided with an engine for the creation of aggregated profiles composed of data assets from several individuals sharing certain similarities (generation of these personas).

The creation of such personas is based on the obfuscation and merging of data originating from multiple users with similar characteristics; therefore, it is paramount to preserve their privacy. Such personas are exactly aimed at preserving the privacy and anonymity of the indistinct individuals considered for the specific representation/model though, at the same time, they provide valuable information to data seekers. In DataVaults, it is up to the individual to decide whether to share personal data in this way: the individuals have indicated in the sharing configuration their intention to share data for the personas generation. In any case, their privacy is protected, as all data assets to

be shared under this condition, are appropriately anonymised prior to being transferred to the Cloud and being used in one or more personas.

One of the challenges that need further investigation, in this regard, pertains to the revoked consent for data assets used for building personas. All the data processing operations based on consent, which took place before the withdrawal, remain lawful but also that, in principle, any further processing of these data is prevented, if there is no other lawful basis justifying the continued retention and/or processing of the data. It is important to consider whether there is non-expired contract in place comprising such data assets: in that case, it is reasonable to conclude that the withdrawal can be exercised for the future without retroactive effect.

In relation to this issue, it is important to bear in mind different aspects: the individuals' right to withdraw consent anytime, the right to erasure/right to be forgotten and its boundaries (in consideration of the available technology, means, and possible reasonable steps), and the other legitimate grounds for personal data processing and the limits to their applicability, with possible switching from one legal basis to another (for instance, in case of urban data platforms), as well as the interest of the data seekers. The legitimacy and fairness of technologies need to be sought by promoting the balance between competing interests and the determination of the required level of protection for the personal information involved in these cases. However, another concern related to this regards the unlinkability of created user personas, in case of deletion of such selected data assets from any created user personas. In other words, in case some data assets are deleted from the personas, the unlinkability to the user identity from whom (obfuscated) data are also included in these personas should be preserved.

As regards the creation of personas, it has also to be further explored if this implies or not in the specific personal data platform concerned, some "profiling", in the meaning provided by GDPR and therefore whether Article 22 is applicable and, in case it is, if additional measures need to be taken. It needs to be clarified on a case-by-case basis whether the creation of the persona and its use imply or not an automated decision-making. It is important that the human intervention will be part of the task, especially in case some effects on the individuals could occur (such as exclusion/limitation from some service or from a data sharing contract).

On the other hand, when the data scientists create the merged persona, the current user privacy risk exposure, as calculated by the DataVaults Risk Assessment framework, should respect the privacy choices defined by the user (in the data sharing configuration): in other words, the quantified privacy risk exposure values need to be kept within the user acceptable boundaries.

Otherwise, the personal data platform should inform the user of appropriate actions to be taken for privacy enhancement.

Moving to the digital twins, first of all, it is useful to provide a snapshot of the concept. "A digital twin is a digital representation of a physical process, person, place, system or device". This concept, which emerged in the field of manufacturing domain, refers to digital simulation models that run alongside real-time processes[24] and it is conceptualised as digital replicas of physical entities, made possible by the use of technological breakthroughs as sensing, processing, and data transmission.

The digital twin concept is wide and can cover different aspects in different domains. For instance, there are urban scale digital twins, which are "that are used to simulate environments and develop scenarios in response to policy problems".[25]

The notion of urban scale digital twin has a central role within the field concerning smart cities design, and although there is not a commonly accepted definition of urban digital twins, the common denominator of the different definitions relies on the "bi-directional mapping relationship that exists between physical space and virtual space" for establishing "real-time connection(s) between the virtual and the real".[26]

The urban scale digital twins, besides useful for observing, recognising, and understanding the physical world, are also aimed at controlling and transforming it[27] since they entail the capacity to monitor activities in the city but even to use such data captured through monitoring for shaping more efficient and more sustainable cities and services in different areas, such as data concerning traffic and transportation, utilities provisioning, power generation, water supply, and waste management among other.

As acknowledged also by the DUET Project and the Living-in.EU Initiatives, "local digital twins can change the way cities are planned, operated, monitored and managed".[28]

---

[24] Grieves, M. (2014). Digital twin: manufacturing excellence through virtual factory replication. White paper, 1(2014), 1–7.

[25] Charitonidou, M. (2022). Urban scale digital twins in data-driven society: Challenging digital universalism in urban planning decision-making. International Journal of Architectural Computing, 20(2), 238–253. https://doi.org/10.1177/14780771211070005

[26] Deren, L., Wenbo, Y. & Zhenfeng, S. Smart city based on digital twins. Comput.Urban Sci. 1, 4 (2021). https://doi.org/10.1007/s43762-021-00005-y

[27] Tao, F., & Qi, Q. (2019). Make more digital twins. Nature, 573(7775), 490–491. https://doi.org/10.1038/d41586-019-02849-1

[28] Local Digital Twin - Living in EU. Available at: https://living-in.eu/groups/solutions/local-digital-twin (accessed Jul. 29,2022)

Within this overall debate around the urban scale digital twins and their future potentialities for the research on smart cities and their big data as well as, more in general, within the overall debate on digital twins, this chapter will refer only to the personal digital twins relevant in the framework of a data platform based on personal data and their exchange using the elaboration of the digital replication of individual human data. We can refer to them as personal digital twins, since they reflect an individual (habits, history, behaviour, and social interaction) and their personal data.

In particular, in the DataVaults project, the individual can configure the sharing anonymisation level by selecting the preferred level of anonymisation for the data asset they are going to share, ranging from sharing data without applying anonymisation (eponymous), to anonymise personal data at an individual level (digital twin) or, as already mentioned, to anonymise them at a group level making them available for the creation of personas. In case of selection of this data sharing configuration (digital twins), the DataVaults Cloud Platform shall generate the digital twin of an individual by anonymising and obfuscating personally identifiable data while preserving the valuable information enclosed in the data asset, through the use of the identity provided by another DataVaults component, the Identities Wallet. The individual is allowed to view at any time under which digital twin identities they have shared data anonymously with the DataVaults Cloud Platform. In an urban landscape, the personal data that can, potentially, be part of a personal digital twin, comprise both the small portion of data generated and captured by the individual (self-measurement), as well as, mainly, the data resulting from interaction of the individual with their environment, which will be likely captured by third parties.[29] In an urban ecosystem, the exploitation of the personal digital twins is consistent also with the citizen-centric approach of urban digital twins for the benefit of people themselves by ensuring that people have better experiences in complex situations and will also inform better infrastructure investment decisions.

Some of the ethical challenges potentially raised by the digital twins, for instance, based on data captured through Internet-of-Things-based sensing technologies have been initially explored by the narratives[30] and are illustrated below, though the issues are still open.

---

[29] Saracco R., Personal Digital Twins: What Data? – IEEE Future Directions, 2022. Available at: https://cmte.ieee.org/futuredirections/2018/01/16/the-rise-of-digital-twins/ (accesses Jul. 29, 2022)

[30] D. Helbing, J.A. Sanchez-Vaquerizo, "Digital twins: Potentials, Limitations and Ethical Challenges", Preprint, 2022.

This regards, for instance, the case of use of personal digital twins to run "smart cities". First of all, privacy and security issues might be entailed due, for instance, to the pervasive mass surveillance implied by ubiquitous measurements, or risk of new kinds of discrimination when the individual's social or medical status is measurable or known and can be used to determine their right to access services, facilities, opportunities, or other.

Of course, from an ethical point of view, there may be further concerns of undesired side effects.

Some of them are related to the nature of the human beings and the fact that people are often complex and adaptive to the changing environment: for instance, people can learn, exchange knowledge, have consciousness, are moved by goals changing over time, have emotions, and so on. Similar characteristics might pose particular challenges for creating digital twins and to tackle with such variables it would be necessary to collect and analyse massive amount of sensitive personal data in order to generate increasingly detailed digital twins and this raises privacy issues and the risk of promotion of a society oriented towards control (dataveillance).

There is the risk that application based on personal digital twins might interfere with individual thoughts, decisions and behaviours, human rights, and human dignity.

Other ethical concerns pertain, for example, on the risk of new forms of identity theft, abuse, and deception and how to mitigate them as well as the risk that people are entirely replaced by digital twins.

Running a city based on personal digital twin could be misused: for instance, by knowing individuals' strengths and weaknesses, there is the risk of tricking or manipulating everybody.[31] Furthermore, "a digital twin of society would also make it possible to determine how much one can pressure people without triggering a revolution, or figure out how to overcome majorities, how to break the will of people, and how to impose policies on them, which do not represent their will",[31] thereby undermining human rights.

A further concern regards the risk that personal digital twins are given greater opportunities and authority than human beings themselves, even though the digital representation of people and their desires could be biased, manipulated, or hacked. A personal digital twin and its data could be given more attention by the system/platform more than to humans, ignoring the opinion of the human the digital twin should represent.

---

[31] Isaak, J.; Hanna, M.J. User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. Computer 51, 8 (2018), 56–59. https://doi.org/10.1109/MC.2018.3191268

There is also the risk of over-simplifications and of neglecting details and human dignity and other hardly measurable aspects, therefore undermining one of the main strengths of social systems: their ability to self-adaptation, self-organisation and co-evolution, or, in other words, of a "technological determinism" of society.

In order to avoid that, people could be managed like things; it is, therefore, paramount in a highly networked, complex urban context characterised by data-driven and AI-empowered solutions, to prevent these risks to materialise by strongly relying on ethical mandates and soft law. We can mention, as examples, the Ethics Guidelines for Trustworthy AI and the UN's "Agenda 2030" with its 17 sustainability development goals (SDGs), as well as UNESCO's Recommendation on the Ethics of Artificial Intelligence,[32] as well as, more in general, the current regulatory reforms under development.

It is also critical that, rather than replacing individual preferences by automated machine decisions, to keep the individual's control on their data and on the decision made relying on them. This is what systems like DataVaults are directed to do, thereby minimising the potential misuse of powerful digital technologies while maximising benefits for the society.

15.9 Challenges Related to Smart Contracts, the eIDAS Regulation, and the Self-Sovereign Identity

In order to set, sustain, and mobilise an ever-growing ecosystem for personal data and insights sharing and to foster an enhanced collaboration between individuals and data seekers capable of rejuvenating the personal data value chain, it is key to secure value flow based on smart contracts safeguarding personal data ownership, privacy, and usage and attributing value to the ones who produce it. Interesting approaches of personal data management therefore make use of smart contracts and distributed ledger technology.

For the purposes of a personal data sharing platform, it should be investigated if and how to ensure the electronic identification and to get the verifiable credential (on the basis of a national digital identity), where necessary for accessing to online public services.

The eIDAS[33] Regulation states that the processing of personal data must be carried out in accordance with the GDPR and respecting its principle of

[32] UNESCO, Recommendation on the Ethics of Artificial Intelligence, 2021. Available at: https://en.unesco.org/artificial-intelligence/ethics (accessed Jul. 29,2022)

[33] Alamillo Domingo, I., "SSI EIDAS Legal Report - How EIDAS Can Legally Support Digital Identity and Trustworthy DLT-Based Transactions in the Digital Single Market", 2020.

confidentiality and security of processing: as clarified in its Recital 11, the authentication for an online service should concern processing of only those identification data that are adequate, relevant, and not excessive to grant access to that service online.

In case the platform concerned foresees to use electronic identification for its users, either natural or legal persons, this eIDAS Regulation can become applicable for its services and should be investigated especially in the context of the wallets and the smart contracts. Its electronic identification (eID) tools can be used for the identification of users, as they broadly offer enhanced security and accuracy, swifter, and less costly processes, while they may mitigate risk of fraud, identification theft, and legal challenges.

On the other hand, the concept of self-sovereign identity (SSI)[34] could also present advantages for the purpose of a personal data platform deployment and use and should therefore be investigated, including its compliance with eIDAS.

Sovrin[35] argued that the "self-sovereign identity (SSI) is a term used to describe the digital movement that recognises that an individual should own and control their identity without the intervention of administrative authorities. SSI allows people to interact in the digital world with the same freedom and capacity for trust as they do in the offline world". Furthermore, "Blockchain and SSI are natural complements, making the perfect symbiosis": the user is able to individually create and manage his/her identify thanks to the use of distributed ledger technologies (e.g., blockchain), without the involvement of a third party, but often making use of the "decentralised identifier" (DID) associated with an entity. Such entity using SSI to authenticate itself can be an individual (natural person), and, therefore, in this case, the DID usually relates to an identified or identifiable person (thus being personal data).

The SSI enables sovereignty for individuals over their digital assets and credentials, often by using digital wallets. In case the individual presents such assets and credentials to a third party to prove ownership, the public, decentralised, and immutable registry (such as a blockchain network) can be employed: the cryptographic proofs of the asset or credential were registered and are kept in a standardised and trustable way.

Available at: https://joinup.ec.europa.eu/sites/default/files/document/2020-04/SSI_eIDAS_legal_report_final_0.pdf (accessed Jul. 29, 2022)

[34] Allende Lopez, M., Self-Sovereign Identity: The Future of Identity: Self-Sovereignty, Digital Wallets, and Blockchain, 2020, http://dx.doi.org/10.18235/0002635

[35] Sovrin, Trust Assurance Framework, 2019. Available at: https://sovrin.org/wp-content/uploads/Sovrin-Trust-Assurance-Framework-V1.pdf (accessed Jul. 29, 2022)

Nonetheless, the question whether eIDAS is already suitable for SSI and blockchain technology is still open, as well as whether, on the one hand, the smart contracts could be considered electronic documents and, on the other hand, the means used to sign blockchain transactions could be considered electronic signatures, with all the legal consequences it implies. Some scholars[34] argue that the eIDAS Regulation will need some adjustments to become the legal and trust framework for SSI in the European Union: it was created as a legal framework supporting a digital identity metasystem mainly based on delegated authentication, which is more limited than the self-sovereign approach which enables, among other things, pseudonymity and selective disclosure mechanisms.

In the US system, the situation is not exactly the same and some authors underlined that blockchain transactions can constitute, or evidence, electronic signatures and that, virtually, all transactions stored on a blockchain, and retrievable in perceivable form, constitute an electronic record under the US law.[36,37]

In conclusion, it is not fully clear whether for the purposes of a personal data sharing platform, it should be ensured (and how) the electronic identification and it should be necessary to get the verifiable credential (on the basis of a national digital identity), where necessary for accessing to online public services.

On the other hand, from the viewpoint of the smart contract itself, often used in the personal data platform to give the compensation for the sharing of own personal data, the debate is still ongoing whether and to what extent and conditions, these can give rise to legally binding and enforceable contracts and whether this necessarily requires the identification of the individual pursuant to eIDAS.

The smart contract satisfies the elements of a contract under several national laws, such as Spanish Civil Code, and, therefore, smart contract code represents a valid mechanism to define the parties' contractual rights and obligations as a matter of contract law in many jurisdictions. Therefore, "under certain circumstances, and if so decided by the parties, smart contracts can fulfill the elements of a legally binding contract under common law and civil law systems".[38] Though the parties may act pseudonymously,

---

[36] U.S. Government, Public Law 106 - 229 - Electronic Signatures in Global and National Commerce Act (ESIGN), 2000. Available at: https://www.govinfo.gov/app/details/PLAW-106publ229

[37] Therefore, under certain legislation, blockchain platforms may constitute or store electronic records and electronic signatures and thus may be used to evidence, or give effect to, electronic or smart legal contracts

[38] Smart Contract Alliance, "Smart Contracts: is the Law Ready?" 2018. Available at: https://digitalchamber.org/smart-contracts-whitepaper/ (accessed Jul. 29, 2022)

it is necessary a link (including off-chain) to their real identity to provide for valid consent, which is a crucial element of a contract under several national systems. However, even if its deployment does not give rise to a legally binding contract, the smart contract may still affect legal relations (either between the parties or with third parties) and therefore may have legal effects.

At the same time, both smart contracts and conventional natural language contracts can coexist in relation to the same (or related) subject matter and create together the entire legal framework within which a smart contract operates. This is the case of the so-called "external smart contract", where "the code does not form the entirety of the parties' legal agreement, but merely automates the performance of some of its terms".[37] The code merely automates the performance of some of the conventional contract's terms. In this case, the legal relationship is intended to be governed by the natural language version of the contract, rather than by the code. In the internal model, on the contrary, the code could either encompass the entire agreement between the parties, or, alternatively, could form only an integral part of the legally binding contract (rather than the entirety of the contract), and would supersede any other clauses written in natural language: the code would be given legal effect and is an integral part of the agreement.

Principally, it is necessary to refer to the governing law applicable to the smart contracts in order to determine whether these give rise to legally binding contracts, whether personal identification is necessary or not according to eIDAS, as well as to evaluate the effects of the DTL/blockchain, and, ultimately, to ensure that the model chosen meet local law requirements. However, considering that the DataVaults offering can constitute an electronic registered delivery service according to eIDAS (Article 3, (36) eIDAS), such regulations and the obligations established for the providers of such services have to be taken into account in the design, development, and future use of personal data platform.

15.10 DataVaults as a Flagship Initiative for Personal Data Sharing Under User Control and Benefitting All the Actors Involved: Experiences and Lessons Learnt

The DataVaults project is directed to rejuvenate the personal data value chain by delivering a framework and a platform having personal data, coming from diverse sources (wearables, web APIs, smart home sensors, personal data records, etc.) in its centre. Secure, trusted, and privacy-preserving mechanisms have been designed to allow the individuals to take ownership and control of their data and share them at will, through flexible data sharing

solutions and fair compensation schemes with other entities (companies, public bodies, or other organisations).

DataVaults aspires to become one of the flagship personal data platforms in the European landscape, characterised by full respect of GDPR provision and satisfaction of the privacy and trust consideration of users, with a novel, fair, and understandable value compensation mechanism to data owners.

Therefore, the whole Consortium paid great attention to tackle any potential ethics issues raised by the platform's validation and future operation in order to give rise to a technology respectful of the data subjects' privacy and dignity and capable of prioritising human wellbeing and flourishing.

For this purpose, they elaborated the DataVaults Ethical Policy at the beginning of the project and adhered to it, conducted an in-depth regulatory review, elicited a set of legal and ethical requirements and related guidelines and recommendations for the overall DataVaults cloud-based platform and its components, as well as the Personal App and the demonstration activities. They also followed (and are going to conduct again at the end of the project) an Ethics and Data Protection Impact Assessment methodology, besides capturing the citizens' perspective through dedicated interactive channels.

The following outlines the activities performed and outcomes achieved by the Consortium in order to adhere to the highest ethical standards and comply with the legislation, *in primis* the Data Protection Law (especially the GDPR).

15.11 Case Study: Approach and Legal and Ethical Requirements for DataVaults Ethical Policy

The DataVaults Ethical Policy has been conceived and implemented to ensure the legitimacy and fairness of project technologies and demonstrations. It depicts the ethical procedures and responsibilities, including those relevant for human participation and personal data collection and processing in the demonstrators, besides identifying the oversight responsibilities (with the appointment and involvement in project's activities of the DataVaults Ethics & Data Protection Officer and DataVaults Ethical Board) and setting the basis for the comprehensive Data Protection Impact Assessment methodology used during the demonstrators operations. The Policy also drew the roadmap for the implementation of ethics-related activities within the project.

The Policy is driven by the Fairness & Privacy-by-Design-and-by-Default enriched with the Protection Goals Approach, adopted for analysing the composite regulatory landscape, for deriving the legal and ethical requirements, as well as for providing recommendations and insights on how

to face the identified boundaries and constrains. This approach is functional to ensure that the research activities, results, and validation activities are legally compliant and ethically sound. First of all, GDPR itself sets forth among the principles relating to processing of personal data the so-called "Fairness Principle". Fairness, which can be explained through the concepts of loyalty and good faith to be respected in all the steps of any personal data processing, requires that personal data must be used in a fair way, avoiding to process in a way that is unduly detrimental, unexpected, or misleading to the individuals concerned or that could have adverse impact on them. The "Fairness by Design" has identified a straightforward requirement for DataVaults technology in order to ensure that individuals' privacy and real control over their data. The procedural dimension of the fairness entails the effective exercise of the data subjects' rights (rectification, erasure, object, etc.), whilst its substantive dimension implies moving towards the equal and just distribution of benefits and costs, without unfair bias, discrimination, and stigmatisation for individuals and groups. This is linked with another high-level ethical requirement, the "sharing the wealth" paradigm,[39] aligned with the vision of a win–win data sharing ecosystem fostered by the Big Data Value Association[40] as a contribution to help unlock the social value of personal data, going beyond user consent for fostering individual human empowerment and flourishing, as well as the common good of society and businesses' interests. The DataVaults Consortium followed this approach and directed its efforts to promote the alignment of its research and outcomes with social needs and expectations, also in view to strengthen the societal uptake of DataVaults cloud-based platform, given that high ethical standards generally imply public trust.

This approach might be particularly relevant also in an urban and public environment since it supports the identification, on a case-by-case basis, of the proper balance between competing interests and encompasses societal fairness, based on equal opportunities and on the need to avoid that individuals are deceived or unjustifiably impaired in their freedom of choice. In view of fully ensuring the fairness of the technological artefact, it is advisable

[39] Bormida, M.D., "The Big Data World: Benefits, Threats and Ethical Challenges", Iphofen, R. and O'Mathúna, D. (Ed.) Ethical Issues in Covert, Security and Surveillance Research (Advances in Research Ethics and Integrity, Vol. 8), Emerald Publishing Limited, Bingley, pp. 71–91, 2021. https://doi.org/10.1108/S2398-601820210000008007

[40] BDVA Position Paper "Towards a European Data Sharing Space - Enabling data exchange and unlocking AI potential", 2019. Available at: https://www.bdva.eu/sites/default/files/BDVA%20DataSharingSpace%20PositionPaper_April2019_V1.pdf (accessed Jul. 29, 2022)

to investigate several dimensions and take into account different perspective, for instance, focusing the attention on different kinds of compensation mechanisms, besides data monetisation schemes, such as other rewarding incentives, so that the different brackets of the population will be encouraged to share data.

The chosen approach strongly relies also on human-centricity. Exploring and deepening individuals' viewpoint was considered essential by the Consortium for effectively adhering to the chosen Ethics, Fairness & Privacy-and-Security-by-Design-and-by-Default Approach and for contributing to build a win–win data sharing ecosystem.

For this reason, in order to capture citizens' perspective, expectations, needs, and concerns on personal data sharing, the Consortium conducted a survey directed to individuals in their role of data owner. Results from the survey provided an understanding of:

- attitudes towards personal data sharing;
- data retrieval, storage, and deletion;
- privacy preservation on the shared data;
- compensation mechanisms;
- control and informed consent.

These results, as well as of the other stakeholder engagement activities, were key for driving the design, development, and deployment of the Personal Data Platform and App planned in DataVaults, whilst also providing important indications for the future progress of the Personal Data Market in Europe.

This attention to the individual is also consistent with the EC strategy and vision[41] directed to put people first in developing technology and to promote European values and rights in any design, development, and deployment of the technology in the real economy.

The Ethics Board offered guidance, advice, monitoring, and recommendations for future work, mainly with respect to ethics and privacy, whilst the Ethics and Data Protection Officer (EDPO) mainly supported the partners in ethics compliance and in the handling and management of personal data in accordance with the existing provisions of GDPR and other relevant EU and national legislations, providing guidance and advice, training of researchers, assisting in ethics risk assessment, and supporting in relation to the Ethics and Data Protection Impact Assessments.

[41] See, for instance, COM/2020/66 final, "A European strategy for data" (ref. number 4).

On the other hand, the Policy also drew the ethical procedures for the human involvement and personal data collection and handling in the demonstration activities, since individuals will be involved in the pilots and their personal data, coming from diverse sources (sensors, IoT, wearables, data APIs, historical data, social network data, activity trackers, health records, demographic profiles, etc.) were gathered, processed, and shared. These procedures include those used to identify/recruit research participants, as well as the high-level description of the informed consent procedures for the participation of humans and personal data collection and processing, including also the sample of the informed consent/assent forms and information sheets distributed to the research participants. Such samples were fine-tuned and adapted by each relevant demonstrator, taking into account the specific context, technologies, and scenarios, with advice available from the EDPO where required.

The Ethical Policy guided the ethics-related work carried out by the project partners, both in the technical work-packages where the technological assets are designed and developed, and in the demonstration activity, where the results are assessed.

In particular, the Policy is strongly interrelated with the legal and ethical requirements elicitation. At an early stage of the project, the legal and ethical requirements for the design, development, and validation of DataVaults cloud-based platform and Personal App were set, alongside the future operation of them, clearly laying out a first guideline for legal compliance and ethically sound activities and results, without forgetting checkpoints. The initial requirements list was extended taking into account the enriched legal review, where additional areas of law were analysed, as well as the regulatory reforms under development and their accompanying documents.

All these requirements were elicited adopting a systematic and holistic approach, driven by Fairness & Privacy-by-Design-and-by-Default enriched with the Protection Goals method and relying on the analysis of the regulatory landscape and the factual analysis of the privacy-relevant properties and personal data collection, processing, and sharing in each service and tool, including details on the data categories, data sources, and purposes of processing.

Some of the requirements are binding (when directly deriving from the legislation, such as GDPR), whilst others, where not directly imposed by the legislation, have to be interpreted more than recommendations or preferable requirements. Some requirements, being quite challenging, need to be assessed with a certain degree of flexibility, taking into account the state-of-the-art of the technological developments and the risk-based approach

fostered by GDPR itself: in other words, this demands for a certain degree of flexibility in the assessment of the adequateness of measures and technological solutions, to be specifically established on a case-by-case basis, considering a set of circumstances rotating around the severity of the risks and the reasonable efforts to face with them.

The nature of the requirement is clearly stated in the description of each of them and they are provided in a table format, in order to facilitate the quick understanding and reference to them by the technical team. Furthermore, in order to promote the operationalisation of the requirements, additional notes, recommendations, and guidelines were provided.

The fulfilment of the requirements regarding the DataVaults technology ensures that it is legally compliant, ethically sound, and gives rise to a trusted, secure privacy-friendly enhanced (holistic) data sharing solution. The assessment of the compliance with these requirements was conducted in a triple iteration, respectively, concerning the alpha, beta, and final version of the DataVaults technology (in particular, the platform).

15.11.1 Ethics and data protection impact assessment methodology

An important element of DataVaults Ethical Policy was the definition and implementation of the Ethics and Data Protection Impact Assessment Methodology for the demonstrator cases, functional to the assessment of risks for individuals' rights, freedoms, and wellbeing, for ensuring compliance with the data protection law (GDPR and national regimes), and ethical mandates.

This methodology regarding the risks for the personal data was conducted following the indications of Article 35 section 1 GDPR, taking into account the nature, scope, context, and purposes of the processing operations in each demonstrator in view of evaluating their impact on the protection of personal data, to identify and reduce the data protection risk[42] and the likelihood of privacy harms to individuals, as well as to identify and put in place the appropriate technical and organisational measures to tackle with/mitigate such risks.

A model inspired by the ISACA Model[43] was adopted for conducting such data protection assessment, which maps the 14 ISACA privacy principles

[42] The concept of risk is clarified in Recitals 75–79 of the GDPR.

[43] ISACA, "GDPR Data Protection Impact Assessment", 2017. Available at: https://isaca-gwdc.org/wp-content/uploads/2018/01/GDPR_res_eng_0917.pdf (accessed Jul. 29, 2022)

to the specific GDPR requirements and therefore allows an easy integration with any additional privacy impact assessment (PIA) standards required for other possible multiple privacy principles relevant for the demonstrators. Furthermore, this model is well aligned with the protection model focused on individual privacy and user control and efficaciously supports accountability, representing a useful instrument for the demonstrators to showing commitment and due diligence in taking adequate actions to ensure full compliance on an ongoing basis.

The demonstration sites elaborated their own EDPIA in conjunction with the respective technological supporting partners and the overall technical team of the project. It considered the specific technologies (like services and components) relevant to their context, the data lifecycle and each use cases scenarios, as well as their own privacy and security policies/practices.

Furthermore, in order to adequately cover also the ethical dimensions and to assess to what extent the principle of fairness has been operationalised in each of the demonstrator, the model inspired by the ISACA scheme was enriched with the Data Ethics Canvas.[44] This tool was elaborated by the ADAPT Centre for Digital Content Technology on the basis on the original Business Model Canvas by Alex Osterwalder.

This model consists in a useful tool giving a higher level framework to develop ethical guidance that suits any context and to assess the ethical implications of any project, thereby allowing to be more trustworthy with data processing.

The Data Ethics Canvas is capable of helping those who collect, share, and use data in identifying and managing ethical uses, both at the start of the initiative which imply data collection/processing and throughout[45] the implementation of the initiative. On the other hand, thanks to it, the data seekers are supported in putting in place practices ensuring that the way the data is collected and used is trustworthy and ethical, beyond legal compliance.

The Open Data Institute's Theory of Change is strongly consistent with the DataVaults' vision and with the Citizen Control of Personal Data Initiative

---

[44] Reijers, W., Koidl, K., Lewis, D., Pandit, H.J., Gordijn, B., Discussing Ethical Impacts in Research and Innovation: The Ethics Canvas. In: Kreps, D., Ess, C., Leenen, L., Kimppa, K. (eds) This Changes Everything – ICT and Climate Change: What Can We Do?. HCC13 2018. IFIP Advances in Information and Communication Technology, vol 537, 2018. Springer, Cham. https://doi.org/10.1007/978-3-319-99605-9_23

[45] Open Data Initiative (The ODI), "Helping organizations navigate ethical concerns in their data practices", 2017. Available at: https://theodi.org/article/the-data-ethics-canvas-2021/ (accessed Jul. 29, 2022)

within the Smart Cities Marketplace – Citizen Focus Action Cluster: "We want people who steward data, and people who create things with it, to act in ways that bring about positive impacts. Ethical use of data helps to improve trust and bring about the best economic and social outcomes. We want to avoid a future where data is feared or hoarded. We want data to work for everyone".[46]

The Ethics and Data Protection Impact Assessment was conducted in each project's pilot through a questionnaire comprising elements coming both from the ISACA Model and from the Data Ethics Canvas. Strong reference was made, besides internal own policies, to the legal and ethical requirements set by the project itself. The EDPIA represented a key tool for ethical assessment and compliance in DataVaults and can be easily replicable, with the necessary adaptations, for use in other contexts like the public sphere.

15.12 Conclusion

In view of strengthening the development and growth of the data economy also in relation to personal data, it is key to foster the adoption of trusted and secure personal data platforms capable of handling back control over the use of personal data to individuals giving them actual benefits, not-necessarily financial. Future efforts should be directed towards building a win–win data sharing ecosystem in order to unlock the social value of personal data, going beyond user consent for fostering individual human empowerment and flourishing, as well as the common good of society and businesses' interests. In alignment with the EC's vision of personal data sharing that includes benefits for all the actors in the value chain, trusted, secure, and value generating data management and sharing platforms for personal data should be encouraged to the extent that they allow stakeholders' collaboration for supporting their own goals and operations, as well as allowing further stakeholders, such as the local communities and local authorities, to offer new socially and environmentally sustainable solutions and business models.

In this environment, on the other hand, the technologies should move to regain the trust of individuals when it comes to data sharing, leaving the control in their hands for deciding how, how much, and in which manner they would like to share their data, whilst at the same time guaranteeing their privacy and with adequate security levels, as well as ensuring

[46] Open Data Initiative (The ODI)– Our theory of change. Available at: https://theodi.org/about-the-odi/our-vision-and-manifesto/our-theory-of-change/ (accessed Jul. 29, 2022)

fair share of the value that their data generates, also in case of secondary operations.

In other words, human-centricity should be at the centre of the future technological developments and their operation when it comes to data sharing. Prioritising human wellbeing and fundamental rights and putting people first in the data-driven economy are expected to contribute to rebuild public trust and, therefore, societal acceptance of such innovations. This is also aligned with the Communication "2030 Digital Compass: The European Way for the Digital Decade".[47] Its Vision for 2030 relies on empowered citizens and businesses: "the European way to a digitalised economy and society is about solidarity, prosperity, and sustainability, anchored in the empowerment of its citizens and businesses, ensuring the security and resilience of its digital ecosystem and supply chains" with four cardinal points for mapping the EU's trajectory.

Personal data sharing platforms, like DataVaults cloud-based platform, capable of fully embracing this vision and the promotion of the EU's fundamental values (including protection of privacy) are expected to contribute to the creation of a single market for data that will ensure Europe's global competitiveness and data sovereignty. This will allow an increased amount of data made available for use in the economy and society, but at the same time safeguard individuals by effectively empowering them to exercise their rights with regard to the use of the data they generate and to decide at a granular level about what is done with their data, moving towards "personal data spaces".

[47] COM/2021/118 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "2030 Digital Compass: the European way for the Digital Decade". Available at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118