1 Access

1.1 Access to data: the two regulatory dimensions

Data access is a crucial element of contemporary European policy and regulation of digital markets. In late 2020, the European Commission issued a proposal for a Regulation on a European Data Governance Act,[1] which defines data access as the 'processing by a data user of data that has been provided by a data holder, in accordance with specific technical, legal, or organisational requirements, without necessarily implying the transmission or downloading of such data'.[2]

Data sharing is conversely related to the 'the provision by a data holder of data to a data user for the purpose of joint or individual use of the shared data, based on voluntary agreements, directly or through an intermediary'.[3]

In respect of data access a vertical and a horizontal regulatory dimension can be distinguished.

The first one regards access to data and related processing information by single data subjects vis-à-vis data controllers. From this perspective, access rights are a substantiation of the principle of transparency and are an essential means for the protection of data subjects' fundamental rights, first of all the fundamental right to data protection. The horizontal perspective relates to access to data among third parties, such as other businesses or public institutions. From this perspective, thus, access regimes and corresponding rights advance the free flow of personal data within the internal market for the ultimate promotion of market innovation objectives.

Individual access rights regarding personal data are provided by the General Data Protection Regulation (GDPR).[4] The same Regulation also governs transfers of personal data among stakeholders, setting relevant conditions and limits to it. The European framework sets further conditions for access to non-personal information and public sector data.

1.2 The vertical perspective: data subjects' access to personal data

Data subjects have the right to access the personal data that are being processed and a series of other information regarding the nature and the features of ongoing processing operations. Under Article 13(2)(b) and Article 14(2)(c) GDPR data controllers must inform data subjects about the 'existence of the right to request from the controller access' to such information.

The right to data access is envisaged under Article 15(1) GDPR, affirming that the 'data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to personal data'. In addition to the right to personal data, the right to access encompasses a variety of other types of information regarding 'the purposes of the processing'; 'the categories of personal data concerned'; 'the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations'; the period of storage 'and, if not possible, the criteria used to determine that period'; 'the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing'; 'the right to lodge a complaint with a supervisory authority'; the source of collection of personal data in case the data are not collected from the data subject; 'the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject'.

As recital 63 GDPR specifies, moreover, for the satisfaction of data subjects' right to data access, data controllers should be able to 'provide remote access to a secure system which would provide the data subject with direct access to his or her personal data'.

As opposed to the notification duties borne by data controllers under Articles 13–14

[1] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act)' COM(2020) 767 final.
[2] Ibid., art. 2(8).
[3] Ibid., art. 2(7).
[4] European Parliament and Council Regulation 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

GDPR, the right to access must be actively exercised by the data subject through a specific request.

The request can be forwarded at any time, with no deadline, also after an automated decision has been made. In these regards, however, it is still an object of debate if, in case the request is forwarded after an automated decision has been made, the right to access would grant also an *ex post* explanation of the consequences of specific decisions that are already reached. Against this interpretative option, it should be noted that the provision refers only to 'envisaged consequences' of processing activities: this wording seems to the contrary to suggest that the right to access is circumscribed to the possible consequences of the automated decision-making before the processing occurs.

In the case of an access request, the controller shall provide, as established under Article 15(3) GDPR, a copy of the personal data that are being processed. Where the data subject requires more copies, the controller can charge a fee that is based on administrative costs. Access requests can also be made through electronic means. If this is the case, the controller shall provide the requested information in a commonly used electronic form.

Through the exercise of the right to access, the data subject is able to review the lawfulness of data processing and enact legal remedies. This is expressed under recital 63 GDPR, which states that 'a data subject should … exercise that right … in order to be aware of, and verify, the lawfulness of processing'. The exercise of the right to access under Article 15 GDPR, thus enables the data subject to actively exercise his/her rights, in particular the right to rectification, under Article 16 GDPR; the right to erasure under Article 17 GDPR; the right to portability under Article 20 GDPR.

In these regards, the right to data portability consisting in the data subject's right to transfer his/her personal data to another controller, implies as the same Article 20(1) GDPR clarifies, data subjects' right to receive their personal data in a structured, commonly used and machine-readable format.

From the data subjects' perspective, the ability to transmit personal data to another controller is a direct expression of their fundamental right to informational self-determination to which the right to data protection is inherently connected. A further corollary of the right to data portability, is related to the stimulation of data mobility and thus sharing among different platforms, upon the condition of data subjects' stimulus.

The general right to data portability has been further specified in the banking sector under the Payment Service Directive 2 (PSD2),[5] establishing under Article 67 the payment service users' right to access its account information.

Businesses' and public entities' access rights to data are to be more broadly contextualised in the Digital Single Market's free flow of information initiative and in the 'European Strategy for data'. In this different horizontal perspective, access rights are enshrined in the GDPR, in the Regulation regarding the free flow of non-personal data,[6] as well as in the Open Data Directive,[7] regarding public sector information.

1.2.1 Data sharing in European policy

Data access and sharing has been increasingly considered as a fundamental engine for the maximisation of the 'growth potential of the digital economy' and of the efficient employment of data in the digital European economy. Over the last years, the relevance of data sharing has been increasingly stressed at policy level, where a paradigm shift has been called upon within the framework of the free flow of information initiative, which has become a fundamental pillar in the development of the Digital Single Market Strategy. In this context, the European Commission has very recently considered the phenomenon of the sharing of privately held data among businesses (B2B), of governmental data to businesses (G2B), of business data to governments (B2G), and ultimately among public authorities.

The relevance of data sharing in these various forms has been placed at the heart of the latest European strategy for data, as centred

[5] Council Directive 2015/2366/EC of 25 November 2015 on payment services in the internal market amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Council Regulation (EC) 1093/2010/EC, repealing Directive 2007/64/EC [2015] OJ L 337/35.

[6] European Parliament and Council Regulation 2018/1807 of 14 November 2018 on a framework for the free flow of non-personal data in the European Union [2018] OJ L 303/59.

[7] Council Directive 2019/1024/EC of 20 June 2019 on open data and the reuse of public sector information [2019] OJ L 172/56.

on businesses' contractual freedom. In the new strategy, the Commission reaffirms the importance of informing future regulatory and policy actions regarding data, upon the principle of 'as open as possible, as closed as necessary', which promotes data reusability and analysis across different sectors of the economy.

In this respect, specific principles for the encouragement of data sharing among the above-identified stakeholders have been outlined. More precisely, the European Commission's Communication 'Towards a Common European Data Space' and the accompanying working staff document providing Guidance on Sharing Private Sector Data in the European Data Economy introduce general principles addressing contractual freedom in data sharing, respectively related to transparency, shared value creation, respect for commercial interests, ensuring undistorted competition, minimisation of data lock-in, proportionality and purpose limitation in the use of private sector data.

The underlying goal of these principles is to 'ensure fair markets for IoT objects and for products and services relying on data created by such objects'. Conversely, B2G data should conform to the principles of proportionality in the use of private sector data, purpose limitation, 'do no harm', conditions for data reuse, mitigate limitations of private sector data and ultimately transparency and societal participation.

Although the European policy regarding data accessibility has mainly focused on non-legislative measures setting the best conditions for economic actors to exercise their freedom of contract, there have also been more direct regulatory interventions, such as those that have led to the Regulation on the free flow of non-personal data and the Open Data Directive.

The Proposed Data Governance Act complements the Open Data Directive, by introducing new rules regarding the sharing of data sets held by public sector bodies, when the data are 'subject to the rights of others', as intellectual property and data protection rights.

In addition to this, the proposed Data Governance Act establishes new mechanisms of data sharing based on 'data altruism', which is defined under Article 2(10) of the proposed Regulation, as 'consent by data subjects to process personal data pertaining to them, or permissions of other data holders to allow the use of their non-personal data without seeking a reward, for purposes of general interest, such as scientific research purposes or improving public services'. Organisations intending to share data for data altruistic purposes need to be entered in a register of recognised data altruism organisations.

Ultimately, the proposed Data Governance Act regulates data sharing service providers, which perform intermediating tasks in the sharing operation between a data holder and a data user. As stated under Article 9(1)(a) of the proposed Regulation, data intermediaries shall make available technical or other means enabling the sharing, as the 'creation of platforms or databases enabling the exchange or joint exploitation of data, as well as the establishment of a specific infrastructure for the interconnection of data holders and data users'.

Data sharing practices among different economic stakeholders are moreover subject to the GDPR's provisions. As Article 2(2) of the Regulation on the free flow of non-personal data and Article 1(4) of the Open Data Directive state, the application of the GDPR prevails in the case of mixed data sets.

1.2.2 Third parties' access to personal data

Access to personal data sets by a third party amounts to a further processing operation for the data holder and thus requires a lawful basis under the GDPR. In this respect, Article 6(4) GDPR establishes that further processing operations of personal data do not require a different basis in addition to the one relied on for the initial collection of personal data in case the purpose of the processing operation is compatible with the initial processing purpose. Compatibility is to be assessed in respect of various factors such as the context in which the data has been collected, the nature of the data, the consequences of the further processing for the data subjects, the existence of adequate safeguards.

The compatibility rule thus permits the access to personal data by a third party, but in very limited circumstances. Conversely, as established by Article 6(4) GDPR, in the absence of compatibility between the purposes of initial collection and of access of the data by a third party, the further processing of the personal data is possible only if the data subject has given its consent to the sharing of data or the controller has a legal obligation of rendering collected data accessible.

Different considerations need to be made in respect of the subject who accesses personal data sets. Indeed, in accordance with the principle of separate justification, the recipient also needs to have a lawful basis for accessing personal data sets. Contrary to what occurs for the original data controller, the data recipient can rely on any of the lawful bases under Article 6(1) GDPR, which are, apart from data subjects' consent, the performance of a contract to which the data subject is party, the protection of a vital interest of the data subject, the processing is necessary for the exercise of a legitimate interest of the same third party, if data subjects' fundamental rights and freedoms do not override this same interest.

Apart from the legal grounds for access to personal data by third parties established under Article 6(1) GDPR, European data protection law provides a further ground for data access under the so-called research exemption. This research exemption is to be found in the combined reading of Articles 5(1)(b), 6(1), 6(4) and 89 GDPR. In particular, Article 5(1)(b) GDPR provides that the processing of personal data for statistical and research purposes is to be considered per se compatible with the initial processing.

Operationally speaking, this means that if it is for research purposes, access to personal data by third parties for statistical or research purposes is always lawful, provided some conditions are fulfilled by data controllers. In the GDPR's system, the processing of personal data for research purposes is indeed related to a special data protection regime, which entails significant derogations to ordinary data subjects' rights and controllers' obligations and at the same time requires the enactment of adequate safeguards for the protection of data subjects' rights in the context of data-driven research projects.

The derogations in the case of research-oriented processing activities, first of all, invest fundamental data protection principles, such as the principle of storage limitation under Article 5(1)(e) GDPR and the principle of purpose limitation under the combined reading of Articles 6(4) and 5(1)(b) GDPR.

Also, substantial data subjects' rights as the right to be forgotten under Article 17(3) GDPR and the right to be informed under Article 14(5)(b) GDPR can be restricted where the exercise of these rights undermines set research objectives. Member states' laws can provide further derogations for research processing activities, as established under Article 89(2) GDPR.

The above-cited derogations, however, are counterbalanced by the requirement under Article 89(1) GDPR for data controllers to enact appropriate safeguards for the protection of the rights and freedoms of the data subject, encompassing, in particular, technical and organisational measures assuring compliance of processing activities with the principle of data minimisation. A first relevant safeguard is provided by the same Article 89(1) GDPR, referring to pseudonymisation of research data. Further safeguards for personal data accessibility in the context of collaborative research projects will have to be defined by sectoral codes of conduct and guidelines issued by national authorities.

A further provision regarding access to personal data is to be found in Article 20(2) GDPR establishing data subjects' right to have their personal data transferred from one controller to another, provided that consent is given for this operation and that it is technically feasible. Also from this further perspective, the PSD2 has established under Article 36 that providers of payment initiation services and the providers of account information services' right to access the payment account information of the users of their services, provided they have explicitly consented to such access.

For these purposes, banks are under an obligation to make the transferability of the account information technically feasible (recital 93 of PSD2), in particular through the use of open application programming interfaces (APIs). This specific obligation regarding technical interoperability is implied but not directly expressed in the GDPR's right to data portability under Article 20(2) GDPR.

1.2.3 Third parties' access to non-personal data and public sector data

The policy principles established by the European Commission regarding data sharing have been substantiated at regulatory level in the Regulation on the free flow of non-personal data and the Open Data Directive, respectively regarding non-personal and public data. Both regulatory frameworks highlight the importance of research data and their transferability for the ultimate purpose of creating the right market conditions for innovation. In particular, the two frameworks place particular emphasis

on the value of access and transferability of research data, in consistency with the paradigm of open science and innovation, aiming to foster the interaction between research results and market innovation objectives.

The Regulation on the free flow of non-personal data establishes a general principle of free movement of non-personal data, which can only be restricted by national authorities on grounds of public security in compliance with the principle of proportionality (Article 4(1)). Article 6(1) of the same Regulation encourages, in accordance with a self-regulatory approach, the adoption of codes of conduct, providing best practices for facilitating the 'porting of data in a structured, commonly used and machine-readable format including open standards formats'.

Following a similar approach, the new Open Data Directive expressly considers research data under Article 10 stating that 'member states shall support the availability of research data' on the basis of 'open access policies, following the principle of "open by default" and compatible with the FAIR principles'. The Directive thus leaves to member states the definition of access regimes regarding public data.

As can be derived from the cited provisions, both the Regulation on the free flow of non-personal data and the Open Data Directive place great emphasis on data accessibility of both non-personal data and public generated data. These frameworks defer the concrete implementation of access regimes regarding these two types of data to codes of conduct and national legislation.

Differentiations in applicable access regimes could hamper data transferability across both different economic sectors and member states.

The proposed Data Governance Act ultimately provides a harmonised framework for access regarding public sector data, which is protected on grounds of commercial confidentiality; statistical confidentiality; protection of intellectual property rights of third parties; protection of personal data.

Public sector bodies can engage in sharing operations regarding such data, subject to specific conditions set out under Article 5 of the proposed Regulation. In particular, public sector bodies shall make publicly available the conditions for allowing data reuse.

These conditions shall be non-discriminatory, proportionate and objectively justified with regard to categories of data and purposes of reuse and the nature of the data for which reuse is allowed. These conditions shall not restrict competition in the internal market. Public sector bodies should also assure the integrity of the functioning of the technical systems of the secure processing environments used.

1.3 Ad hoc sharing obligations under competition law

Already in 2017, the European Commission was acknowledging that in case 'the negotiation power of the different market participants is unequal, market-based solutions alone might not be sufficient to ensure fair and innovation-friendly results, facilitate easy access for new market entrants and avoid lock-in situations'. More precisely, the refusal to grant access to essential business data has been acknowledged by the Commission as one of the principal unfair trading practices on online platforms.

Under these premises, the sharing remedy under the essential facilities doctrine has been expressly put in connection with the objectives of the free flow of information in digital markets.

The extent to which competition law and competition authorities can impose access obligations on dominant companies is debated in the scholarly literature: the proactive imposition by a competition authority of disclosure duties on a dominant company or a merging party is indeed feared to be an operation of outright market design, and related sharing remedies are believed to be para-regulatory measures.

In light of these concerns, the applicability of the essential facilities doctrine for data sharing purposes is questionable. Against this backdrop, the 2019 *Competition Policy for the Digital Era* report has underlined the need for European regulators to define the conditions under which dominant companies are required to give access to their data. The Proposed Digital Markets Act[8] codifies sharing obligations of 'gatekeepers', defined under Article 3(1) as 'core platform services' that (1) have a significant impact on the internal market; (2) operate a core platform service which serves as an important gateway for business users to

[8] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector (Digital Markets Act)' COM (2020) 842 final.

reach end users; and (3) enjoy an entrenched and durable position in their operations or it is foreseeable that they will enjoy such a position in the near future.

These businesses shall be subject to the obligations established under Article 6 to 'provide effective portability of data generated through the activity of a business user or end user'; 'provide business users, or third parties authorised by a business user, free of charge, with effective, high-quality, continuous and real-time access and use of aggregated or non-aggregated data, that is provided for or generated in the context of the use of the relevant core platform services by those business users and the end users engaging with the products or services provided by those business users'; 'provide to any third party providers of online search engines, upon their request, with access on fair, reasonable and non-discriminatory terms to ranking, query, click and view data in relation to free and paid search generated by end users on online search engines of the gatekeeper, subject to anonymisation for the query, click and view data that constitutes personal data'.

1.4 Access rights and intellectual property rights

The creation of a free market zone for the sharing and accessibility of data is impaired by several factors, among which there is the lack of trust between public and private actors and companies' competitive pressure to enclose their data 'silos' through both technical and legal means. In this last regard, intellectual property rights are a direct obstacle to both individual and horizontal access rights.

From the first individual perspective, recital 63 GDPR states that the right to data access 'should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software'. According to the recital, thus, the protection of intellectual property rights can affect the scope and the amount of the information the data subject is entitled to access. This requires a careful balancing between the data subjects' right to access and the controllers' intellectual property rights over the information regarding the automated processing of personal data. This is further confirmed by recital 4 GDPR that states that the right to the protection of personal data – and thus its specifications as the right to access – 'is not an absolute right' but it needs to 'be balanced against other fundamental rights, in accordance with the principle of proportionality'.

Among the fundamental rights mentioned by the recital, there is also the freedom to conduct a business, of which intellectual property rights are a direct expression.

The balancing between these different rights can be solved if one considers that access to information regarding the controllers' processing activities by data subjects, directly serving the protection of the individual fundamental right to data protection, does not amount to a commercial use of the relevant information and should thus fall outside the scope of intellectual property protection or other rights, such as trade secrets. Moreover, the same consideration of the individual nature of the right to data protection also suggests its prevalence over other economic-based fundamental rights. In this respect, the European Data Protection Supervisor has underlined the importance of the involvement of national data protection authorities in the controversies regarding the balancing between controllers' intellectual property rights and data subjects' access rights.

Intellectual property rights can be an impairment to accessibility of data sets also in third horizontal parties' relationships. This is directly acknowledged under Article 10 of the Open Data Directive, recalling the principle 'as open as possible, as closed as necessary', which has been set by the European Commission as a guiding principle of the new data strategy. This calls for a delicate balancing between the objectives of research data reusability and analysis and concerns related to 'intellectual property rights' and 'legitimate commercial interests'. Key for these purposes is the employment of licensing schemes which are consistent with open access policies.

1.5 Access rights and interoperability

From both a vertical and a horizontal perspective, further obstacles to data access and sharing between economic operators are found also in the lack of interoperability standards.

Apart from technical interoperability, which structurally enables communication between differently controlled systems through standards regarding formats and semantics, legal interoperability primarily relates to licence interoperability, which is the possibility of

legally mixing data coming from different sources and using them within a broad range of projects and business models. If technical interoperability enables the sharing of data in a machine-readable format, legal interoperability relates to the licences that allow the reuse of data and related processing technology.

Under these premises, an important enabler of technical interoperability is given by APIs, which are protocols defining communications patterns between different software components. A comprehensive standardisation framework of APIs is, however, still missing. Interestingly, in this regard, the Recommendation on access to and preservation of scientific information[9] considers the new text and data mining technologies[10] and the technical standards for data[11] as important catalysts for the access and reuse of extracted scientific information generated by public stakeholders.

Legal interoperability is meant to overcome what in the legal literature are known as 'digital hurdles', relating to all forms of encryption, digital rights management, technical protection measures and proprietary formats that (en)close digital health technologies both with regard to their infrastructure (processing tools) and their content (data). These digital hurdles impede access to third parties or to exogenous applications, in this way blocking the development of digital interactions among relevant stakeholders, and ultimately, the related disruptive or cumulative innovation in the relevant research sector.

Legal interoperability is a particularly relevant topic in the context of machine learning processes, where both processed data and information regarding automated systems' internal functioning mechanisms are encumbered most of the time with an array of different intellectual property rights. In this perspective, legal interoperability ultimately relates to the coordination of different rightsholders.

Licences of data are a particularly complex issue, increasingly debated at policy and academic level. Among the majorly debated issues related to data licences, there are the suitability of FRAND (fair, reasonable and non-discriminatory) terms to the licensing of data and the encouragement of the employment of specific licences (e.g. FLOSS: licences granted for commercial or only non-commercial uses) in respect of the different access regimes regarding personal, non-personal or public data.

GIULIA SCHNEIDER

2 Accountability

2.1 Machine learning and accountability

In the context of artificial intelligence systems, accountability is related to the ability to establish whether a decision is made in conformity with substantive and procedural standards. Where these standards are not accomplished, controllers' liability arises.

Accountability is regarded as a structural component of both public and private governance. It can be generally defined as the ability of decision makers to provide good reasons and justifications with regard to the decisions they have made in respect of the subjects that are impacted by their decisions. In the more theoretical reconstructions, accountability has two main components, respectively related to justifiability and answerability. Framed in these terms, accountability is related to the identification and the demonstration of the reasons of a decision, of the alternatives of the same decisions and the justifications for which a given decision was taken over existing alternatives. If, in respect of public governance, accountability relates to citizens' participation and empowerment vis-à-vis public authorities, with regard to private governance it relates more to the verifiability of enacted processing activities and decision-making criteria.[12]

Since machine learning systems are developed by many different stakeholders, the literature has underlined the difficulties of allocating the responsibilities of accountability within the technological environment.[13] Data protection

[9] Commission Recommendation (EC) 2018/790 of 25 April 2018 on access and preservation of scientific information [2018] OJ L 134/12.

[10] Ibid., 3.

[11] Ibid., 6–7.

[12] Sabina Leonelli, 'Locating Ethics in Data Science: Responsibility and Accountability in Global and Distributed Knowledge Production Systems' (2016) 374(2083) *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*.

[13] Giovanni Comandé, 'Intelligenza artificiale e responsabilità tra liability e accountability. Il carattere trasformativo dell'IA e il problema