Data Management Tools and Privacy by Design and by Default

Data Management Tools and Privacy by Design & by Default

Fabio Bravo*

1 Data Management Tools (DMTs) and Main Legal Issues on Data Protection Law

The legal regulation in the matter of personal data protection has undergone relatively recent modifications through Reg. EU 679/2016 (GDPR), issued to replace Dir. 95/46/EEC. The new European regulation, applicable since 2018, must not be viewed as a finish point: we are in fact in the middle of an extensive regulatory evolution, bound to change radically in the near future, as can be clearly felt through the issuance of the Proposal for an EU Regulation in the matter of Data Governance of 25.11.2020 (Data Governance Act). This regulatory evolution has led to a significant paradigm shift: the long journey that led to the final establishment of a fundamental right to personal data protection (Art. 8 Charter of Fundamental Rights of the EU) and to its legal recognition within European legislation on data protection, then undertook a different path, in which matter the central issue becomes the usability, also of economic nature, of data and control over them. In this regard, the role played by the technological tools which manage data (known as Data Management Tools or DMTs) and allow not only the processing of personal data but also their management, sharing, control and usability, becomes paramount (Rundle 2006). They are therefore both data processing and data governance tools. With regard to the latter, DMTs can also be used to manage recognised rights in

* Fabio Bravo, Full Professor of Private Law, University of Bologna (fabio.bravo@unibo.it) | doi: https://doi.org/10.1007/978-981-16-3049-1_8

favour of the data subject, so as to achieve profitability from personal data. This phenomenon can be seen, in particular, in "infomediation" relations (Bravo, 2020, 2021; Hagel and Rayport 1997).

The GDPR has imposed the guarantee of the respect of the rights and freedoms of the data subject ever since the design of the personal data processing (privacy by design) and privacy by default, through the obligation to put in place specific technical and organisational measures (Article 25 GDPR) (Bravo 2019; Bygrave 2017). This obligation, which also applies to DMTs, as to any (tool used for the) processing of personal data, entails significant interpretative problems, concerning both objective and subjective aspects.

DMTs can also be used to manage or enhance the data protection of the data subjects, they are therefore also at the centre of the debate on the enhancement of personal data protection and, in this regard, can take on Privacy Enhancing Technology (PET) functions. At the same time, DMTs can also be used as Privacy Management Tools (PMTs), with 'data governance' functions. They allow for both the exercise of rights of the data subject in the economic sphere (consent to processing in exchange for payment or another economic benefit; data portability; usability of data in the perspective indicated on the proposal for a regulation on data governance). Here the legal issues are different, and also concern the reification and capitalisation of data, their sharing also for commercial purposes and their use also for altruistic purposes.

2 Privacy by Design & by Default. Privacy Design Pattern and Privacy Dashboard

In Article 25(1) GDPR, it is said that the data controller shall "implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects". These are measures that must be put in place not only "at the time of the processing itself", but also "at the time of the determination of the

means for processing". These are therefore technical and organisational measures that the controller must undertake ever since the 'design' stage of the processing, taking into account a complex series of parameters set by the legislator, namely "the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing".
Prepared during the design stage, they must then accompany the processing throughout its entire life cycle. The controller is tasked with establishing what measures can be considered "appropriate" in accordance with the above-mentioned provision: among these, however, the legislator expressly includes, by way of example, "pseudonymisation", meaning the set of processing operations appropriate to impede that personal data "be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person" (Article 4(1)(5) GDPR). Thus, personal data are temporarily stripped of the references necessary to identify the data subject of to make them identifiable, separating the additional information necessary for the identification. These must be kept separate and must undergo measures aimed at guaranteeing their non-traceability to a given subject (for example through 'encryption'), if not through a reverse procedure (for example a 'reversal of pseudonymisation').

During the design, the 'privacy design patterns' (or 'privacy patterns') are especially useful, which in the matter of privacy are a form of design patterns (Bravo 2019). Design patterns are generally used in the creation of software and can be understood as recurring code 'modules' or 'portions', to realise, with the appropriate readjustments where necessary, a certain function present in an application, without having to rewrite the code every time from scratch. Among the communities of developers, 'pattern libraries' emerge, which can be consulted to more rapidly enter a given function, without having to rewrite it every time from scratch. The use of such design patterns, with various contents, therefore affects the architecture itself of the software, which can benefit from ready-made and already tested 'modules' for the given use one seeks, envisaged during the design stage of the software. These design modalities may comply with the

concept of privacy by design provided for in Article 25(1) GDPR (Bravo 2019).

The new Regulation aims at resorting to a protection solution of personal data protection which can be reached during the design stage, so as to put in place an architecture (of the software, but also of the device, of the computer system as a whole, etc.) capable of offering adequate guarantees for the protection of personal data (e.g. privacypatterns.org, privacypatterns.eu). Thus, one of the most useful applications, in this direction, comes from the use of privacy design patterns, meaning the modular portions of 'code' with which programmers or developers create – and make available to the community of programmers and developers, for a subsequent reuse – certain functions aimed at structurally ensuring the compliance (Reidenberg 1998) with personal data protection. In this regard online there are also portals – managed in the matter of international research projects carried out at university level – aiming to conduct censuses on and disseminate privacy patterns, in order to spread their use and improve their functions.

The concept behind these projects is to develop and promote the use of technologies capable of ensuring compliance with personal data protection, identifying also the correct methodology to adopt to create privacy patterns, in reference to which one must keep into account not only the more IT-related aspects concerning the 'code' creation, but also legal aspects, given the difficulty in translating into computer language the regulatory data and the (legal) *principles* regulating the matter under examination.

The procedure leading to the provision of technological tools, in the prospect evoked by Article 25 GDPR, is made up of different stages: the design does not in fact constitute the initial stage, as it is preceded by the *analysis* stage, aimed at determining the characteristics of the system and the aspects concerning personal data protection, based on two possible approaches (*risk-based approach* or *goal-oriented approach*). Resorting to predetermined privacy patterns, and also the development of new privacy patterns, deploys all its efficacy thanks to the replicability of adaptable 'methodologies' and 'models', during the design stage, to the different systems used for personal data processing. Privacy patterns fall under the realisation modalities of what has been defined as 'privacy by design' (or 'data protection by design') (Cavoukian 2009; Pagallo 2012), belonging to the more complex type of technologies with which one seeks to realise or

enhance the protection requirements of personal data in the computer system used for processing (known as Privacy Enhancing Technologies, PETs) (Burkert 1997).

Along with data protection by design, the European legislator also regulated data protection by default, laying down that the data controller shall "implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed" (Article 25(2) GDPR).

This protection technique is complementary to the first, based on the use of procedures and technologies protecting one's privacy, resorting to data-oriented strategies: no intervention is required on the structure of the software, of the device or of the computer system or of the processing, in its entirety; an intervention entailing a 'control' on personal data processing is instead required, both during the acquisition stage and the subsequent reprocessing, employing technical and organisational measures (Crespo Garcia et a. 2015). In particular, the application of the regulation under examination requires that the technologies devised during the design stage for privacy protection – therefore present in the computer system in compliance with the obligation referred to in Article 25(1) GDPR – be then 'pre-set' by default to limit processing solely to the *necessary data* for achieving the purposes of the processing.

Data protection by default, outlined in Article 25(2) GDPR, focuses its attention solely on the setup of the control over the data subject to processing, requiring that they be 'filtered' by default for the entire life cycle of the processing, ever since their acquisition, through technical and organisational-procedural measures. The default setup (*ex-ante*) does not exclude a different setup in a subsequent stage, as is clarified in the previous examples: the default setup ordered by the European legislator seems to be oriented toward a 'dynamic' use of Privacy Enhancing Technologies (PETs), in that the level of protection ensured by them varies depending on "each specific purpose of the processing" the controller decides to legitimately realise. To assess what are the sole *necessary data* that the processing, as default setup, must consider, Article 25(2) GDPR sets qualitative and quantitative criteria, always to be estimated in relation to the "purposes", and expressly provides for "that obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility". It

would therefore be useful to allow the data controller and the data subject to benefit from a privacy dashboard to set up the "privacy options" ensuring, by default, the greatest protection for the data subject, which can then be modified in relation to the requirements and purposes pursued, allowing a subsequent intervention on the privacy settings of the Privacy Management Tools, where necessary.

3 Application Issues

The implementation obligation of privacy by design and by default (Article 25 GDPR) must be carried out by the data controller by implementing the accountability principle (Articles 5(2), 24(1) GDPR), whereby the data controller shall guarantee and be able to prove, through adequate and, where necessary, updated technical and organisational measures that the processing is performed in compliance with the provisions of the GDPR. Navigating this is not easy in light of remarkable application issues entailed in the formulation of Article 25 GDPR.

3.1 Excessive Vagueness of the Obligation and Difficult Identification of Contents

The first problem concerns the excessive vagueness of the regulation in question, especially if compared with the different solution in the "Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data" (25.01.2012, COM (2012) 11 final).

Indeed, in Article 23 of this proposal – corresponding to current Article 25 GDPR – there were two paragraphs eliminated in the final text, in which, after the requirements aimed at guaranteeing the privacy by design and by default obligations (Article 23(1) and 23(2) Proposal) the Commission being "empowered to adopt delegated acts (…) for the purpose of specifying any further criteria and requirements for data protection by design requirements applicable across sectors, products and services" (Article 23(3) Proposal) was contemplated, together with the further power to "lay down technical standards for the requirements laid down in paragraph 1 and 2" (Article 23(4) Proposal).

In the final text of the regulation in question the powers of the Commission were drastically diminished, thus now the GDPR merely includes (in Article 25 GDPR) the obligation to adopt technical and organisational measures aimed at protection starting from the design and by default setting, delegating said measures directly to the subject which sets up the technological structure necessary for the personal data processing.

The step back by the European legislator has been justified owing to the difficulty in legitimising, pursuant to Article 290(1) TFEU, the powers delegated to the Commission, admitted solely for "non-legislative" acts of general scope, which integrate or modify certain "non-essential" elements of a legislative act, explicitly defining objectives, content, duration, scope and conditions of the delegation (Koops and Leenes 2013). Therefore current Article 25 GDPR, which has remained vague in its content and impossible to integrate at an institutional level, was deemed overly generic, which makes the precept non-implementable in all its possible applications, if not even evanescent: the translation of the regulation into a computer 'code' (and, before that, into an algorithm) becomes extremely complicated, if not concretely non-implementable, as there are multiple and diverse modalities of interpreting and concretely implementing the provisions of current Article 25 GDPR.

3.2 Doubts on the Existence of the 'Hardcoding' Obligation

There is another issue related to Article 25 GDPR. The formulation of the regulation has been perhaps overestimated owing to the emphasis of the 'privacy by design' principle in the debate concerning *Privacy Enhancing Technologies* (PETs): in fact it should be scaled down, in that performing 'architectural' interventions on the software or the hardware used for personal data processing in order to guarantee compliance with the regulation in the matter of data protection (known as hardcoding) is not an operation that can be concretely translated into operative practice, given the various obstacles undermining its feasibility (therefore, it has been maintained that "Privacy regulation cannot be hardcoded") (Koops and Leenes 2013). This argumentation is largely acceptable.

One difficulty is due to the complexity of the regulatory

system concerning personal data protection, which cannot be limited solely the GDPR provisions: at a European level, for example, Article 8 of the Charter of Fundamental Rights of the EU, Directive 2002/58/EC (known as e-Privacy Directive) subject to review (it will be replaced by a European Regulation, complementary to the GDPR). For example, the next issuance of the EU Regulation on "Data Governance" (still as a proposal). At national level, instead, there are other provisions which may become relevant in the matter of data protection, albeit not contained in said Regulation (see for example the provisions concerning remote control of workers).

Other significant matters include the technical impossibility of translating the 'legal' rule into a 'technical' rule integrated in the software or hardware, owing to the modalities in which it is formulated, the need for interpretation, often not univocal and changeable over time, also in relation with the court decisions or the decisions by the supervisory authority (Koops and Leenes 2013).

The critical aspects do not, however, lead to complete dismantling, in that hardcoding can be performed on computer systems tasked with personal data processing due to certain well-defined and easily identifiable legal rules (such as use of encryption, data pseudonymisation, specific technologies for access control to a computer system and the fields of the allowed processing, etc.), but not as a general mandatory rule (Koops and Leenes, 2013).

Moreover, the stress of the legal theory and of the institutions on technological constraints – suggested by the use of the term Privacy Enhancing Technologies (PETs) – seemed excessive, when considering that the 'protective obligations' outlined by Article 25 GDPR do not solely entail "technical" but also "organisational" measures, meaning that the principles of privacy by design and by default can be achieved also by resorting to a less rigid interpretation of the regulation in question (Koops and Leenes 2013).

3.3 On the Appropriateness Criteria of the Measures

As already specified, Article 25(1) GDPR begins by establishing that the obligation of the data controller to put in place "*appropriate*" technical and organisational measures – aimed at

effectively implementing the principles of data protection and integrating in the processing the necessary guarantees to both meet the requirements referred to in the Regulation and protect the rights of the data subjects – must be complied with "taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing (…)".

These are not *selective* criteria with regard to the application or lack thereof of the obligation of the measures in question, which must in any case be met, but rather *assessment* criteria concerning the appropriateness (and congruity) of the measures to be applied, which – if left to decide solely to the controller – may be overly evanescent, if not defined within a self-disciplinary regulatory framework (codes of conduct and certification mechanism) and, above all, by resorting to "standard models and (…) operational schemes put in place at the initiative (and under the leadership) of the European Data Protection Board (Article 70), whose contribution promises to be decisive so that, in the tension between people's rights and technological evolution, it is technologies and economic practices that conform to the institutions and concepts of personal data protection, and not these, and the underlying concepts, to merely have to adapt to the former to allow the development of certain technological applications" (D'Orazio 2016).

Thus, the critical issues related to the risks of not determining these criteria, detectable in any case during the initial stage, are bound to be gradually overcome in an objective manner, although one can at any rate resort to the "reasonableness" principle to hermeneutically guide the interpreter in the concrete application of the above-mentioned assessment elements *ex* Article 25 GDPR.

3.4 On the Recipients of the Obligation

Another complex issue concerns the correct identification of the recipients of the obligation referred to in Article 25 GDPR. The problem had already been highlighted, in Italy, with regard to the application of Article 3 Italian Legislative Decree 196/2003 (Italian Privacy Code), which however was characterised by an 'impersonal' formulation, i.e. without specifying the subject to

whom the provision was to be considered applicable ("The information systems and the computer programmes are configured…"). Although it was clear that the first recipient of this regulation was the processing controller, solutions have been put forward to extend the applicative scope to include also producers of hardware and software used in the processing (Buttarelli 2007), which can also be traced in the measures of the Italian Supervisory Authority (e.g. Italian Data Protection Authority, provision on the measures to adopt for the legitimate use of videophones, 20.01.2005, doc. web n. 1089812, para. 4). It is however an extension of the applicative scope of the regulation which appears to act more with regard to moral suasion than to the compliance with a mandatory provision, given that the manufacturers – and the providers – of technological tools used by the controller to process other persons' personal data are not – normally – controllers themselves of the processed data (big players of IT – such as Google and Facebook – do not fall under this category, as they process personal data through technological tools they themselves designed, manufactured and used: in this case the producer of the technology can also be the data controller, but this evaluation must at any rate be made in each single concrete case).

With regard to the obligations to adopt the technical and organisational measures referred to in Article 25 GDPR, in particular in pursuance of the privacy by design principle, similar issues arise, which the Article 29 Working party has already sought to solve with "Opinion 02/2013 on apps on smart devices" of 27.02.2013, highlighting the cases in which manufacturers of operating systems (OSs) and devices can be considered 'data controllers' or 'joint controllers'): "The OS and device manufacturers should also be considered as data controllers (and where relevant, as *joint controllers*) for any personal data which is processed for their own purposes such as the smooth running of the device, security etc. This would include user generated data (e.g. user details at registration), data automatically generated by the device (e.g. if the device has a 'phone home' functionality for its whereabouts) or personal data processed by the OS or device manufacturer resulting from the installation or use of apps. Where the OS or device manufacturer provides additional functionality such as a back-up or remote locate facility they would also be the *data controller* for personal data processed for this purpose. Apps

that require access to geolocation must use the location services of the OS. When an app uses geolocation, the OS may collect personal data to provide the geolocation information to the apps and may also consider using the data to improve its own location services. For this latter purpose, the OS is the *data controller*."

As can also be noted by discussing the above-mentioned specifications of the WP29, the application of the obligations referred to in Article 25 GDPR in the matter of privacy by design to the manufacturers of technological tools is neither generalised nor automatic: it may occur that a data controller may decide he or she must use a device or a software of 'third parties' to process personal data, as they remain unrelated to the processing in question, they cannot be considered directly recipients of said provision (which, unlike Article 3 of Italian Privacy Code is not built in an impersonal manner, but refers its precept, textually, to the 'controller').

In other words, the GDPR cannot be applied to manufacturers of technological tools unless they entail, at least partially, the quality of controllers or joint-controllers of the processing, therefore, where this condition – which must be ascertained case by case – is not met, data protection by design seems to be bound to remain a sort of empty box, given the inapplicability of the obligations to the subjects who, during the design stage, can affect the compliance of the technological tool with the regulatory provisions. This seems to be confirmed also by the content of Recital 78 GDPR, where – after tracing back the data protection by design and by default obligation to the field of the more general security obligation referred to in Article 32 GDPR – is addressed to the 'manufacturers' not as direct recipients of these obligations, but as subjects toward whom an action of 'encouragement' must be made, based on the logic of moral suasion, which is not unrelated to 'social responsibility' (CSR).

Although in these cases the regulation in Article 25 GDPR is not directly applicable to the manufacturers, it can be understood as to impose to the data controllers, to resort (solely) to technological tools which are compliant with the regulation in the matter of personal data protection, for which manufacturers, during the design stage, have adjusted to the rationale referred to in the provision in question. In discussing Article 25(1) GDPR, it must not be forgotten that "at the time of the determination of the means for processing", "the controller" shall "implement appropriate technical and organisational measures (…) which are

designed to implement data-protection principles (…)", "taking into account the state of the art". Thus, the data controller who cannot technically intervene during the design determining the "privacy-compliant" architecture of the tool to use, would nevertheless be obliged, while determining the means to use for the processing, to organise oneself to effectively implement the privacy (or data protection) by design principle, resorting to tools which, based on the state of the art, have been prepared by the manufacturer in compliance with the requirements of the Regulation.

Therefore, if the obligation to put in place the "privacy-compliant" tool to use for processing personal data is not immediately applicable to the manufacturers, the same result can be reached if one considers that the controller (different from the manufacturer) is at any rate required, while determining the means to use for the processing, to select the tools with the above-mentioned compliance characteristics.

4 A Look Forward: European Data Governance

With the Proposal for a Regulation on Data Governance the EU embraces the prospect of the control of personal data for purposes that are commercial, of public interest or 'altruistic'. The reuse in the EU of certain data categories held by public entities, voluntary registration systems for entities that collect and process data made available for altruistic purposes, and "a notification and supervisory framework for the provision of data sharing services" (Article 1), meaning "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" (Article 2(1)(7)) are regulated.

The notification must be made by the service provider to the competent national authority, which shall submit it to the authorities of the other Member States and to the European Commission, which will keep a register of data sharing service providers. The notification shall be a necessary requirement for the performance of the sharing service (Bravo 2021), which shall then be provided only if further conditions are met, including: the ban from using the data "for other purposes than to put them at the disposal of data users"; the obligation to use "the metadata collected from the provision of the data sharing service (…) only

for the development of that service"; respecting the competitive dynamics; pursuing the best interest of the subjects receiving the service; the obligation of guaranteeing high level security, of guaranteeing continuity in the service provision and access to the data on the part of the "data holders" and "data users" (Article 11). The national authorities shall conduct the supervision of the provision of the data-sharing service (Bravo 2021) and, in the event of violations of the regulation in question, they can impose "dissuasive financial penalties which may include periodic penalties with retroactive effect" and put in place the "cessation or postponement of the provision of the data sharing service".
The response of the European legal system to the datafication process of society (and of the economy) is underpinned by the enhancement of the supervision regarding data protection, where data traffic, also thanks to DMTs, is increasingly present in market dynamics.

References

Bravo F (2019) L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi. In: Cuffaro V, D'Orazio R, Ricciuto V (eds) I dati personali nel diritto europeo. Giappichelli, Torino, pp 775-854

Bravo F (2020) Il commercio elettronico dei dati personali. In: Pasquino T, Rizzo A, Tescaro M (eds) Questioni attuali in tema di commercio elettronico. Edizioni Scientifiche Italiane, Napoli, pp 83-130

Bravo F (2021) Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act. Contratto e impresa Europa 1(1):199-256

Burkert H (1997) Privacy-enhancing technologies. Typology, critique, vision. In: Agre PE, Roten- berg M (eds) Technology and privacy. The new landscape. San Diego, California, US, pp 125–142

Buttarelli G (2007) Commento sub art. 3 d.lgs. 196/20013. In: Bianca CM, Busnessi FD (eds), La protezione dei dati personali. Commentario al D.Lgs. 30 giugno 2003, n. 196 («Codice della privacy»). Cedam, Padova, I, pp 32-40

Bygrave LA (2017) Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements. Oslo Law Review 4(2):105-120

Cavoukian A (2009) Privacy by Design. The 7 Foundational Principles, Ottawa. Available at www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf. Accessed 13 Jan 2021

Crespo Garcia A et al (2015) Privacy- and Security-by-design Methodology Handbook, v. 1.0, 31 Dec 2015. Available at http://pripareproject.eu/wp-content/uploads/2013/11/PRIPARE-Methodology-Handbook-Final-Feb-24-2016.pdf. Accessed 6 Jun 2017

D'Orazio R (2016) Protezione dei dati by default e by design. In: Sica S, D'Antonio V, Riccio GM (eds) La nuova disciplina europea della privacy. Wolters Kluwer-Cedam, Milano, pp 79-110

Hagel J, Rayport JF (1997) The new infomediaries. Mckinsey Quart 4:54–70

Koops BJ, Leenes RE (2013) Privacy regulation cannot be hardcoded: A critical comment on the "privacy by design" provision in data-protection law. Int Rev Law Comput Technol 28(2):159–171

Pagallo U (2012) On the Principle of Privacy by Design and its Limits: Technology, Ethics and the Rule of Law. In: Gutwirth S et al. (eds), European Data Protection: In Good Health? Springer Science & Business Media, pp 331–346

Reidenberg JR (1998) Lex Informatica: The Formulation of Information Policy Rules Through Technology. Texas Law Review 76(3):553–593

Rundle, MC (2006) International Personal Data Protection and Digital Identity Management Tools. Berkman Center Research Publication No. 2006-06, Available via SSRN. https://ssrn.com/abstract=911607. Accessed 13 Jan 2021