Accountability principle under the GDPR: is data protection law moving from theory to practice?

by **ERNANI FRANCESCO CERASARO**

Abstract

Tra le molte novità introdotte dal nuovo Regolamento Generale sulla Protezione dei Dati, vi è è certamente l'affermazione normativa del principio dell'accountability, non esplicitamente previsto all'interno della previgente Direttiva 95/46/EC.
Il principio, non solo esige che il titolare del trattamento garantisca il rispetto delle disposizioni normative in materia di trattamento dei dati, ma richiede anche la concreta dimostrazione dell'adozione di adeguate misure legali, organizzative e tecniche a garanzia della tutela delle posizioni individuali.
Lo scopo di questo articolo è quello di dimostrare come l'introduzione di un siffatto principio costituisca un'opportunità per garantire l'effettività delle norme in materia di privacy, superando così l'incertezza giuridica che troppo spesso affligge il diritto fondamentale alla protezione dei dati personali.
Seguendo il *fil rouge* dell'effettività, sarà poi possibile analizzare gli effetti più rilevanti derivanti dall'applicazione del principio dell'accountability: l'adozione di un approccio basato sul rischio ed il conseguente obbligo di fornire una valutazione dell'impatto sulla protezione dei dati.

1. Accountability principle as a natural follow-up of the need for trust. Rapid technological developments and globalisation have brought new challenges for the protection of personal data. Those developments required a stronger and more coherent data protection framework in the European Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market[1]. Since the protection of personal data was regulated by the Directive 95/46/EC, which dates back to 20 years ago and therefore was too obsolete and inadequate to regulate such a dynamic and technological-dependent topic (MAGUIRE S., 2015), a reform in the regulatory framework was almost mandatory.

In fact, even if the core objectives and principles of the former Directive remain valid, it has not prevented, among others, three substantial problems:

1 Cfr. Recital n.7 of the GDPR

fragmentation in the implementation of data protection across the Union; legal uncertainty; a general public perception that there were significant risks to the protection of natural persons[2].

So, after four long years of negotiations, the European legislator adopted the GDPR[3], replacing the former Directive.

The new Regulation, is designed to harmonize data privacy laws across Europe and to ensure a satisfactory protection also outside the Union[4]; to protect and empower all EU citizens; and to reshape the way in which organizations, citizens, companies and freelancers approach to data protection and privacy.

What these general issues have in common is the necessity of an effective protection of individual positions, mainly because with the relentless technological development we face every day, processing of personal data is increasingly becoming dependent on the ubiquity of the data flow.

This needed new rules and procedures[5], which hopefully are more appropriate to regulate this absence of an individuated or detectable geographical regulatory area.

After a careful reading of the new legislation, what become evident is that the European legislator, attempting to translate in practice the many-parties requests formulated in the previous years, has adopted a legal framework which follows the primary and general objective of the trust-building in relations between data subject, controllers, processors and in general all the actors involved.

---

2 Cfr. Recital n.9 of the GDPR: The present differences in the level of protection of the right to the protection of personal data may prevent the free flow of personal data throughout the Union and therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law.

3 European Regulation (EU) 2016/679

4 A first and essential element of the new legislation is that it is a Regulation, which results in its direct applicability in all Member States, without the adoption of a legislative provision at national level. Furthermore, the Regulation will apply to companies which, although located outside the Union territory, offer services or products to persons within one of the Member States.

5 On this regard, a fundamental step is that the Europeanization of the legislation will not only affect rules, but also processes (e.g.: the introduction of the Stop-shop principle, according to which companies operating in different territories can address their requests and their claims to a single national DPA, will ensure huge savings and uniformity in the application of the laws).

In trying to provide an effective and efficient protection of personal data in a socio-economic context that is constantly changing, data protection enters in a new era, in which all the data controllers and processors will be subject to new obligations, including the adoption of internal policies, mechanisms to implement privacy policies, internal oversight systems, transparency and remediation.

The GDPR introduces new rights for citizens, which will be fully respected only if it will be ensured the effective application of the new obligations provided for data controllers.

This means, in a very a-technical way, that individuals' rights depend on the willingness of data controllers in doing their homework, far more than before.

In other words, GDPR's «cornerstone is the concept of trust: trust in data controllers to treat personal information responsibly, and trust that the rules will be effectively enforced» (BUTTARELLI G., 2016).

The material consequence of the regulatory importance of the concept of trust is the formal introduction of the principle of "accountability" within the GDPR.

This is an important recognition at the regulatory level of a principle which was recognized solely from a theoretical point of view, as a way to regulate and self-regulate privacy responsibilities exercised by organizations.
The theoretical concept of privacy accountability, as a model, «is a set of activities (dimensions) that should be undertaken by (...) organizations in order to become a privacy-accountable entity» (RABAN Y., 2012)[6].

6 *«This model includes dimensions and indicators (concrete activities) as follows:a) Planning, awareness building, conceiving and strategizing related to privacy (reflexivity). Such activities may be fulfilled by appointing a privacy officer, by conducting regular consulting cycles regarding privacy and by the execution of privacy impact assessments.b) Making privacy-related information available to the public (information availability). Indicators for information availability may include privacy statements, codes of ethics, the use of Transparency Enhancing Technologies (TETs), and compliance reports.*
c) Exercising two-sided communication with stakeholders, including citizens, on issues of privacy (communicability). Indicators of communicability may include hotlines, discussions in forums and social media such as Facebook where issues discussed may include ethics and privacy.

More generally, with respect to a norm, «a relationship qualifies as a case of accountability with respect to an obligation when: there is a relationship between an actor and a forum, in which the actor is obliged to report, explain, and justify his conduct relative to the norm, the forum can pose questions, pass judgement, and the actor may face consequences» (RAAB C., 2017).

In order to fully understand the reason of the introduction of such a principle to regulate data protection, it should take a few steps back in the years.

The accountability privacy principle appeared the first time in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data in 1980, in which was already present the taste of a lack of effectiveness in the protection of individual privacy.

Guidelines stated that a «data controller should be accountable for complying with measures which give effect to the principles» of the data protection. This means that the organization that collects the personal data responsible for the data while it or its agents have control or custody of the data.

From a "statutory" perspective, the first appearance of the principle was in the Personal Information Protection and Electronic Documents Act in the Canadian Fair Information Principles. The principle required to develop and implement policies and practices to uphold the 10 Fair Information Principles, including implementing procedures for protecting personal information and establishing procedures for receiving and responding to complaints and inquiries.

Then, in 2010, the Article 29 Working Party (WP29) complained more expressly about the necessity to add in the regulatory framework some additional tools to ensure the effectiveness in the application of privacy laws.

---

d) Changing the behavior of security organizations with respect to privacy (action-ability). This may be indicated by the enabling of citizen's requirements to be implemented through focus groups or citizen's juries. Other indicators may simply be changes in products due to Privacy by Design (PbD), or the introduction of privacy enhancing technologies.
e) Evidencing and verification of privacy accountability (testability). Indicators may include compliance with standards and regulations, including compliance with self-regulation mechanisms».

In particular, in the opinion 3/2010, the WP29 pitched a concrete proposal for a regulatory recognition of the accountability principle «which would require data controllers to put in place appropriate and effective measures to ensure that the principles and obligations set out in the Directive (95/46/CE) are complied with and to demonstrate so to supervisory authorities upon request. This should contribute to moving data protection from 'theory to practice' as well as helping data protection authorities in their supervision and enforcement tasks»[7].

In that opinion, WP29 explained, on one hand, how the accountability principle can bring to legal certainty; on the other, it highlighted how such principle could impact other areas, including international data transfers, notification requirements, sanctions, and eventually also the development of certification programs or seals.

In its conclusions, the WP29 stressed that «the increase of both the risks and the value of personal data per se support the need to strengthen the role and responsibility of data controllers». It was clear then that a possible future regulation had to contain the necessary tools to encourage data controllers to apply in practice appropriate and effective measures that deliver the outcomes of the data protection principles.

Six years after that, by adopting the GDPR, the European legislator has almost exhaustively implemented the advice pushed forward by WP29.

With the GDPR, accountability, as a data protection principle, «gained fresh prominence» (JASMONTAITE L., VERDOODT V., 2016) and became a keystone of the data regulatory framework.

Accountability is now expressly recognized in the art. 5, second paragraph, of the Regulation, where the data controller is identified as the competent person to ensure compliance with the principles laid down in the first subparagraph of the same article (lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality).

7 WP29 Opinion 3/2010.

The data controller, moreover - and perhaps in this is entailed the most important novelty, as well as it is the core of the principle of accountability - will have not only to ensure compliance with the principles, but he will also have to "demonstrate" such compliance.

The controller will be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with the Regulation, including the effectiveness of the measures[8].

The accountability of data controller is further specified in the article 24 of the Regulation, bearing the "Responsibility of the controller", which provides that «taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation" Those measures shall be reviewed and updated where necessary»[9].

In other words, «an organization must be responsible for personal information and be able to "account for it" within the organization and when it flows to business partners (vendors and service providers) by being able to demonstrate the status of their privacy program to internal stakeholders such as senior management and, if desired (or required), to external stakeholders such as regulators, commissioners, data protection authorities, attorneys general and business partners»[10].

So, the principle of accountability, on the one hand, restores the discretion of the controller to the identification of the measures considered to be more appropriate, while taking into account the above-mentioned criteria; on the other hand, the controller is the same person who deals with the concrete demonstration of the necessity and adequacy of the measures chosen.

8 Recital 74 of the GDPR

9 In the Italian regulatory landscape, requiring the data controller to take appropriate measures, taking into account the characteristics of processing, goes beyond the prevailing discipline contained in Annex B to the italian Privacy Code where more general "minimum measures" were required.

10 https://iapp.org/news/a/demonstrating-privacy-accountability/

The principle of accountability, however, is not limited only to compliance and to its concrete demonstration through appropriate and adequate measures.

Accountability is far more complex and catchy than this.

It sets a higher standard than compliance, and be subject to rules is not enough.

The recognition of accountability as a principle raises socio-cultural reflections, which could lead to a paradigmatic change in how to conceive the protection of personal data.

Data protection seems moving from a static and rigid view to a dynamic and flexible one in which all involved actors are accountable.

Accountability is a paradigmatic change in how to approach data protection. Accountability is the foundation for a social policy change in the affirmation of the fundamental right to the protection of personal data. Therefore, accountability «is an opportunity: if properly implemented, it is an incredible tool to implement tailor-made and personalized measures adopted to the specificities of each organisations, in order to make data protection more effective» (BUTTARELLI G., 2017).

2. Concretizing accountability: risk based approach and DPIA. The principle of accountability can be taken as a theoretical basis of a number of some (more or less) concrete obligations that should ensure effective compliance with the regulatory provisions, resulting otherwise in risks for data subject, with different probabilities and severity. Such risks are likely to cause physical, material or immaterial damage (discrimination, identity theft, financial loss, reputation damage, loss of confidentiality of personal data protected by professional secrecy, etc.)

The risk of treatment is therefore not a novelty in the privacy law scene.

However, what is certainly an important novelty, is the centrality that the figure of the risk assumes within the new Regulation due to the adoption of the “accountable” approach.

While, on the one hand, it is true that the concept of "risk" was already present within the Directive 95/46/EC, on the other hand, it is equally true that with the GDPR the risk assessment becomes an indispensable tool to correctly process personal data.

In doing so, the Regulation would seem to overcome the Directive95/46/EC which providing for a general obligation to notify the control authorities of the processing has not always helped to improve the protection of personal data.

The European legislator considered then appropriate to abolish these general and indiscriminate notification obligations and replace them with procedures focused on identifying treatments that potentially pose a high risk to the rights and freedoms of natural persons by their nature, scope, application, context and purpose, by introducing the "risk-based approach".

By adopting this approach, the GDPR encourages organizations and companies to evaluate in advance the strength and probability of the risk, in order to facilitate the adoption of appropriate and effective measures.
Appropriate and effective because they essentially correspond to the level of risk.

This does not mean that the protection of individual rights will depend solely on the level of risk involved with the activity which it is referred to, but that in order to effectively protect individual positions, it is necessary for the data subjects to modulate the adoption of the necessary measures relying on risk assessments.

From a different point of view, a preventive risk assessment can only benefit organizations handling data, as it will be possible for them to concentrate their efforts on the most risky activities, maximizing the possible benefits of a treatment-related activities.

In other words, such approach could ultimately help to overcome the abstractness and nebulosity of some privacy regulations.

In fact, the Regulation introduces the Data Protection Impact Assessment (DPIA), a fundamental procedure «in order to define an adequate strategy to limit privacy risks» (MANTELERO A., 2013).

It is an instrument designed to describe the processing, assess the necessity and proportionality of a processing and to help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data.

DPIAs ensure that «a conscious and systematic effort is made to assess privacy risks to individuals in the collection, use and disclosure of their personal data. DPIAs help identify privacy risks, foresee problems and bring forward solutions»[11].

As the WP29 has underlined in its guidelines, «DPIAs are important tools for accountability, as they help controllers not only to comply with requirements of the GDPR, but also to demonstrate that appropriate measures have been taken to ensure compliance with the Regulation. In other words, a DPIA is a process for building and demonstrating compliance»[12].

In accordance with Article 35, the DPIA must be carried out in presence of those situations in which the processing of data, because of its nature, scope, context and purpose A DPIA is only required when the processing is *«likely to result in a high risk to the rights and freedoms of natural persons»*.

There is no definition of "high risk" under the GDPR, but Article 35(3) provides some non- exhaustive examples of processing activities in which processing is "*likely to result in a high risk"*:

a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

11 Commission Staff Working Paper - Impact Assessment /* SEC/2012/0072 final.
12 WP29 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, published on 4 April 2017.

b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

c) a systematic monitoring of a publicly accessible area on a large scale.

In such cases, the data controller should carry out a prognostic evaluation of the impact that the treatment might have on the affected persons.

More specifically, the DPIA must contain, as minimum features[13]: a description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the controller; an assessment of the necessity and proportionality of the processing in relation to the purpose; an assessment of the risks to individuals.

This impact assessment should also cover measures, guarantees and mechanisms designed to mitigate this risk, including security and to demonstrate compliance, thus ensuring the protection of personal data and demonstrating compliance with the Regulation.

As a result of this evaluation, a number of alternatives are more or less analytically described in the Regulation.

First, where the assessment would result that treatment could pose a high risk to the rights and freedoms of natural persons and the data subject was of the opinion that the risk could not be reasonably mitigated in terms of available technologies and implementation costs. The Regulation considers appropriate that the holder contacts the supervisory authority prior to the start of the treatment activities.

The supervisory authority that receives the request for consultation should do so within a specified time limit.

A DPIA may concern mostly a single data processing operation. However, Article 35(1) states that «a single assessment may address a set of similar processing operations that present similar high risks». Recital 92 adds that there are circumstances under which it may be reasonable and economical for the subject of a data protection impact assessment to be broader than a

13 Article 35(7), and recitals 84 and 90

single project, for example where public authorities or bodies intend to establish a common application or processing platform or where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity.

DPIA is certainly an important instrument to ensure effectiveness to the application of the principle of accountability.

In fact, under the GDPR, non-compliance with DPIA requirements can lead to fines imposed by the competent supervisory authority. Failure to carry out a DPIA when the processing is subject to a DPIA (Article 35(1) and (3)), carrying out a DPIA in an wrong way (Article 35(2) and (7) to (9)), or failing to consult the competent supervisory authority where required (Article 36(3)(e)), can each result in an administrative fine of up to 10M€, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher[14].

Conclusively, the impact assessment, using a «three-phase model focused on prescription, ex post evaluation, and sanction», «is able to generate privacy oriented solutions, offering a high level of data protection and, in this way, it contributes to increasing users' trust in technology and its related services» (MANTELERO A., 2013).

3. Conclusions. As the European Data Protection Supervisor Giovanni Buttarelli highlights, the GDPR's «cornerstone is the concept of trust» (BUTTARELLI G, 2016).

Relying on this concept, the Regulation introduces in the regulatory framework the principle of accountability, which constitutes a tangible normative intent to move data protection from theory to practice.

In fact, even if «Accountability has been perceived as a soft approach to data protection (...) (it) requires hard work, continuous review and a complete understanding of your data flows» (BERMÚDEZ J.A., 2015).

14 Cfr. Cit. WP29 Opinion, p. 8.

The centrality of accountability in data management is then undoubtedly one of the most challenges in applying the new Regulation.

At the same time, «accountability may be neither a necessary nor a sufficient condition for trust. In order to provide an improved basis for trustworthiness via enhancing accountability, certain conditions need to be met» (PEARSON S., 2017).

Accountability does not redefine completely privacy or replace laws.

It «shifts the focus of privacy governance to an organization's ability to demonstrate its capacity to achieve specified privacy objectives»[15].

In other words, «figuratively, accountability is the flu vaccine for the data protection immune system. When an organisation has the data protection sniffles, accountability, like the flu vaccine, enhances the immune system» (ABRAMS M., 2017).

Nevertheless, accountability can be taken as a driver for effective implementation of data protection principles, not as a magic stick.

It is then imperative to carry out a cultural shift in the approach to data management.

This «means a change to the culture of an organisation. That isn't an easy thing to do, and it's certainly true that accountability cannot be bolted on: it needs to be a part of the company's overall systems approach to how it manages and processes personal data. But this shift in approach is what is needed. It is what consumers expect. The benefit for organisations is not just compliance but also providing an opportunity to develop the trust of its consumers in a sustained way» (DENHAM E., 2017).

The new Regulation, following a trust-building approach, represents an opportunity for growth for all the actors: data subject, regulators, businesses, etc.

But as in life, so in law, growing involves responsibility.

Therefore, the GDPR rightly requires more proactivity, which concretizes in accountability and in a risk-based approach.

15 https://iapp.org/resources/article/accountability-5/

The effective reception of these normative and conceptual innovations will be an important crossroads for the future of European citizens, increasingly subjected to threatening data processes they ignore, requiring therefore the most real and concrete guarantees.

However, without a strong inversion of cultural tendencies within all the actors involved, nothing will significantly change.

The year which separates us from the full applicability of the Regulation will be fundamental. It will show us if the necessity of such a cultural shift is already internalized.

Riferimenti bibliografici

G. BUTTARELLI, *The EU GDPR as a clarion call for a new global digital gold standard,* International Data Privacy Law 6.2 (2016): pp. 77-78.
G.BUTTARELLI, *Hitting the ground running: How regulators and businesses can really put data protection accountability into practice*, Keynote speech at European Data Protection Days (EDPD) Conference Berlin, 15 May 2017
E. DENHAM, delivered this speech at a lecture for the Institute of Chartered Accountants in England and Wales in London on 17 January 2017. She discussed the role of accountability in the GDPR, underlining that "*We're all going to have to change how we think about data protection".*
L. JASMONTAITE, V. VERDOODT, *Accountability in the EU Data Protection Reform: Balancing Citizens' and Business' Rights. Privacy and Identity Management. Time for a Revolution?*,
S. MAGUIRE, *A metadata-based architecture for user-centered data accountability*, Electronic Markets 25.2 (2015): 155-160: «Data is rapidly changing how companies operate, offering them new business opportunities as they generate increasingly sophisticated insights from the analysis of an ever-increasing pool of information. Businesses have clearly moved beyond a focus on data collection to data use, but users have an inadequate model of notice and consent at the point of data collection to limit inappropriate use»
A. MANTELERO, *Competitive value of data protection: the impact of data protection regulation on online behavior,* International Data Privacy Law (2013), 3(4): 229-238. http://dx.doi.org/10.1093/idpl/ipt016, pp.234-326.
S. PEARSON, *Strong Accountability and Its Contribution to Trustworthy Data Handling in the Information Society. IFIP International Conference on Trust Management*. Springer, Cham, 2017.
Y. RABAN, *Privacy Accountability Model and Policy for Security Organizations (2012*[1] C. Raab, *Information Privacy: Ethics and Accountability, Ethik in den Kulturen-Kulturen in der Ethik: Eine Festschrift für Regina Ammicht Quinn* (2017), p. 335.

Sitografia

https://iapp.org/resources/article/accountability-5/
http://informationaccountability.org/time-to-double-down-on-accountability/