Accountability

Gaetana Natale*

"The concept of privacy is elusive and ill defined" as Richard Posner wrote in his famous essay entitled *"The right of Privacy"* (1977). In leading case *Melvin v Reid* Samuel D.Warren and Luis D.Brandeis defined *"the right to be let alone"* without digital data, analytics or algorithms.

With Artificial Intelligence how will the concept of *accountability* change? Must the accountability go over the territoriality of the States in Europe and, after the case Schrems II (Privacy Shield), in USA?

So, reading the articles of GDPR, we can make some reflections.

Article 24 - EU GDPR
"Responsibility of the controller"

1. 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.
2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.
3. Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.

Suitable recitals

Recital 74
Responsibility and liability of the controller

The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures. Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons.

(*) Avvocato dello Stato, Professore a contratto presso l'Università degli Studi di Salerno, Consigliere giuridico del Garante per la Privacy.

Costituisce il presente scritto la relazione presentata dall'Autrice, in qualità di consigliere giuridico del Garante per la Privacy, ad un meeting internazionale con l'Autorità della Privacy albanese - 2 marzo 2021.

Recital 75
Risks to the rights and freedoms of natural persons
The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.

Recital 76
Risk assessment
The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk.

Recital 77
Risk assessment guidelines
Guidance on the implementation of appropriate measures and on the demonstration of compliance by the controller or the processor, especially as regards the identification of the risk related to the processing, their assessment in terms of origin, nature, likelihood and severity, and the identification of best practices to mitigate the risk, could be provided in particular by means of approved codes of conduct, approved certifications, guidelines provided by the Board or indications provided by a data protection officer. The Board may also issue guidelines on processing operations that are considered to be unlikely to result in a high risk to the rights and freedoms of natural persons and indicate what measures may be sufficient in such cases to address such risk.

Article 25 - EU GDPR
"Data protection by design and by default"

1. 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, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, 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.
2. The 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. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.
3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

Suitable recitals

Recital 78
Appropriate technical and organisational measures
The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations. The principles of data protection by design and by default should also be taken into consideration in the context of public tenders.

Controller and *processor*, but today we have the figure of *prossimer* and the algorithm is *not mere tool*, but with the scheme *if this than that* it becames an essential element of *"automatic decision"*.The privacy is not a static, but dynamic concept.

1. Accountability.

Accountability is a common principle for organisations across many disciplines; the principle embodies that organisations live up to expectations for instance in the delivery of their products and their behaviour towards those they interact with. The General Data Protection Regulation (GDPR) integrates accountability as a principle which requires that organisations put in place ap-

propriate technical and organisational measures and be able to demonstrate what they did and its effectiveness when requested.

Organisations, and not Data Protection Authorities, must demonstrate that they are compliant with the law. Such measures include: adequate documentation on what personal data are processed, how, to what purpose, how long; documented processes and procedures aiming at tackling data protection issues at an early state when building information systems or responding to a data breach; the presence of a Data Protection Officer that be integrated in the organisation planning and operations etc.

In 2015, in anticipation of the GDPR, the EDPS initiated a project to develop a framework for greater accountability in data processing to be applied to our own organisation, as an institution, a manager of financial resources and people - and a controller.

In addition, we have started to promote the accountability principle through visits to small, medium and large EU bodies to explain the new obligations resulting from the revised legal framework and the implications for EU institutions and the EDPS' work as their supervisory authority.

Accountability is one of the data protection principles - it makes you responsible for complying with the GDPR and says that you must be able to demonstrate your compliance.

You need to put in place appropriate technical and organisational measures to meet the requirements of accountability.

There are a number of measures that you can, and in some cases must, take including:

- adopting and implementing data protection policies;
- taking a 'data protection by design and default' approach;
- putting written contracts in place with organisations that process personal data on your behalf;
- maintaining documentation of your processing activities;
- implementing appropriate security measures;
- recording and, where necessary, reporting personal data breaches;
- carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests;
- appointing a data protection officer; and
- adhering to relevant codes of conduct and signing up to certification schemes.

Accountability obligations are ongoing. You must review and, where necessary, update the measures you put in place.

If you implement a privacy management framework this can help you embed your accountability measures and create a culture of privacy across your organisation.

Being accountable can help you to build trust with individuals and may help you mitigate enforcement action.

There are two key elements. First, the accountability principle makes it clear that you are responsible for complying with the GDPR. Second, you must be able to demonstrate your compliance.

Taking responsibility for what you do with personal data, and demonstrating the steps you have taken to protect people's rights not only results in better legal compliance, it also offers you a competitive edge. Accountability is a real opportunity for you to show, and prove, how you respect people's privacy. This can help you to develop and sustain people's trust.

Furthermore, if something does go wrong, then being able to show that you actively considered the risks and put in place measures and safeguards can help you provide mitigation against any potential enforcement action. On the other hand, if you can't show good data protection practices, it may leave you open to fines and reputational damage.

Accountability is not a box-ticking exercise. Being responsible for compliance with the GDPR means that you need to be proactive and organised about your approach to data protection, while demonstrating your compliance means that you must be able to evidence the steps you take to comply.

To achieve this, if you are a larger organisation you may choose to put in place a privacy management framework. This can help you create a culture of commitment to data protection, by embedding systematic and demonstrable compliance across your organisation. Amongst other things, your framework should include:

- robust program controls informed by the requirements of the GDPR;
- appropriate reporting structures; and
- assessment and evaluation procedures.

If you are a smaller organisation you will most likely benefit from a smaller scale approach to accountability. Amongst other things you should:

- ensure a good level of understanding and awareness of data protection amongst your staff;
- implement comprehensive but proportionate policies and procedures for handling personal data; and
- keep records of what you do and why.

Article 24(1) of the GDPR says that:

- you must implement technical and organisational measures to ensure, and demonstrate, compliance with the GDPR;
- the measures should be risk-based and proportionate; and
- you need to review and update the measures as necessary.

While the GDPR does not specify an exhaustive list of things you need to do to be accountable, it does set out several different measures you can take that will help you get there. These are summarised under the headings below, with links to the relevant parts of the guide. Some measures you are obliged to take and some are voluntary. It will differ depending on what personal data

you have and what you do with it. These measures can form the basis of your programme controls if you opt to put in place a privacy management framework across your organisation.

Should we implement data protection policies?

For many organisations, putting in place relevant policies is a fundamental part of their approach to data protection compliance. The GDPR explicitly says that, where proportionate, implementing data protection policies is one of the measures you can take to ensure, and demonstrate, compliance.

What you have policies for, and their level of detail, depends on what you do with personal data. If, for instance, you handle large volumes of personal data, or particularly sensitive information such as special category data, then you should take greater care to ensure that your policies are robust and comprehensive.

As well as drafting data protection policies, you should also be able to show that you have implemented and adhered to them. This could include awareness raising, training, monitoring and audits - all tasks that your data protection officer can undertake (see below for more on data protection officers).

Privacy by design has long been seen as a good practice approach when designing new products, processes and systems that use personal data. Under the heading 'data protection by design and by default', the GDPR legally requires you to take this approach.

Data protection by design and default is an integral element of being accountable. It is about embedding data protection into everything you do, throughout all your processing operations. The GDPR suggests measures that may be appropriate such as minimising the data you collect, applying pseudonymisation techniques, and improving security features.

Integrating data protection considerations into your operations helps you to comply with your obligations, while documenting the decisions you take (often in data protection impact assessments - see below) demonstrates this.

Whenever a controller uses a processor to handle personal data on their behalf, it needs to put in place a written contract that sets out each party's responsibilities and liabilities.

Contracts must include certain specific terms as a minimum, such as requiring the processor to take appropriate measures to ensure the security of processing and obliging it to assist the controller in allowing individuals to exercise their rights under the GDPR.

Using clear and comprehensive contracts with your processors helps to ensure that everyone understands their data protection obligations and is a good way to demonstrate this formally.

The above measures can help to support an accountable approach to data protection, but it is not limited to these. You need to be able to prove what steps you have taken to comply. In practice this means keeping records of what you do and justifying your decisions.

Accountability is not just about being answerable to the regulator; you must also demonstrate your compliance to individuals. Amongst other things, individuals have the right to be informed about what personal data you collect, why you use it and who you share it with. Additionally, if you use techniques such as artificial intelligence and machine learning to make decisions about people, in certain cases individuals have the right to hold you to account by requesting explanations of those decisions and contesting them. You therefore need to find effective ways to provide information to people about what you do with their personal data, and explain and review automated decisions.

The obligations that accountability places on you are ongoing - you cannot simply sign off a particular processing operation as 'accountable' and move on. You must review the measures you implement at appropriate intervals to ensure that they remain effective. You should update measures that are no longer fit for purpose. If you regularly change what you do with personal data, or the types of information that you collect, you should review and update your measures frequently, remembering to document what you do and why.

2. The principle of accountability.

The General Data Protection Regulation (GDPR) introduces a new principle to data protection rules in Europe: that of accountability. The GDPR requires that the controller is responsible for making sure all privacy principles are adhered to. Moreover, the GDPR requires that your organisation can demonstrate compliance with all the principles. So, which steps should your organisation take to build such a culture and to be able to demonstrate accountability?

Firstly, the organisation must know what principles need to be adhered to. There are six principles set out in the GDPR. These are the principles of lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, and integrity and confidentiality. One of the best ways to make sure these principles are adhered to is to make sure your internal privacy governance structure is set up correctly and comprehensively.

The ways to incorporate these principles are woven in throughout the GDPR. For instance, the GDPR states your organisation is required to deploy appropriate technical and organisational measures as laid out in the GDPR. Some (new) measures mentioned in the GDPR are: documented processes/policies, data protection impact assessments (DPIA), suggested data security methods, data protection by design and by default, a mandatory data protection officer (DPO) for large scale personal data processing, and keeping records of your processing activities. Special attention is given to (industry) code of conducts and self-certification, data breach notification and transparency requirements.

3. A culture and organisational change.

A strong governance structure is essential to standardise privacy and develop privacy by design and default. To create a cultural and organisational change for GDPR compliance within your organisation, buy-in from stakeholders is of significant importance. By developing internal guidelines for employees, compliance with legal obligations for data processing and securing data can be ensured. Incorporate training and awareness programs for everyone who is going to be involved in the processing of personal data. Your organisation can also consider subscribing to an industry code of conduct or creating internal guidelines and a review process for data analytics.

Subscribing to an industry code of conduct can demonstrate compliance, especially when the certifications are issued by the certification bodies. These mechanisms are not obligatory under the GDPR, but are highly recommended. Developing your own ethical standards with respect to processing personal data, may further enhance your accountability efforts. The risks of new initiatives are weighed against possible benefits. Questions like 'can we legally do this?' should be complemented by 'do we want to do this and how will it be perceived by our customers?' to safeguard the ethical use of the data.

Furthermore the GDPR obligates your organisation to maintain an internal record of all your processing activities. Your organisation is, among others things, required to record the purposes of the processing and a description of technical and organisational security measures.

New in the GDPR is the requirement to designate a Data Privacy Officer (DPO) within your organisation. Although the requirement is only mandatory in certain circumstances, a DPO can monitor the activities of your organisation and the processing activities to help you become compliant with the GDPR.

4. Conclusion.

Today this system of rules is not enough. The level of protection must follow the technology.

The Commission has made a proposal of *Digital Service Act* that will introduce a concept of accountability in terms of strict liability for contents of Big Data. Data are considered important items of digital economy, making the concept of *Data Driven Economy.* It is important to create a multilevel system of protection, enhancing the power of inspection and injunction of SA with *pre-emptive remedy* and with *web-tax* to regulate economic influence of social platforms. The criteria of *One stop Shop* and *consistency mechanism* must be integrated by common european culture of right of privacy in a general context of safeguard of human rights.