Accountability in the EU Data Protection Reform: Balancing Citizens' and Business' Rights

Lina Jasmontaite, Valerie Verdoodt

Accountability in the EU data protection reform: Balancing citizens' and business' rights

Lina Jasmontaite & Valerie Verdoodt

KU Leuven – Centre for IT and IP Law – iMinds, Leuven, Belgium

lina.jasmontaite@law.kuleuven.be, valerie.verdoodt@law.kuleuven.be

Abstract. The principle of accountability has been present in the field of data protection and privacy for several decades. Recently, accountability as a data protection principle gained fresh prominence with the revision of the data protection frameworks by the leading actors – the OECD, the Council of Europe, and the European Union. Anticipating the adoption of the General Data Protection Regulation, this contribution examines the positions of the EU legislative actors on Article 22 defining the responsibility of the data controller ("the general accountability article"). To date, there has been little agreement on the limitations of the newly introduced Article 22 and its practical implications for individuals and business. As such, this contribution analyses the debates that took place among the Council of the EU, the European Parliament and the European Commission throughout the negotiation process of General Data Protection Regulation. The contribution aims at providing new insights into the underpinning values and objectives of the accountability article.

Keywords. Accountability · controllers · data subjects · the General Data Protection Regulation · a risk-based approach· a rules-based approach · a principles-based approach · processors.

1 Introduction

In the field of data protection, the principle of accountability has been rather implicit and mostly referred to as the responsibility of data controllers for their data processing activities. In this respect, Article 22 on the responsibility of the controller ("the general accountability article") of the draft General Data Protection Regulation ("Regulation") was not revolutionary. Nevertheless, if adopted in its initial form as proposed by the EC, the general accountability article would have marked a new development within the EU data protection framework by introducing a non-exhaustive list of accountability measures for data controllers. Indeed, it would not only have required data controllers to develop policies addressing the management of personal data but also to imple-

ment measures allowing demonstration of compliance with the EU data protection framework. The initial draft Regulation foresaw five measures facilitating the implementation of the accountability principle in practice (see infra). As the EU data protection reform is almost completed, the final text of the general accountability article is known.[1] Accordingly, it is timely to analyse the past and current discussions on Article 22 to gain a better idea of the practical implications of this provision.

It seems that the amendments put forward by the European Parliament ("Parliament"), as well as the Council of the EU ("Council"), prevailed over the initial EC's approach. The Parliament and the Council suggested to delete the non-exhaustive list of accountability measures and leave only the general requirement for data controllers to "implement appropriate measures" and be able to demonstrate compliance with the legal framework (Council of the EU 2015). In view of the compromise text of the Regulation, we question the significance and the impact of Article 22 for EU citizens and business.

The aim of this paper is to examine the practical implications of the accountability measures for both business and citizens' rights. To achieve this objective, the contribution reflects on the origin and layout of the general accountability provision. Then, it reflects on the EU legislators' debates on the provision. In the subsequent sections, the paper compares and analyses the different views of the Commission, the Parliament and the Council on Article 22. The concluding part recognises that the issue of implementing accountability in practice is an intriguing one and needs to be further addressed in research analysing the attribution of responsibilities between controllers and processors.

2 Accountability in the field of data protection and privacy

To better understand the discussions on the accountability principle, one has to grasp the general obligations arising from accountability, such as reporting and explaining policies and actions taken with respect to one's business practices. The following sections go beyond the general premise that being accountable

[1] This contribution was initially drafted in November 2015. The text was revised in February 2016 and now includes references to the compromise text of political agreement, published by the Council of EU on the 28 January 2016. At the moment, it is estimated that the final text of the General Data Protection Regulation will be published in Official Journal in June 2016. Note that the numbering of the provisions and recitals may change in the final version of the General Data Protection Regulation.

is being transparent and responsible to your stakeholders for your performance and conduct, and give a brief overview of accountability debates in the context of the EU data protection reform.

2.1 The concept of accountability

The concept of accountability is relevant for different sectors ranging from public administration and finance to data protection and ICT. Accordingly, accountability entails different meanings that are assigned to it by various scholars and organisations. A definition that has been widely recognised originates from the governance scholar, Bovens, defining accountability as both a virtue that entails "a normative concept, as a set of standards for the behaviour of actors, or as a desirable state of affairs" and as a mechanism "that involves an obligation to explain and justify conduct" (Bovens 2010). An example of such a mechanism could be an obligation to demonstrate that the processing of personal data is in compliance with the EU data protection framework.

In the field of data protection and privacy, "accountability is [considered to be] a form of enhanced responsibility" (Bennett 2012). The actual recognition of the principle within EU data protection legislation marks a shift from a primarily reactive approach to a proactive one, according to certain scholars. As per Alhadeff, Van Alsenoy and Dumortier, accountability is "a proactive demonstration of an organization's capacity to comply has the potential of improving the current state of the art in two ways: 1) transparency and confidence for both regulators and data subjects, and 2) greater transparency of corporate practices" (Alhadeff et al 2010). Indeed, the proposed accountability provision requires the controller to adopt policies and implement appropriate measures to ensure, and be able to demonstrate compliance with the data protection framework (EC 2012). At the same time, it is suggested that "accountability instruments are ways to make the [EU] adequacy framework work more effectively" (Bennett 2010). In other words, the introduction of the accountability mechanism can be regarded as a remedy for the widely criticised EU adequacy framework, which prohibits personal data transfers to (third) countries that are not recognised by the Commission as having an "adequate" level of protection as under Directive 95/46/EC.

2.2 The endless debate: 'Who is accountable'?

In Europe, discussions on the question 'who is accountable' in the field of data protection have been influenced by the European Convention for the Protection

of Human Rights and Fundamental Freedoms ("Convention"). The European Court of Human Rights, while interpreting the Convention, has developed a doctrine of positive obligations in its case law (De Hert 2012). According to this doctrine, states have an obligation to take appropriate actions to ensure that citizens can exercise their rights without any constraints (De Hert 2012). In other words, governments are not only required to provide adequate legislation and policies, but they also need to ensure effective enforcement of legislative measures. Furthermore, this doctrine calls for a clear attribution and effective implementation of responsibilities of the actors involved. In the context of privacy and data protection, this means that governments are the main duty-bearers responsible for ensuring that both controllers and processors take an appropriate share of responsibility for the protection of data subjects' rights (De Hert 2012).

While the concept of a controller's accountability has been present ever since the adoption of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data ("Guidelines"), this attribution of responsibility has become controversial because of the growing processors' influence over personal data processing operations (OECD 2013). Some legislators, in particular the Council of Europe, have been addressing this issue in their attempts to modernise the existing data protection frameworks. The Council of Europe seeks to introduce additional obligations for both processors and controllers in the revised Convention No. 108 (Council of Europe 2012). More specifically, the Council of Europe sees processors as active agents who have to take appropriate measures to implement data protection requirements (Article 8 bis). At the moment, the discussions on the modernisation of the Convention No. 108 are still ongoing and the final text of the provision remains uncertain (CAHDATA 2014). Nevertheless, given the support of the Data Protection Authorities to the accountability principle, it is reasonable to expect that additional accountability obligations will be introduced for both controllers and processors (European Conference of Data Protection Authorities 2014).

Similar to the Council of Europe proposal, the Regulation provides input for the accountability debate and the attribution of responsibility between the agents engaged in the processing of personal data. According to Recital 62, one of the main objectives of the Regulation is to clarify the responsibilities of controllers and processors (EC 2012). To achieve this, the general accountability article (Article 22) describes obligations for the controller to comply with the Regulation and to demonstrate compliance. The processor's obligations are

clarified in Article 26, which is partly based on Article 17 (2) of the Data Protection Directive, but also implements new elements. For instance, processors should be regarded as joint controllers if they process data beyond the controller's instructions (EC Explanatory Memorandum 2012). Other new obligations that would apply to both controllers and processors are the documentation obligation (Article 28) and the obligation to carry out a Data Protection Impact Assessment (DPIA). Furthermore, the Regulation would extend liability and the right to compensation of damages caused by processors (Article 77). Therefore, it seems that the concept of accountability in data protection goes beyond the controller's accountability foreseen in Article 22, forcing processors to take their share of responsibility for the protection of personal data.

At the same time, the debate on accountability essentially relates to the evolving role of national data protection authorities and data subjects. The latter are no longer seen as "merely passive objects who require protection of the law against exploitation" (EDPS 2015). Indeed, individuals actively engage in online services and generate content. Therefore, it is suggested that citizens should bear responsibility for their choices made in the online environment, similarly to the situation in the offline world, rather than merely being the ones to whom controllers and processors should be accountable (EDPS 2015).

3 Towards the EU institutions' agreement on accountability

Now that the concept of accountability and the actors involved have been discussed, the following section of the paper focuses on the accountability debate within the EU data protection reform. The section firstly introduces the initial EC proposal for the accountability provision and then addresses the positions of the European Parliament and the Council of the EU.

3.1 The EC rules-based approach: More prescriptions yet no remedy?

As indicated, the EC proposal for the General Data Protection Regulation introduced a non-exhaustive list of mechanisms to implement the accountability principle for controllers in Article 22. The first mechanism encompassed documentation requirement, according to which, controllers should keep relevant documentation of "all processing operations under its responsibility" (Article 28) (EC 2012). The second mechanism included security obligations, according to which, controllers should take appropriate technical and organisational measures ensuring an adequate level of security of the processing operations (Article 30). The third mechanism required controllers to conduct a DPIA in

situations where the processing may "present risks to the rights and freedoms of data subjects" (Article 33). The fourth mechanism included an obligation for controllers to obtain an authorisation from the DPA prior to the processing operations in cases where the DPIA is required or the DPA deems it to be necessary (Article 34). Lastly, the fifth mechanism addressed a designation of a data protection officer ("DPO") who would be responsible for the entity's compliance with the EU data protection framework (Article 35). It should be noted that while the draft Regulation, published by the EC explicitly, listed the DPO appointment amongst the accountability measures, it would have been obligatory only in a limited number of situations.

With regard to the non-exhaustive list of accountability measures, it seems that the EC's position was shaped by the opinions of the Article 29 Data Protection Working Party ("Working Party"), which presents the views of the European national data protection authorities ("DPAs"). The Working Party has suggested to introduce the accountability principle in response to the EC call for consultation on a comprehensive approach of the EU data protection framework (Article 29 Working Party, WP168). The European DPAs suggested that in order to be accountable, data controllers (depending on the nature of their data processing activities) should take both proactive and reactive measures (Article 29 Working Party, WP168). The following section discusses the positions of and the amendments to Article 22 proposed by the Parliament and the Council.

3.2 EU legislators' discussions during the trilogue

The proposed Regulation, after being embroiled in the EU legislative process since January 2012, entered into the last stage of the first reading process – the trilogue – in 2015. While the Parliament decided on the proposed data protection package in March 2014, by approving amendments proposed by the LIBE Committee (European Parliament 2014), the Council of the EU ("Council") struggled to reach a political agreement. After difficult deliberations, the Council adopted a common position on the proposal in June 2015. Having political agreements in both the Parliament and the Council allowed to proceed with further negotiations in the trilogue stage.

The amendments of the Parliament sought to clarify the responsibilities of controllers under Article 22. The Parliament specified that controllers should develop "appropriate policies and implement appropriate and demonstrable technical and organizational measures" (LIBE 2014). In particular, the Parliament suggested to develop compliance measures that would take into consideration "the state of the art, the nature of personal data processing, the context, scope

and purposes of the processing, the risks for the rights and freedoms of the data subjects and the type of the organization, both at the time of the determination of the means for processing and at the time of the processing itself" (LIBE 2014). Aside from the amendments related to the proportionality principle, the Parliament followed up on the European Data Protection Supervisor's recommendation and introduced a requirement to review, and, if needed, update compliance policies every two years (LIBE 2014). The Parliament also took into consideration recommendations of civil liberty groups and included a new obligation for publicly listed companies requiring to summarise the implemented accountability mechanisms in "any regular general reports of the activities" (LIBE 2014).

The Council on the other hand introduced a risk based approach according to which the controller, when implementing accountability mechanisms, would have to consider "the nature, scope context and purposes of the processing as well as the likelihood and severity of risk for the rights and freedoms of individuals" (Council of the EU 2015 (June)). The contributions of delegations submitted in fall 2014 reveal that the Member States were considering the use of both "high risks" and "low risks", yet the concept of "high risks" prevailed (Council of the EU 2014 (September)). It can be observed that despite delegations representing Denmark, Germany, the Netherlands, Portugal, and the United Kingdom expressed doubts about the costs associated with the implementation of the accountability provision, the Member States reached a satisfactory agreement (Council of the EU 2014 (July)).

While there were many differences between the positions of the Parliament and the Council, there were also several similarities. Both the Parliament and the Council suggested to delete the non-exhaustive list of measures implementing the accountability principle from the final text of the Regulation (Council of the EU 2014 (August)). Furthermore, both EU institutions emphasised the need to reflect on the nature, context, scope and risk associated with the data processing when selecting accountability mechanisms. However, the Council's amendments to the article entailed a more business-friendly approach. The Council was striving for an accountability provision that would not be overly prescriptive and leave discretion to data controllers to select measures implementing the provision in practice.

4 Practical implications of the general accountability article

After analysing the positions of the EU institutions, it is timely to reflect on the actual implications of the newly introduced Article 22 in practice. This section will first reflect on how accountability relates to the key principles of good governance, which are also embedded in the EU data protection framework. Second, it will further investigate the implications of the proposed general accountability article for data subjects and businesses, in light of the different positions of the EC and the Council. On the one hand, the EC advocated for a prescriptive, rules-based approach and included the non-exhaustive list of measures, which were supposed to be applicable to data controllers when processing personal data. On the other hand, the Council insisted on a risk-based approach (or a principle-based approach) with respect to the accountability principle. In particular, the Council suggested to correlate accountability measures with risks associated with a particular processing and to remove the list of accountability measures.

4.1 Good governance meets data protection

In general, good governance facilitates the implementation of the human rights' framework, and, as such, is relevant in the context of data protection where the fundamental rights to privacy and data protection are at stake. The Working Party has played an important role in providing guidance on how accountability in the context of data protection links to elements of good governance, such as transparency, proportionality and a risk-based approach. It could be argued that by introducing the accountability principle in the GDPR, the elements of good governance will be formally integrated in the EU data protection framework. Consequently, this may have a positive impact on rights of data subjects and businesses.

Transparency - a first step on the path to empowerment.

First, the Working Party recognises a close link between accountability and the notion of transparency in its opinions (WP217). In particular, the Working Party considers transparency to be "an integral element of many accountability measures" (WP173). In the context of big data analytics, for instance, the Working Party lists transparency among the additional safeguards preventing undue impact on data subjects (WP203). Moreover, transparency is deemed to be a precondition for user empowerment, as it would allow data subjects to exercise

their rights more effectively (WP203). To this end, the Working Party recommends data controllers to document the internal assessment conducted at the purpose specification stage (WP203). Such documentation would allow data controllers to demonstrate compliance with legal requirements, and additionally, could facilitate an easier demonstration of accountability. Accordingly, the Working Party has recognised that documentation could (in certain cases) facilitate the exercise of data subjects' rights and enforcement actions of national data protection authorities (WP217). Finally, being transparent vis-à-vis data processing practices can be a competitive advantage as it enhances user trust in online services.

Proportionality calls for a balanced approach.

Secondly, the Working Party has established a link between accountability and proportionality. For instance, if controllers opt for their legitimate interest as the ground legitimising the data processing (Article 7 (f) Directive 95/46/EC), controllers should perform a balancing test at the time of specifying the purposes of data collection. The balancing test would allow to determine whether the controller has a legitimate interest to undertake the foreseen data collection in a particular situation and whether that processing will not impinge on data subjects' rights (WP217). Moreover, the balancing test would allow to take into consideration the context and purposes of the processing as well as the risks in relation to the fundamental rights and freedoms of individuals.

Risk-based approach as an integral part of accountability.

Finally, at the core of good governance programmes lies the concept of "risk management", which includes the processes of identification, assessment, monitoring, mitigation and re-evaluation of risks. The Working Party has clarified that the core element of accountability in the data protection context is a risk based-approach (WP218). Specifically, the following provisions are developed with a risk based-approach in mind:

- the obligations of security (Article 30),
- the data protection impact assessment (Article 33),
- the data protection by design principle (Article 23),
- the obligation for documentation (Article 28), and
- the certification and codes of conduct (Articles 38 and 39).

The above listed provisions allow data controllers to select appropriate measures ensuring compliance with data protection rules. Furthermore, the provisions are based on the principle of proportionality and, as such, allow for business models, sectors and the particular risks associated with the processing of personal data to be taken into consideration. Developing measures on a case-by-case basis could ensure scalability of the accountability principle (WP173). In addition, the assessment and evaluation of the risks associated with the processing of personal data can enhance the practice of written policies and documentation. Therefore, it can be observed that the elements of good governance may benefit data subjects and businesses.

The following two sections of this paper will discuss the potential impact of the accountability measures as proposed by the Commission and the Council on data subjects and businesses.

4.2 Accountability measures to empower individuals?

First of all, the potential impact of the proposed accountability article on data subjects' rights such as the right to access, the right to be informed and the right not to be subjected to automated processing in certain circumstances will be examined. It should be noted that Article 22 does not refer to data subjects' right per se. Data subjects' rights and controllers' obligations to respect these rights are specified in the third chapter of the Regulation.

The third chapter strengthens the existing data subjects' rights (e.g., right to access) and introduces new ones (e.g., right to data portability). Accordingly, it attains the core objective of the EU data protection reform, namely to empower data subjects. In particular, this objective is achieved by moving the primary responsibility for data protection enforcement from the individual (i.e., the data subject filing complaints with the DPA) to the organisation that processes personal data (i.e., the data controller) (Alhadeff et al 2012). In other words, the initial aim of Article 22 was to move the EU data protection rules from a reactive or complaint-based approach to a proactive approach, where the controller has to:

(1) ensure compliance with the data protection framework;

(2) be able to demonstrate that the processing is performed in compliance with the data protection framework; and

(3) be able to verify that it has implemented mechanisms ensuring the effectiveness of the accountability measures (such verification should be carried out by independent internal or external auditors).

When considering the impact of the proactive approach on data subjects, it is worthwhile to reflect on the way data subjects could invoke the redress mechanism. In other words, how could data subjects ensure that controllers implement their accountability obligations? Should they bring complaints or requests directly to controllers or processors or should they rely on the actions of national data protection authorities? Under which conditions could individual data subjects or their representatives bring such claims? In practice, data subjects should bring complaints to their DPA, which then on behalf of a data subject would start an investigation or an enforcement action.

Documentation to facilitate accountable storytelling: Honesty is the best policy.

The EC emphasised the importance of formal procedures and listed documentation among the accountability measures (Article 28). Supporters of this rather prescriptive approach to accountability may argue that it could increase transparency of data controllers' and processors' data processing practices towards individuals and as such increase trust of individuals. In fact, European Digital Rights, an international non-profit association which brings together 33 privacy and civil rights organisations, even advocated a stronger provision which would include an obligation for data controllers and processors to publicly disclose a summary of the implemented accountability measures (EDRI 2012). While this suggestion was supported by the Parliament, it was erased during the trilogue phase.

Nevertheless, it is important to note that the act of documentation can be meaningful to the extent it is honest and truthful. Indeed, account giving should not be about persuasion and manipulation. As per Raab, accountability does not only entail "giving an account" but also challenging an account giver and asking for evidence in support of any claims (Raab 2012). Considering this point of view, the possibility to challenge controllers' and processors' policies and measures taken in a particular data processing operation can empower data subjects.

Data protection impact assessment: The representation of data subjects in the decision-making process.

Secondly, data subjects should be given a voice in the decision-making related to certain processing operations. Indeed, the EC text suggested that controllers and processors take data subjects' views into consideration when conducting DPIA for processing operations that entail "risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes" (EC 2012). While scholars and practitioners generally agree on the DPIA's added value to the data protection framework (and in particular to data subjects' rights) the process of carrying out the DPIA entails several challenges (Wright et al. 2011). Some of these challenges were addressed in the Parliament's amendments introducing categories of information that need to be included in a DPIA and that could potentially enhance the level of transparency of the DPIA process. In particular, it was suggested to include the systematic description of personal data processed, the purposes of the operations, the assessment of the necessity and proportionality of the processing and the measures to mitigate the identified risks to individuals (Council of the EU 2015 (June)).

The Council, on the other hand has diluted the scope of an obligation to carry out a DPIA by limiting it only to controllers (Council of the EU 2015 (June)). As a result, many businesses that process personal data on behalf of the controller will be excluded from its application. Moreover, the Council followed a risk-based approach and suggested to only conduct a DPIA "where a type of processing […] is likely to result in a high risk for the rights and freedoms of individuals" (Council of the EU 2015 (June)). Limiting the scope of the obligation would favour businesses rather than individuals, and as such it is not welcomed by privacy advocates.

Data Protection Officer: An enabler of data subjects' rights.

Although Article 18 of Directive 95/46/EC already refers to a "Data Protection Officer" the mandatory appointment of a DPO would mean a new obligation for both controllers and processors in most of the EU Member States. The initial requirement, as proposed by the EC, for businesses with more than 250 employees to appoint such an officer was met with resistance (EUROCHAMBRES 2012). In particular, the new obligation triggered discus-

sions on indicators of high risks of data processing activities among stakeholders (BEUC 2012). The Parliament took this debate further by suggesting that businesses should appoint a DPO where processing operations exceed "more than 5000 data subjects in any consecutive 12-month period" (LIBE 2014). As far as this provision is concerned, it seems that the Council sided with businesses – it deleted the mandatory nature of the DPO. By doing so, the Council not only awarded data controllers (and processors) with more flexibility when it comes to appointing a DPO but also with a possibility to save on personnel costs. This being said, it should be noted that a DPO would be responsible for a company's compliance with the EU data protection framework and for handling data subjects' access requests. The latter point is often undermined, yet it is in the interest of data subjects that companies appoint a DPO – a contact person – who would essentially facilitate the exercise of individuals' rights to access, rectification and deletion of the collected personal data.

Prior authorisation and prior consultation: Adding a layer of accountability.

Getting rid of the prior notification requirement to the DPAs was one of the objectives of the EU data protection reform. Primarily this change was considered in the business context because it would allow cutting the costs of the administration and speed up the decision-making process of new processing operations. In fact, the prior notification requirement is not deemed to be a tool protecting data subjects' rights, but rather a way for a DPA to learn about the scale and scope of data processing operations in its jurisdiction. Accordingly, the purpose of prior authorisation or prior consultation is fundamentally different from the current prior notification to the DPA. Prior authorisation or consultation would be limited to situations where a DPIA would conclude that the processing operations pose high risks to data subjects' rights. In response to requests for a consultation, DPAs could issue recommendations on how to address and mitigate specific data protection risks. These recommendations could in turn foster the protection of data subjects' rights.

The Parliament supported such a measure, yet it suggested limiting it to situations where the controller and processor did not appoint a DPO, or where the DPO or DPIA would have concluded that such consultation is necessary. The Council amendments on the other hand wreck the rationale of Article 34 and the concept of prior checking as set forth in Article 20 of Directive 95/46/EC. The Council suggested making the consultation of the DPA mandatory only for the controllers (and not processors) "in the absence of measures to be taken by

the controller to mitigate the risk" ( ). In practice, however, such a situation seems highly unlikely.

Data security requirements for controllers and processors: Secure processing.

The draft Regulation listed the implementation of data security requirements among the accountability mechanisms for controllers in Article 22. However, Article 30 requires both controllers and processors to take appropriate technical and organisational measures that would ensure adequate security of personal data. Both the Parliament and the Council supported this provision and added that those measures should be proportional and take into consideration the state of the art of available technology. The Parliament further specified this obligation by requiring controllers and processors to have a security policy, which would "ensure the ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data" (LIBE 2014). It could be argued that this attribution of responsibilities between controllers and processors benefits both business and citizens. Indeed, the Regulation will force processors to step up and accept their share of responsibility for the implementation of accountability and the compliance with the data security requirements.

4.3 Accountability is a burden for business: in need of deep pockets

While it is argued that the general accountability article will create a data protection culture within companies, it can be speculated that those prescriptive obligations would significantly increase the administrative burden and costs of compliance for businesses (BEUC 2012). For instance, the Dutch delegation to the Council of the EU has estimated that obligatory documentation, DPIA and designation of a data protection officer would result in a significant (up to double) increase of compliance costs for businesses (Council of the EU 2014 (September)). Due to the potential increase of business costs, the proposed article was especially criticised by representatives of small and medium enterprises ("SMEs"). For example, the European Small Business Alliance ("ESBA"), an NGO representing the interests of SMEs considered an obligation to conduct a DPIA appropriate only if the processing of data is part of the SME's core activity. It also pointed out that the appointment of a DPO would unrealistically burden newly set up SMEs.

Indeed, businesses will not be keen on implementing such obligations, unless there are strong incentives for doing so (e.g., a reduction of fines or limitation

of their liability in case of a data breach). On several occasions, the Working Party examined the extent to which DPAs should take into consideration a data controller's implementation attempts when deciding on an appropriate sanction. As per the Working Party, merely implementing the principle does not imply compliance of a data controller with data protection legislation (WP173). In other words, the implementation of various accountability measures would not exempt data controllers or processors from law enforcement actions. At the same time, perhaps each national DPA could clarify its position on this matter.

5 Conclusion

This contribution has provided an overview of discussions surrounding the accountability principle as introduced in Article 22 of the General Data Protection Regulation. The chapter went beyond the mere description of the initial EC text and provided insights into the debates of the EU legislators on the accountability provision. As the final text of the General Data Protection is available, it can be concluded that the foreseen potential of the general accountability article has been significantly reduced. The final wording of Article 22 to some extent reiterates Article 30 governing issues related to the security of processing, whereas it was expected that the proposed provision would mark a shift from a reactive to proactive approach regarding the protection of personal data.

While the general accountability provision is limited to controllers, the EC (in its initial proposal) included processors in several of the articles specifying accountability measures (i.e., documentation, DPIA, prior authorisation or prior consultation of the supervisory authority, appointment of a DPO and security). The authors are inclined to believe that having formal legal accountability requirements for both processors and controllers would be an ideal situation. Indeed, only the clear attribution of responsibilities between actors involved in data processing operations would have benefited the protection of a data subject's rights and freedoms. Other changes concerning Article 22 (i.e., deletion of the non-exhaustive list and removal of a requirement to "adopt policies adopt policies") may have no significant impact on data subjects' rights or on business because the subsequent provisions in Chapter IV outlining obligations of controllers and processors further clarify accountability mechanisms.

Article 22 now entails a flexible, risk based-approach, which requires data controllers to implement appropriate organisational and technical measures and be able to demonstrate such measures. Considering the expectations and the final text of this provision, it can be suggested that the accountability principle, as

formulated in the political agreement among the EU legislators, signifies the need to re-open a wider debate on the scope and meaning of accountability in the field of data protection.

This paper was made possible by the funding of the EU Seventh Framework Programme projects: the PARIS project (PrivAcy pReserving Infrastructure for Surveillance), grant no. 312504; the EPISECC project (Establish Pan-European information space to Enhance seCurity of Citizens), grant no. 607078; and the PREEMPTIVE project (Preventive Methodology and Tools to Protect Utilities), grant no. 607093. It also received funding from the IWT in the context of the SBO project on Security and Privacy for Online Social Networks (SPION) (www.spion.me), as well as the Flemish research institute iMinds (www.iminds.be).

6 References

1. Alhadeff, J., Van Alsenoy, B., Dumortier, J.: The accountability principle in data protection regulation: origin, development and future directions. In Guagnin, D., Hempel, L., Ilten, C., Kroener, I., Neyland, D., Postigo H. (eds.), Managing Privacy through Accountability, Springer (2012)
2. Article 29 Working Party Working Party, The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data (WP168)
3. Article 29 Data Protection Working Party, Opinion 3/2010 on the principle of accountability (WP173)
4. Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation (WP203)
5. Article 29 Data Protection Working Party, Opinion 06/2014 on the Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP217)
6. Article 29 Data Protection Working Party, Statement on the role of a risk based approach in data protection legal frameworks (WP218)
7. Association of European Chambers of Commerce (EUROCHAMBRES), EC proposal for a General Data Protection Regulation, available at: http://www.eurochambres.eu/objects/1/Files/PositionPaperDataProtectionRegulation.pdf
8. BEUC the European Consumer Organisation (BEUC), Data Protection Proposal for a Regulation BEUC Position Paper, available at: https://epic.org/privacy/BEUC-Position-Paper.pdf

9. Bennett, C.: “International Privacy Standards: Can Accountability Be Adequate?” Privacy Laws and Business International, Vol. 106 (2010)

10. Bennett, C.: The Accountability Approach to Privacy and Data Protection: Assumptions and Caveats. In Guagnin, D., Hempel, L., Ilten, C., Kroener, I., Neyland, D., Postigo H. (eds.), Managing Privacy through Accountability, Springer (2012)

11. Bovens, M.: Two Concepts of Accountability: Accountability as a Virtue and as a Mechanism, West European Politics, 946 — 967 (2010)

12. Council of the EU, Delegations Comments on Risk Based Approach (12267/2/14), 2 September 2014, http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2012267%202014%20REV%202

13. Council of Europe, Modernisation proposals adopted by the 29th Plenary meeting (2012) 8 bis

14. Council of Europe, Ad Hoc Committee on Data Protection (CAHDATA), Working Document on Convention 108 with Additional Protocol and Modernisation proposals, Strasbourg, 25 March 2014

15. Council of the EU, General Data Protection Regulation - Preparation of a general approach, June 2015

16. Council of the EU, Delegations Comments on Risk Based Approach (12267/2/2014 September 2, 2014), available at: http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2012267%202014%20REV%202

17. Council of the EU, Risk Based Approach (11481/14 July 3, 2014), available at: http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2011481%202014%20INIT

18. Council of the EU, 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 (General Data Protection Regulation) - Chapter IV (12312/14 August 1, 2014), available at: http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2012312%202014%20INIT

19. Council of the EU, 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 (General Data Protection Regulation) - Preparation of a general approach (9565/15 June 11, 2015), available at: http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf (“Council of the EU, General Data Protection Regulation - Preparation of a general approach, June 2015”)

20. De Hert, P.: From the principle of accountability to system responsibility key concepts in data protection law and human rights discussions. In Guagnin, D., Hempel, L., Ilten, C., Kroener, I., Neyland, D., Postigo H. (eds.), Managing Privacy through Accountability, Springer (2012)

21. Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (O.J. L 281 31) (Directive 95/46/EC)

22. EC, 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 (General Data Protection Regulation) January 2012

23. EC, Explanatory Memorandum to the proposal for a General Data Protection Regulation, 20 January 2012, 10, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011&from=en

24. European Conference of Data Protection Authorities, Resolution on the revision of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), Strasbourg, 5 June 2014

25. European Data Protection Supervisor (EDPS), Opinion 4/2015 Towards a new digital ethics

26. European Digital Rights (EDRi), "Everything you need to know about the Data Protection Regulation", 2012, accessible at http://protectmydata.eu/topics/tasks-and-obligations/

27. European Parliament, Legislative resolution of 12 March 2014 on 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 (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))

28. Raab, C.: The Meaning of 'Accountability' in the Information Privacy Context", in D. Guagnin, L. Hempel, C. Ilten, I. Kroener, D. Neyland, D. and H. Postigo, (eds.), Managing Privacy through Accountability, 2012, Palgrave Macmillan, Vol, 1-27

29. Wright, D., Gellert, R., Gutwirth, S., Friedewald, M.: Precaution and privacy impact assessment as modes towards risk governance. Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields" Von Schomberg, R. (eds.) Publications Office of the European Union, Luxembourg (2011)