The accountability culture in its European union dress. Sticks but no carrots to make the proposed data protection regulation work

Paul de Hert
Vrije Universiteit Brussels & Tilburg University
Dimitra Stefanatou
Tilburg University

1. INTRODUCTION

Having largely influenced governance within the public sector, the concept of accountability is being lately transferred in the private sector too. One might even speak of a culture of accountability, including specific patterns, traits, and products that—although initially emerged in the public sector—are now expanding, increasingly defining governance in the private sector. In the subsequent sections we first demonstrate how accountability is embodied in the proposed data protection framework (section 1 & 2). The discussion elaborates further on why and how accountability appears to be one of the distinct modalities of our time (section 3), paving the ground for a more critical analysis on the way the accountability concept is introduced in the proposed EU regulation (section 4 & 5).

2. ACCOUNTABILITY IN THE PROPOSED EU REGULATION

The European Commission’s proposal for a General Data Protection Regulation\(^1\) puts forward accountability within the field of

\(^1\) Commission, “Proposal for a Regulation of the European Parliament and of The Council on the protection of individuals with regard to the processing
the European data protection. The initiative was followed by the OECD in 2013\(^2\) and fits within a broader global trend with several other world data protection actors considering its introduction too.\(^3\) The original text of the EU proposal establishes explicitly the principle of accountability — a reference to which was missing within the text of the Data Protection Directive\(^4\) and the 1981 Council of Europe Data Protection Convention\(^-\), while introducing a series of accountability provisions\(^5\). Given that accountability raises expectations for a better protected processing of personal data, the proposed provisions were received positively in the broader area of EU data protection. The impact of the proposed provisions on strengthening accountability —especially in the private sector— does call, for further reflection for which it would be useful to seek the link between the particular amendments and the logic hidden behind such a regulatory approach.

According to the definition adopted by the European Data Protection Supervisor (EDPS), —manifestly one of the proponents behind the introduction of the principle as an autonomous principle in the EU—, the accountability principle intends to ensure that data controllers are more generally in control and in the position to ensure and demonstrate compliance with data protection principles in practice.\(^6\) It requires "that controllers put in place internal mechanisms and control systems that ensure compliance and provide evidence—such as audit reports— to demonstrate compliance to external stakeholders, including supervisory authorities". In this context—and taking into account that the accountability principle relates to the reality of data processing—, it is considered that accountability is based upon three components, namely, a) ensuring, b) demonstrating and c) verifying compliance with the data protection rules\(^7\). We will come back to this EDPS definition of accountability below (sub 3).

The interpretation above summarizes the objectives of the accountability framework within the text of the proposed regulation, putting emphasis on the obligations of data controllers to demonstrate and verify compliance. The accountability principle, though, cannot be captured entirely in any kind of exhaustive listing of concrete actions aiming at ensuring, demonstrating or verifying compliance. On the contrary, the EDPS assumes in this respect that data controllers are more "generally" in the position to exercise control implying that accountability goes beyond mere compliance\(^8\) with concrete requirements set by law (see also section 2, below).

---

\(^2\) The 2013 Privacy Guidelines of Organisation for Economic Co-operation and Development (OECD) underlines that data controllers have an important role in making data protection work in practice. A reference to the accountability principle is contained in the following provision: "a data controller should be accountable for complying with measures which give effect to the [material] principles stated above" (Art. 14, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal, 2013).


\(^4\) Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995.

\(^5\) For example, articles 22 and 28 of the Commission’s proposal. EDPS Glossary, https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/71#accountability


In his discussion of reform projects world wide with regard to data protection Gihan Gunasekara, notices that policy makers in Europe, Asia and the US all address similar concerns but that their recommendations reflect some philosophical differences as to the way in which individual rights are balanced against corporate and governmental interests. Accountability is without any doubt part of the global reform wave, both as a concept and driver of new duties such as privacy by design and privacy impact assessments. It is, however, object of different interpretations often as a result of differences in expectations. Some, for example, partly amongst those in the business community, see enhanced accountability as a means to have more light-touch self-regulation and a global playing field with watered down privacy protections, notably those granted to EU citizens. Others, on the contrary, see accountability as a complementary layer of duties particularly targeted at making existing regulations work better in practice.

In a now famous passage in an Opinion on accountability, the Article 29 Working Party highlighted that most of the accountability elements, such as record keeping, (see section 2, below) already existed under the EU Directive, albeit less explicitly and concluded that “(f)rom this perspective, a provision on accountability does not represent a great novelty, and for the most part, it does not impose requirements that were not already implicit in the existing legislation. In sum, the new provision does not aim at subjecting data controllers to new principles but rather at ensuring de facto, effective compliance with existing ones.”

---

9 G. Gunasekara, “Paddling in unison or just paddling?” 2.

At least one strong caveat is warranted. We will see in a next section that in the name of accountability a series of five measures are introduced in the Regulation in order for data controllers to be able to ensure and demonstrate their respect to data protection rules and values. Crucial is that failure to comply with these new rules may result in sanction by regulators. Charlesworth and Pearson observe that every broad interpretation of accountability (also in legal regimes outside the EU with less developed legal rules) might *de facto* lead to greater liability.

Inevitably, accountability will impact the way data controllers deal with complex emerging technologies, such as cloud computing, where multiple actors are involved in processing operations. The accountability obligations imposed on data controllers will influence the type of obligations allocated on joint-controllers and data processors through the contractual agreements concluded. In cases where processing implies the participation of series of processors and sub-processors, the transferred burden of accountability obligations, allocated initially on data controllers across the chain of actors, will lead to the creation of accountability chains.

The following section will discuss the most representative newly introduced accountability obligations assigned to data control-
lers, pointing out the legal consequences established in the form of sanctions, if these obligations are not met. Note that due to the factual influence of multiple actors on the reality of processing nowadays, the proposed Regulation—as explained further below—does not limit liabilities only to data controllers extending them, also, to processors.

2. NEW DUTIES AND SANCTIONS FOR CONTROLLERS AND PROCESSORS IN THE REGULATION

Although “accountability” as a term is solely mentioned in the Explanatory Memorandum, the proposed Regulation dedicates the entire Chapter IV (Articles 22-29) on the obligations of data controllers and processors. The Explanatory Memorandum states in this respect that “Article 22 takes account of the debate on a principle of accountability and describes in detail the obligation of responsibility of the controller to comply with this Regulation and to demonstrate this compliance, including by way of adoption of internal policies and and mechanisms for ensuring such compliance”.

In particular, Article 22(2) lists a series of five measures that must be taken by data controllers, in order for them to be able to ensure and demonstrate that the processing of personal information they perform meets the requirements put in place by the Regulation. The data controllers must, therefore, (a) keep the documentation pursuant to Article 28, (b) implement the data security requirements laid down in Article 30, (c) perform a data protection impact assessment pursuant to Article 33; (d) comply with the requirements for prior authorization or prior consultation of the supervisory authority pursuant to Article 34(1) and (2) and (e) designate a data protection officer pursuant to Article 35(1). Interestingly, the Regulation provides for measures, which

“in particular” data controllers must take, implying that that they are free to take further initiatives, going beyond the minimum requirements set by the text of the Regulation.

The measures above aim at implementing accountability in practice in the sense that they demonstrate tangibly compliance with the provisions of the Regulation, while Article 22(3) provides for the verification of such compliance. It stipulates in this respect that: “The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external auditors”. The formulation of the particular provision seems to endorse an underlying results-oriented criterion: as long as data controllers achieve verifiable results, they are free to decide upon which policies and measures to employ.

The obligation to maintain documentation forms a very fluent example of an accountability obligation, aiming clearly at demonstrating and verifying compliance with the provisions of the Regulation. Article 28 of the proposed Regulation dictates the minimum of the documented information mentioning—among other—the name and the contact details of the controller, or any joint controller or processor, and of the representative, the transfers of data to a third country or an international organization, including the identification of that third country or international organization, a general indication of the time limits for erasure of the different categories of data etc. The obligation for such an extensive book-keeping would not apply, in the case of an organization employing less than 250 employees, for which processing of personal data would not fall under the scope of their main activities. The maintenance of documentation may clearly

15 En the contrary, according to Article 23 of the Data Protection Directive, data controllers are the ones ultimately liable towards data subjects.

16 According to Article 28(5) and (6), it is up to the European Commission to specify further the requirements for the maintenance of the documentation above by issuing delegating acts, while standards forms to be filled in may be included in the implementing acts adopted by the Commission.
help demonstrate and verify compliance, for instance, in the case of investigations carried out by Data Protection Authorities or of performance of internal or external auditors.

The increased obligations imposed on data controllers — and especially the need to demonstrate compliance — could, also, provide to some extent an explanation for another amendment introduced of fundamental importance: the reversal of the burden of proof in favour of individuals at the expense, of course, of data controllers. A reversal of the burden of proof would oblige data controllers to demonstrate that they comply with the law and that the various legal prescriptions were applied faultlessly. Despite the fact that the burden of proof is not included in Article 22 of the draft Regulation, it derives from other provisions in the text (i.e. articles 7, 12 and 19).

The implications of the proposed accountability framework are not limited to the increased responsibilities allocated to data controllers, given that the draft Regulation provides for strict sanctions. The severity of the proposed legal consequences does, indeed, not only relate to the huge penalties possibly imposed (i.e. 2% of a company’s annual worldwide income), but also to the extension of the liabilities to other actors. Although the Data Protection Directive provides solely for the liability of the data controller, the draft Regulation extends liabilities to a series of actors. In particular, article 77 (2-3) states that all controllers and processors involved in the data processing are jointly and severally liable for the entire amount of any damage suffered, unless they can prove that they are not responsible for the event giving rise to the damage. Moreover, article 78 (2) dictates that the representative of a non EU-based data controller is also liable for any penalties assessed against the controller. The implementation of the sanctions described would be mandatory for any intentional or negligent violation of the data protection provisions they relate to, while article 79(3) — in certain limited cases — allows Data Protection Authorities to give simply a warning in written.

3. DEFINITIONS AND REASONS FOR ACCOUNTABILITY

In our first section we discussed the accountability definition adopted by the European Data Protection Supervisor (EDPS): to ensure that data controllers are more generally in control and in the position to ensure and demonstrate compliance with data protection principles in practice. This definition is in line with the one proposed by Mulgan, advocating a limited, core definition of accountability as a term associated with external scrutiny and the process of being called "to account" to some authority for one's actions. Accountability as account-giving has three components that all have to be present: external scrutiny (the account is given to some other body or person outside the organisation), justification (accountability involves social interaction and exchange; one person seeks answers and the other responds or accepts sanctions) and the idea of sanctions and control (the right to demand answers and to impose sanctions).

Mulgan discusses critically many uses of the term that in fact lack one of these three features. In particular he warns against equating all (legal) norms of a given system aiming at regulating behavior of organizations or citizens with accountability. It is better, Mulgan argues, to see accountability mechanisms as only one

---

17 According to article 79(3): In case of first and non-intentional non-compliance with this Regulation, a warning in writing may be given and no sanction imposed, where: (a) a natural person is processing personal data without a commercial interest; or (b) an enterprise or an organisation employing fewer than 250 persons is processing personal data only as an activity ancillary to its main activities.
regulative mechanism co-existing with other control mechanisms, such as legal regulation and constitutional constraints\textsuperscript{20}.

The distinction is subtle but nevertheless defendable\textsuperscript{21}. The five measures proposed by Article 22(2) of the proposed Regulation (above) are, therefore, more correctly to be understood as legal norms aiming at shaping behavior but additionally allowing more accountability in the sense that they facilitate effective reaction by data subjects and data protection authorities.

Today’s governance of the public and private sector is impregnated with the notion of accountability and the use of accounts\textsuperscript{22}. One might even speak of a culture of accountability; the patterns, traits, and products of accountability increasingly define current governance of the public and private sector. There are many expected outcomes and expected benefits. Introducing systems of accounts in management or regulation (translating objectives into a range of indicators such as efficacy rates) and systems of accountabilities (distributions of responsibility for the accounts) can open-up opaque decision-making processes to greater transparency\textsuperscript{23}. Accounts and accountabilities are expected to contribute to financial and operational efficiency and to structuring and transforming chaos into order by requiring “ritualized” repeti-

\textsuperscript{20} R. Mulgan, "Accountability: a ever-expanding concept?", 564.

\textsuperscript{21} "On the other hand, such an extension of meaning is not irresistible. A reasonably clear distinction may still be maintained between accountability and control by which accountability remains merely one means, or set of means, for enforcing control, through the demand for explanation and the imposition of sanctions" (ibid).


\textsuperscript{23} Note that the risk approach and recent turn to accountability should be understood in their historical context as results of public policy failures to address risks in the past. So it is not only about ensuring compliance and the effectiveness of regulation, but it is rooted in historical origins of failures that call for taking people to account.

\textsuperscript{24} D. Neyland, "Parasitic accountability", 846.


\textsuperscript{26} On the reliance of risk-based regulation on firm’s and other organisation’s internal controls, see J. Black, "The emergence of risk-based regulation", 544.

of governing and controlling is one which they can achieve\textsuperscript{28}. A religion or technology of calculation is introduced in the face of uncertainty, where practical action is only focused on what is rendered accountable and on accountable certainty\textsuperscript{29}. This uncertainty can follow from wider global developments (again neoliberalism, but also globalization, climate change, new technologies, ...), but also with smaller things like changing work methods and organization of labor and changing views on care. Accountability in health, for example, has to do with the wider trend of more autonomous work also in the sense of more out door work. With autonomy comes uncertainty, since professionals who undertake identical tasks can demonstrate markedly different levels of competence and performance. For example, medical practitioners can provide services that vary widely from physician to physician in terms of their cost and quality. Accountability then comes as a natural demand since one doctor or person delivers other service levels than others and technology naturally answers to this demand for comparing performances by collecting data\textsuperscript{30}.

An analogy with data processing and the need for accountability in data protection is not far-off. Data processing is in principle allowed under data protection law when respecting the data protection principles that are often open formulated and require application and evaluation. For data processors, but also for national data protection authorities and judges accounts and standard setting through dialogue is the way forward to make data protection effective, hence a world wide trend to co-regulation\textsuperscript{31}, accountability and accounts and risk-based approaches, for instance the recent 2013 update of OECD data protection guidelines\textsuperscript{32}.

One of the merits of this governance turn to accountability fused with a risk approach is that it makes key decisions clearer: how to operationalize objectives; where to focus attention and resources; and, in the face of uncertainty as to which risks will materialize and which will not, which course of action to take\textsuperscript{33}. However, there are limits to the approach and several (often related) risks such as implementation risks (the framework will not in practice be implemented by officials on the ground); design risk (the framework does not capture all the relevant risks); perception risk

\textsuperscript{28} J. Black, "The emergence of risk-based regulation", 544.

\textsuperscript{29} D. Neyland, "Parasitic accountability", 847-848 with ref. to the work of Law & Mol. Also on page 857: "what is counted usually counts".


\textsuperscript{32} Comp. "The core principles have proved to be capable of adapting to the evolution of technology and reality, and there is an increased focus on implementation and enforcement. The key word is really "more effective protection in practice". For instance, newly OECD Guidelines strongly put emphasis on the accountability of responsible organisations: An organisation's data controller must have a data "privacy management program" and be prepared to demonstrate it is appropriate at the request of a privacy enforcement authority. The new Guidelines introduce the concept of a "privacy risk assessment", echoing the "privacy impact assessment" required under the draft European Union data protection regulation. Newly OECD Guidelines insert of a data security breach notification: This US-originated concept covers both notice to an authority and notice to an individual affected by a security breach affecting his/her personal data. Contrary to the draft EU regulation, the OECD's Guidelines take a more risk-based approach by limiting the notification requirement to significant security breaches. OECD Guidelines also include a reference to "privacy enforcement authorities" which did not exist explicitly under the 1980 version" (C. Levaillois-Barth, "Legal Challenges Facing Global Privacy Governance", in C. Dartigueperrou (ed.), (55-62), 59).

\textsuperscript{33} J. Black, "The emergence of risk-based regulation", 547.
4. ACCOUNTABILITY (STICKS) AND REWARDS (CARROTS) IN THE E-PRIVACY DIRECTIVE

The risks, listed above, induce prudence. Empirical research is needed to assess the efficiency of the new accountability & risk ideas. Hutter quotes an American study into safety performance of the American railroads that found a counter-intuitive negative correlation between safety performance and audits and inspections\textsuperscript{38}, and critically ponders whether the transferability of risk management and accountability practices is a good thing.

In EU law accountability and risk elements seem to pop up in all kinds of new regulations dealing with practices that involve high risks for human rights, such as health law or environmental law. The Directive on Transplantation of Human Organs\textsuperscript{39}, for example, stresses the need for a framework governing donation, allocation and/or transplantation of human organs to ensure — among other accountability, in order for regional, national and international bodies to work together.

In the area of data protection, there was a precedent, although from recent date, namely in the field of electronic communication, an area most related to data protection law. The Directive 2009/136\textsuperscript{40} amending the ePrivacy Directive\textsuperscript{41} brings about the

\textsuperscript{34} J. Black, “The emergence of risk-based regulation”, 542-543.
\textsuperscript{36} B. M. Hutter, 11-13.
\textsuperscript{37} As an example, see the sad description of the reality of care work sketched by B.P. Bloomfield & G. McLean, "Beyond the walls of the asylum: information and organization in the provision of community mental health services", Information and Organization, 2003, Vol. 13, 53-84.
\textsuperscript{38} B.M. Hutter, 11 with ref. to Bailey and Peterson, 1989.
underlying accountability concept by imposing accountabilities and accounts and referring to the benefits of implementation of proactive measures.

A new, amended Article 4 of the ePrivacy Directive now requires that any service provider ought to at least limit access to the data to authorized personnel only, to implement hardware and software security measures and to write down and implement a security policy for its processing of personal data. This last requirement—to establish and implement a security policy—becomes a formal obligation for all providers of publicly available electronic communications services in the EU. Limited guidance is provided as to the exact contents of such a policy; the Directive’s Recitals only mention that it “should be established in order to identify vulnerabilities in the system”, leading to periodical “monitoring and preventive, corrective and mitigating action” (Recital 57). In other words, the security policy should not be a static document illustrating the processing methodology but rather a periodical security report on shortcomings of the processing system. Because such policies shall be viewable, controllable and ultimately used as evidence against them, this change is expected to substantially affect service providers in the EU. The new Article 4 adds that national Data Protection Authorities shall audit the security policies and the measures taken by service providers. In addition, these authorities may recommend best practices on the level of security those measures should aim at. This provision, hence, contains an indirect call for soft law to complement the ePrivacy Directive requirements.

The accountability logic is there: more demonstrations are required of data protection compliance to make controls less resource intensive. Another tool to reinforce this picture are the equally new introduced security breach notifications in a new Article 4.3\textsuperscript{13}. “In the case of a personal data breach, the provider of publicly available electronic communications services shall, without undue delay, notify the personal data breach to the competent national authority”. Apart from the relatively straightforward notification requirement to the “competent national authority” (most likely, the Data Protection Authority), those responsible should also notify subscribers and users “when the personal data breach is likely to adversely affect their personal data or privacy”.

But interesting for what follows is that the ePrivacy Directive contains an exemption of the obligation to notify the subscribers and users. This will be the case when the service provider has implemented appropriate technological protection measures. The “appropriateness” of these measures mostly consists in rendering the data unintelligible to any unauthorized person. Evidently, these measures need to have been applied to the data compromised by the security breach. The decision, whether the above conditions concur, is to be made by the data protection authority.

In the foregoing we see a nice example of “sticks and carrots” logic in regulation: for the tortoise to move, both a stick and a carrot are needed; for a governing mechanism to work, both threats and incentives are needed. Under this perspective, the provisioning of sanctions—and not necessary their imposition—and the increased load of obligations seem to hold the role of the stick in the earlier mentioned metaphor, which needs to be coupled, though, with a “carrot”. The “carrot” implies providing for a “suitable” incentive, for an appropriate stimulation that would

\textsuperscript{12} See also Recital 57, 2009 ePrivacy Directive.


\textsuperscript{14} Article 2, 2009 ePrivacy Directive. See also Art. 29 Data Protection Working Party, Opinion 1/2009, p.6 for objections on the introduction of such exemptions.

sufficiently tempt data controllers to move towards the inspired vision of “not mere compliance”. So notification of breaches, always bad for reputation, are not needed when preventive security measures were taken.

5. A CRITICAL APPROACH AT THE WAY ACCOUNTABILITY IS INTRODUCED IN THE REGULATION

Let us now return to our question whether the transferability of risk management and accountability practices from one policy area to another is a good thing. Following the above, it seems that the regulator introduced concepts from the area of data protection, which were previously established in other related areas such as telecommunications. However, especially in the case of the amended ePrivacy Directive and given the additional time offered for implementation at national level, it seems that there has not been sufficient time for the regulator to reflect on the results achieved. Is accountability as embedded in the ePrivacy Directive the successful way to go, in order to regulate similarly the area of data protection in general? Should the regulator not allow for more time to obtain empirical knowledge, before experimenting with a proposal for a Regulation?

These questions are particularly triggered by the increased responsibilities allocated on data controllers—and processors—as well by the strict legal consequences, in case these obligations are not met (see above, section 2). As it is argued, “use the big stick” or “crack the whip” too zealously may be counterproductive. To be too eager or abrasive in enforcement work is to risk encouraging (...) an unco-operative attitude or even downright hostility (...) co-operation cannot be established in the atmosphere of suspicion and distrust that rigid application of the law generates (...). Enforcement takes time\textsuperscript{46}.

---


Under this perspective, it is questionable whether the proposed Regulation provides for any carrots for data controllers. The only truly tempting carrot is the mitigation of administrative sanctions provided in Article 79(3) of the proposed Regulation under certain circumstances, such as the technical and organizational measures and procedures implemented —pursuant to Article 23—and the degree of cooperation with the supervisory authority in order to remedy the breach.

We realize that many demands for exemptions to data protection rules and principles have been made in recent years with a promise to compensate via more self-imposed accountability\textsuperscript{48}, but this is not our line of reasoning. We saw above (section 3) that one category of risks associated with policies of accountability are implementation risks (the framework will not in practice be implemented by persons, in our case data controllers, on the ground). Accountability in data protection is a new and challenging idea. Underlying the importance of a certain reward for data controllers puts the accountability framework introduced by the

---

\textsuperscript{47} It could be argued, perhaps, that the freedom left to data controllers to decide upon the means they employ, in order to comply with their obligations is a sort of compensation against the load of the increased responsibilities.

\textsuperscript{48} Even if that could work in practice as a sort of relief, it remains highly debatable whether it could be taken as real incentive. The same stands for the exception of softer requirements set for the organizations employing less than 250 employees; even if that could actually work as a "carrot" in certain cases, it would simply be indifferent for the large majority of organizations dealing with processing of personal data.

proposed Regulation into a realistic perspective. Providing for sufficient reward for the increased obligations of data controllers would not aim to serve as a sort of protection in favour of the interests of big companies processing personal data. By contrast, incorporating the missing “carrots” logic in the draft Regulation would make the governing mechanism of accountability work, given that the use of both “sticks and carrots” implies a system of complementary instruments. After all, the achievement of the accountability vision goes hand in hand with its realistic approach. A list of potential “carrots” that we have in mind was identified in a recently published Working Paper. This list includes amongst other things, more clarity regarding respective liabilities, case of accountability duties in situations without risk, and a policy of incentives or carrots: “To incentivise adoption of accountability measures such as codes of conduct, certifications, and seals, consequences of adoption should be made clear”. Interesting for our purpose is their comparison with the defences available to intermediaries under the E-Commerce Directive and their plea to introduce similar defences or reductions of liability for those that have demonstrated their compliance.

6. CONCLUSION: REALISM ABOUT HIGH STANDARDS

The proposed Regulation sets highs standards for data controllers; this is particularly true, if we take into account that the texts set the minimum requirements for data protection, which still seem hard to achieve in practice. Even the “simple” maintenance of extended documentation by data processors raises doubts about the feasibility of the provision in the case, for example, of data centres established in third countries offering cloud services. If the ultimate aim of the Regulation, though, is to stimulate data controllers to do more than the minimum, to go “beyond mere compliance”, then the regulator has not taken into account that it would make sense to provide a reward (not just compensation). If the minimum seems hard to achieve in reality, then data controllers doing “more” or reaching, of course, their maximum, seems science fiction. It is not realistic to expect data controllers to take their own initiatives, to conform with their overarching duty of care towards personal data, to do more than the mandatory minimum in an environment, which treats intentional and negligent violations of the data protection rules the same way.

The accountability principle, as a form of governing mechanism, is placed between bottom-up and top-down regulation. It relies on the practice of the actors involved, while providing for the legal consequences, in case they do not live up to their role. The emphasis on the role of actors taking part in the functioning of the governing mechanism implies an empowerment of their ac-

not be treated as “processors”, our recommendation is to modernise Art 5(b) of the E-Commerce Directive, which currently excludes data protection law matters from its scope, so that it includes such matters, or to introduce similar defences for processors in relation to data protection laws, so that liability defences for mere intermediaries would also apply expressly to data protection law matters (including services not provided for remuneration, eg free storage services). This would make knowledge and control of personal data (including access to intelligible personal data) pre-requisites to cloud provider liability under data protection laws, but providers would lose this defence based on a modified form of “notice and takedown”.


50 Which obligations should trigger “strict liability” for any non-compliance regardless of fault, and which should be risk-based, eg requiring only the taking of measures appropriate to the individual situation or reasonable measures to industry standard.

51 “We support a more focused risk-based approach, as opposed to requiring privacy impact assessments etc in a broad range of situations that may not warrant it from a risks perspective”.

52 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market [2000] OJ L 178/1. See W. Kuan Hon, E. Kosta, C. Millard & D. Stefanatou, 19: “Many cloud providers are neutral intermediaries, and their position as such should be recognised. Therefore, if it is thought too radical to rule that cloud providers should
El interés legítimo como principio para legitimar el tratamiento de datos

JAVIER FERNÁNDEZ-SAMANIEGO
PAULA FERNÁNDEZ-LONGORIA
Abogados
Bird & Bird LLP

1. EL INTERÉS LEGÍTIMO EN LA DIRECTIVA DE PROTECCIÓN DE DATOS

1.1. Supuestos que legitiman el tratamiento o cesión de datos: el artículo 7 de la Directiva 95/46/CE

El artículo 7 de la Directiva 95/46/CE (en adelante, “la Directiva”) relaciona los supuestos que hacen lícito el tratamiento de datos de carácter personal. Dice así:

“Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si:

a) el interesado ha dado su consentimiento de forma inequívoca, o
b) es necesario para la ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado, o
c) es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, o
d) es necesario para proteger el interés vital del interesado, o

---

1 Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.