ARTICLE 29 DATA PROTECTION WORKING PARTY

00062/10/EN
WP 173

Opinion 3/2010 on the principle of accountability

Adopted on 13 July 2010

EXECUTIVE SUMMARY

EU data protection principles and obligations are often insufficiently reflected in concrete internal measures and practices. Unless data protection becomes part of the shared values and practices of an organization, and responsibilities for it are expressly assigned, effective compliance will be at considerable risk, and data protection mishaps are likely to continue.

To foster data protection in practice, the EU regulatory framework needs additional tools. This Opinion aims to advise the Commission on how to amend the Data Protection Directive to this effect. In particular, this Opinion puts forward a concrete proposal for a principle on accountability which would require data controllers to put in place appropriate and effective measures to ensure that the principles and obligations set out in the Directive are complied with and to demonstrate so to supervisory authorities upon request. This should contribute to moving data protection from 'theory to practice' as well as helping data protection authorities in their supervision and enforcement tasks.

The Opinion contains suggestions to ensure that the accountability principle provides legal certainty, while at the same time allowing for scalability (i.e., enabling the determination of the concrete measures to be applied depending on risk of the processing and the types of data processed). It then discusses how such principle could impact other areas, including international data transfers, notification requirements, sanctions, and eventually also the development of certification programs or seals.

The Working Party on the protection of individuals with regard to the processing of personal data

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,

having regard to Articles 29 and 30 paragraphs 1(a) and 3 of that Directive, and Article 15 paragraph 3 of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002,

having regard to its Rules of Procedure,

has adopted the following opinion:

1. INTRODUCTION

1. Data protection must move from 'theory to practice'. Legal requirements must be translated into real data protection measures. To encourage data protection in practice, the EU data protection legal framework needs additional mechanisms. In the discussions on the future of the European and global data protection framework, accountability based mechanisms have been suggested as a way of encouraging data controllers to implement practical tools for effective data protection.

2. In its document on The Future of Privacy (WP168) of December 2009, the Article 29 Working Party expressed the view that the present legal framework has not been fully successful in ensuring that data protection requirements translate into effective mechanisms that deliver real protection. To improve this situation, the Article 29 Working Party proposed that the Commission consider accountability-based mechanisms, with particular emphasis on the possibility to include a principle of "accountability" in the revised Data Protection Directive.[1] This principle would strengthen the role of the data controller and increase his responsibility.

3. In a nutshell, a statutory accountability principle would explicitly require data controllers to implement appropriate and effective measures to put into effect the principles and obligations of the Directive and demonstrate this on request. In practice this should translate into scalable programs aiming at implementing the

[1] "To address this problem, it would be appropriate to introduce in the comprehensive framework an accountability principle. Pursuant to this principle, data controllers would be required to carry out the necessary measures to ensure that substantive principles and obligations of the current Directive are observed when processing personal data. Such provision would reinforce the need to put in place policies and mechanisms to make effective the substantive principles and obligations of the current Directive. It would serve to reinforce the need to take effective steps resulting in an internal effective implementation of the substantive obligations and principles currently embedded in the Directive. In addition, the accountability principle would require data controllers to have the necessary internal mechanisms in place to demonstrate compliance to external stakeholders, including national DPAs. The resulting need to provide evidence of adequate measures taken to ensure compliance will greatly facilitate the enforcement of applicable rules" (WP168, paragraph 79. For more info, see also paragraphs 74-78).

existing data protection principles (sometimes referred to as 'compliance programs'). As a complement to the principle, specific additional requirements aiming at putting into effect data protection safeguards or at ensuring their effectiveness could be set up. One example would be a provision requiring the performance of a privacy impact assessment for higher risk data processing operations.

4. This Opinion aims to build upon the Article 29 Working Party previous contribution on this subject, in the Opinion on the Future of Privacy, with the view to advise the Commission in its ongoing review of Directive 95/46. To this end, this Opinion is divided in four sections: The first one discusses the need for data controllers to strengthen their practical internal arrangements (policies and procedures) to ensure that all processing is conducted in conformity with the applicable rules and how accountability-based systems can contribute to this goal. It then looks into what the legal architecture of an accountability-based system could look like and precedents in data protection and other areas. The second section puts forward a concrete proposal for a principle on accountability and describes the *rationale* behind the different aspects of the proposal. The third section discusses various elements linked to a legal system, which integrates a general accountability system. It includes a discussion on the need for such a proposal to provide legal certainty while at the same time being formulated in sufficiently broad terms to allow scalability (enabling the determination of the concrete measures and verification methods to be applied depending on risk of the processing and the types of data processed). It then discusses related items, such as the relation with overseas transfers, it provides a description of the advantage that an accountability-based mechanism would deliver to data protection authorities, and envisages what role there could be for certification.

II. ACCOUNTABILITY: PURPOSES, LEGAL ARCHITECTURE, PRECEDENTS AND TERMINOLOGY

II.1 Accountability as a driver for effective implementation of data protection principles

5. Nowadays, there is an increasing need and interest for data controllers to ensure that they take effective measures to deliver real data protection. There are several reasons for this, which are discussed further below.

6. Firstly, we are witnessing a so-called 'data deluge' effect, where the amount of personal data that exists, is processed and is further transferred continues to grow. Both technological developments, i.e. the growth of information and communication systems, and the increasing capability for individuals to use and interact with technologies favour this phenomenon. As more data is available and travels across the globe, the risks of data breaches also increase. This further emphasises the need for data controllers, both in the public and private sectors, to implement real and effective internal mechanisms to safeguard the protection of individuals' information.

7. Secondly, the ever-increasing amount of personal information is accompanied by an increase in its value in social, political and economic terms. In some sectors, particularly in the on-line environment, personal data has become the *de facto* currency in exchange for on-line content. At the same time, from a societal point of view, there is an increasing recognition of data protection as a social value. In sum, as personal information becomes more valuable for data controllers across sectors, citizens, consumers and society at large are also increasingly aware of its significance. This in turn reinforces the need to apply stringent measures to safeguard it.

8. Finally, it follows from the above that breaches of personal information may have significant negative effects for data controllers in public and private sectors. Potential glitches in eGovernment, eHealth applications will have devastating consequences in both in economic and particularly in reputational terms. Thus, minimising risks, building and maintaining a good reputation, and ensuring the trust of citizens and consumers is becoming crucial for data controllers in all sectors.

9. In summary, the above shows the critical need for data controllers to apply real and effective data protection measures aimed at good data protection governance, while minimising the legal, economic and reputational risks that are likely to derive from poor data protection practice. As further developed below, accountability-based mechanisms aim at delivering these goals.

II.2 Possible overall legal architecture of accountability based mechanisms

10. In this context a relevant question to discuss is the way in which the legal framework could encourage data controllers to take measures that deliver real protection in practice. In other words, what the legal architecture of accountability-based systems should look like.

11. As a preliminary remark before discussing such architecture, it should be emphasised that at the outset such systems in no way change or affect the substantive principles of data protection, instead they are designed to make them work better.

12. One way to induce data controllers to put in place such measures would be by adding an accountability principle in the revised version of the Directive. The expected effects of such a provision would include the implementation of internal measures and procedures putting into effect existing data protection principles, ensuring their effectiveness and the obligation to prove this should data protection authorities request it. As further described below, the type of procedures and mechanisms would vary according to the risks represented by the processing and the nature of the data.

13. In addition to the above, one could reflect on specific requirements such as the obligation to perform privacy impact assessments in given cases or the appointment of data protection officers. These specific requirements could complement the general accountability principle.

14. The Article 29 Working Party recognises that data controllers may want to implement policies and procedures that are not strictly provided for in the data protection legislation. For example, a data controller may want to commit itself to respond to access requests within a very short period of time; even though the law provides certain flexibility. It may also want to commit itself to respond to access requests simultaneously on and off line, to ensure prompt and effective receipt of such information. One could also imagine situations where the data controller wishes to exceed the minimum requirements that are embedded in the general legal framework. For example, a data controller may decide to appoint a data protection officer even though this is not mandatory under existing law. A data controller may also want to engage a third party to perform an audit on *all* its the data processing operations in order to assess whether they are in line with the data protection legal framework. The Article 29 Working Party applauds these initiatives and encourages the new data protection legal framework to provide incentives for data controllers to do so.

15. Pursuant to the above, the 'legal architecture' of the accountability mechanisms would envisage two levels: the first tier would consist of a basic statutory requirement binding upon *all* data controllers. The content of the requirement would include two elements: the implementation of measures/procedures, and the maintenance of evidence thereto. Specific requirements could complement this first tier. A second tier would include voluntary accountability systems that go above and beyond the minimum legal requirements, as far as the underlying data protection principles (providing higher safeguards than those required under the applicable rules) and/or in terms of how they implement or ensure the effectiveness of the measures (implement requirements that go beyond the minimum level). While acknowledging the importance and benefits of such systems, this Opinion deals mostly with the first tier requirement, particular with the accountability general principle.

II.3 Accountability principle in data protection and other areas and terminology

Precedents

16. The Article 29 Working Party notes that the principle of accountability is not new in itself. Its express recognition can be seen in the Organisation for Economic Cooperation and Development's (OECD) privacy guidelines adopted in 1980. Its accountability principle states: "A data controller should be accountable for complying with measures which give effect to the [material] principles stated above".

17. Recently it was explicitly included in the Madrid International Standards, developed by the International Conference of Data Protection and Privacy Commissioners.[2] It is also incorporated in the more recent ISO draft standard

[2] The responsible person shall: "a. Take all the necessary measures to observe the principles and obligations set out in this Document and in the applicable national legislation, and b. have the necessary internal mechanisms in place for demonstrating such observance both to data subjects and to the supervisory authorities in the exercise of their powers, as established in section 23."

29100 setting a privacy framework, and it is one of the main concepts of the APEC privacy framework and its cross border privacy rules.[3]

18. From a "statutory" perspective, the Article 29 Working Party notes that the Canadian Fair Information Principles contained in the Personal Information Protection and Electronic Documents Act refer to accountability. Among others, the first principle requires developing and implementing policies and practices to uphold the 10 Fair Information Principles, including implementing procedures for protecting personal information and establishing procedures for receiving and responding to complaints and inquiries.

19. In addition to the above, the Article 29 Working Party notes that binding corporate rules ("BCRs"), which are used in the context of international data transfers, reflect the accountability principle. Indeed BCRs are codes of practice, which multinational organisations draw up and follow, containing internal measures designed to put data protection principles into effect (such as audit, training programmes, network of privacy officers, handling complaint system). Once reviewed by national data protection authorities, BCRs are deemed to ensure adequate safeguards for transfers or categories of transfers of personal data between companies that are part of the same corporate group and that are bound by these corporate rules *ex* Article 25 and 26.2 of Directive 95/46.

20. Outside the world of data protection, there are some examples of accountability - as a program specifying a data controller's policies and procedures to ensure compliance with laws and regulations. For example, compliance programs are mandatory under financial services regulations. In other cases, compliance programs are not mandatory but are encouraged, such as in the field of competition law. For example, in Canada, the Competition Commissioner has developed elaborate policies on corporate compliance programs. The decision on whether or not companies apply a program is voluntary. However, the Canadian Competition Commissioner stresses the importance of compliance as a risk mitigation tool and stresses the legal, reputational and economic benefits[4].

Terminology

21. The term "accountability" comes from the Anglo-Saxon world where it is in common use and where there is a broadly shared understanding of its meaning – even though defining what exactly "accountability" means in practice is complex. In general terms though its emphasis is on showing how responsibility is exercised and making this verifiable. Responsibility and accountability are two sides of the same coin and both essential elements of good governance. Only when responsibility is demonstrated as working effectively in practice can sufficient trust be developed.

---

[3] In addition to the above, the Centre for Information Policy Leadership is engaged in an initiative to explore the effects of the principle of accountability as far as data protection and privacy is concerned. See: www.informationpolicycentre.com

[4] www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/eng/02732.html.

22. In most other European languages, due mainly to differences in the legal systems, the term “accountability” cannot easily be translated. As a consequence, the risk of varying interpretation of the term, and thereby lack of harmonisation, is substantial. Other words that have been suggested to capture the meaning of accountability, are “reinforced responsibility”, “assurance”, “reliability”, “trustworthiness” and in French “obligation de rendre des comptes” etc. One may also suggest that accountability refers to the “implementation of data protection principles”.

23. In this document, therefore we focus on the measures which should be taken or provided to ensure compliance in the data protection field. References to accountability should therefore be understood as the meaning used in this Opinion, without prejudice to finding another wording that more accurately reflects the concept given here. This is why the document doesn't focus on terms but pragmatically focuses on the measures that need to be taken rather than on the concept itself.

III. TOWARDS A PROPOSAL FOR A GENERAL PROVISION ON ACCOUNTABILITY

III.1 A general provision to reaffirm and strengthen the responsibility of controllers

24. The Article 29 Working Party has given further thought to the possibility of introducing accountability-based solutions in the new comprehensive data protection legal framework in light of the considerations made in section I.

25. As a result, it has confirmed its views, already expressed in its Opinion on the Future of Privacy, that a general accountability principle should be included in a new comprehensive legislative framework. The purpose of such a provision would be to reaffirm and to strengthen the responsibility of controllers towards the processing of personal data. This is without prejudice to concrete accountability measures that could complement this principle.

26. This new provision would be in line with specific provisions which already exist in the current legislative framework. One may in particular refer to Article 6 of the Directive 95/46/CE, which refers to the principles relating to data quality in its paragraph 1 and which mentions in its paragraph 2 that “It shall be for the controller to ensure that paragraph 1 is complied with”. It would also fit with Article 17.1 which requires data controllers to implement measures, of both a technical and organisational nature. Indeed, a general accountability provision would reinforce the need for data controllers to implement the security requirements of Article 17, in addition to the requirements set forth in the remaining provisions.

III.2 Towards a concrete proposal for a general accountability principle

27. The new provision would aim to foster the adoption of concrete and practical measures, turning the general data protection principles into concrete policies and procedures that are defined at the level of the controller, in compliance with applicable laws and regulations. The controller should also ensure the effectiveness of the measures taken and demonstrate upon request that it has taken these actions.

28. In a schematic manner, such a general provision would focus on two main elements:

    (i) the need for a controller to take appropriate and effective measures to implement data protection principles;
    (ii) the need to demonstrate upon request that appropriate and effective measures have been taken. Thus, the controller shall provide evidence of (i) above.

29. The obligation should cover all controllers and all situations.

30. The first element of the obligation would require data controllers to implement appropriate measures. The types of measures would not be specified in the text of the general provision on accountability. Subsequent guidance given by national data protection authorities by the Article 29 Working Party or by the Commission (through comitology procedures) could specify, for certain cases, a minimum set of specific measures as constituting appropriate measures. One example of such measures would be the adoption in certain cases of internal policies and processes necessary to implement data protection principles, that would reflect applicable laws and regulations.

31. The implementation of these measures and processes may also be done in an effective manner through the assignment of responsibilities and through the training of staff involved in the processing operations. In particular, in compliance with Article 18 of the Directive, controllers should be encouraged to appoint personal data protection officials. One should encourage in any case the assignment of responsibility at different levels in the organisation to ensure that these responsibilities are fulfilled.

32. With respect to transfers of personal data outside of the European Union, data controllers should adopt and implement appropriate measures to comply with the requirement of "adducing adequate safeguards" provided by Article 26 of the Directive such as with BCRs.

33. Controllers should also ensure that the practical measures implemented to comply with data protection principles are effective. In case of larger, more complex or high risk data processing, the effectiveness of the measures adopted should be verified regularly. There are different ways to assess the effectiveness (or ineffectiveness) of the measures: monitoring, internal and external audits, etc.

34. Pursuant to the remarks above, the Article 29 Working Party considered the wording of a concrete provision that could be introduced in a comprehensive legislative framework which could read as follows:

"Article X - Implementation of data protection principles

1. The controller shall implement appropriate and effective measures to ensure that the principles and obligations set out in the Directive are complied with.
2 The controller shall demonstrate compliance with paragraph 1 to the supervisory authority on its request.

IV. DISCUSSION OF VARIOUS ELEMENTS LINKED TO THE GENERAL ACCOUNTABILITY PRINCIPLE

IV.1 Reinforcing existing obligations

35. The Article 29 Working Party notes that some data controllers may perceive the general accountability principle as imposing cumbersome new legal requirements upon data controllers, particularly given the current, challenging EU economic situation. This would be mistaken.

36. The Article 29 Working Party wishes to highlight that most of the requirements set out in this new provision actually already exist, albeit less explicitly, under existing laws. Indeed, under the current legal framework data controllers are obliged to comply with the principles and obligations set forth in the Directive. To do so, it is intrinsically necessary to set up, and possibly verify, data protection related procedures. From 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.

37. In fact, a somewhat similar legislative development took place when Directive 2002/58 was amended in 2009.[5] In this case, the law imposes an obligation to implement a security policy, namely to "*ensure the implementation of a security policy with respect to the processing of personal data*". Thus, as far as the security provisions of that Directive are concerned, the legislator decided that it was necessary to introduce an explicit requirement to have and implement a security policy. Moreover, Article 18 of Directive 95/46 referring to the designation of data protection officials, as well as the system of binding corporate rules mentioned above, already offer examples of practical measures that can be adopted by data controllers.

---

[5] Directive 2009/136/EC of the European Parliament and of the Council (of 25 November 2009) amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

38. A question connected to the above is the consequence attached to compliance (or non-compliance) with the accountability principle. The Article 29 Working Party highlights that fulfilling the accountability principle does not necessarily mean that a data controller is in compliance with the substantive principles set forth in the Directive, i.e., it does not offer a legal presumption of compliance nor does it replace any of those principles. A data controller may have implemented and verified the measures that it has put in place; and yet it may find itself engaged in wrongdoing. Accordingly, adopting measures to observe the principles must not in any case exclude data controllers from being subject to enforcement actions by data protection authorities. In practice, public and private sector data controllers which have adopted measures in robust compliance programs are more likely to be in compliance with the law. Indeed, because they have put in practice effective measures directed towards observing the substantive principles of the data protection, it should be less likely for them to be in breach of the law. Therefore, in assessing sanctions related to data protection violations, data protection authorities could give weight to the implementation (or lack of it) of measures and their verification.

IV.2 Appropriate measures to implement the provisions of the Directive

39. A provision on accountability would require data controllers to define and implement the necessary measures to ensure compliance with the principles and obligations of the Directive and to have their effectiveness verified periodically.

40. The proposed general accountability principle purposefully avoids spelling out in detail the type of measures to be implemented. This raises the following two interlinked fundamental questions: *(i)* which common measures would fulfil the accountability principle? *(ii)* how to scale and tailor the measures to specific circumstances?

The measures: an illustration

41. The Article 29 Working Party considers that common accountability measures may include the following non-exhaustive list:

- Establishment of internal procedures *prior* to the creation of new personal data processing operations (internal review, assessment, etc);[6]
- Setting up written and binding data protection policies to be considered and applied to new data processing operations (e.g., compliance with data quality, notice, security principles, access, etc), which should be available to data subjects.
- Mapping of procedures to ensure proper identification of all data processing operations and maintenance of an inventory of data processing operations,
- Appointment of a data protection officer and other individuals with responsibility for data protection;
- Offering adequate data protection, training and education to staff members. This should include those processing (or responsible for) the personal data (such as human resources directors) but also IT managers, developers and

[6] Existing data processing operations would need a transitional period to be put in line with the law.

directors of business units. Sufficient resources should be allocated for privacy management, etc.

- Setting up of procedures to manage access, correction and deletion requests which should be transparent to data subjects;
- Establishment of an internal complaints handling mechanism;
- Setting up internal procedures for the effective management and reporting of security breaches;
- Performance of privacy impact assessments in specific circumstances;
- Implementation and supervision of verification procedures to ensure that all the measures not only exist on paper but that they are implemented and work in practice (internal or external audits, etc).

42. A complementary approach to the general accountability principle could also be envisaged. Under such an approach the legal framework would include not only a general accountability principle but also an illustrative list of measures that could be encouraged at national level[7]. This provision could give an illustrative and non-exhaustive list of measures that could constitute a "toolbox" for data controllers. It would give guidance to controllers on what could constitute, depending on the cases, the appropriate measures to be adopted by the controller. This illustrative list would of course only accompany the general legal obligation to adopt appropriate measures.

---

[7] For instance, the International Standards adopted in Madrid by data protection authorities contain in its Article 22 a provision on proactive measures, which reads as follows: "*States should encourage, through their domestic law, the implementation by those involved in any stage of the processing of measures to promote better compliance with applicable laws on the protection of privacy with regard to the processing of personal data. Such measures could include, among others:*

a) The implementation of procedures to prevent and detect breaches, which may be based on standardized models of information security governance and/or management.

b) The appointment of one or more data protection or privacy officers, with adequate qualifications, resources and powers for exercising their supervisory functions adequately.

c) The periodic implementation of training, education and awareness programs among the members of the organization aimed at better understanding of the applicable laws on the protection of privacy with regard to the processing of personal data, as well as the procedures established by the organization for that purpose.

d) The periodic conduct of transparent audits by qualified and preferably independent parties to verify compliance with the applicable laws on the protection of privacy with regard to the processing of personal data, as well as with the procedures established by the organization for that purpose.

e) The adaptation of information systems and/or technologies for the processing of personal data to the applicable laws on the protection of privacy with regard to the processing of personal data, particularly at the time of deciding on their technical specifications and on the development and implementation thereof.

f) The implementation of privacy impact assessments prior to implementing new information systems and/or technologies for the processing of personal data, as well as prior to carrying out any new method of processing personal data or substantial modifications in existing processing.

g) The adoption of codes of practice the observance of which are binding and that include elements that allow the measurement of efficiency as far as compliance and level of protection of personal data are concerned, and that set out effective measures in case of non compliance.

h) The implementation of a response plan that establishes guidelines for action in case of verifying a breach of applicable laws on the protection of privacy with regard to the processing of personal data, including at least the obligation to determine the cause and extent of the breach, to describe its harmful effects and to take the appropriate measures to avoid future breaches."

Scaling the measures

43. The above is an illustrative list of measures which data controllers could put into effect to fulfil the first part of the accountability principle (*The controller shall implement appropriate and effective measures to ensure that principles and obligations set out in the Directive are complied with.)*

44. Some of the measures are 'staples' that will have to be implemented in most data processing operations. Drafting internal policies and procedures implementing the principles (procedures to handle access requests, complaints) may constitute examples of appropriate measures for some processing of data. The suitability of measures will need to be decided on a case-by-case basis. It is up to data controllers to make such decisions, following guidance issued by national data protection authorities and the Article 29 Working Party where available (see below).

45. It follows from the above that in determining the types of measures to be implemented, there is no option but "custom built" solutions. Indeed, the specific measures to be applied must be determined depending on the facts and circumstances of each particular case, with particular attention to the risk of the processing and the types of data. A one-size-fits-all approach would only force data controllers into structures that are unfitting and ultimately fail.

46. Under this approach, controllers must be able to tailor the measures to the concrete specifics of the data controller and the data processing operations in question. In this context, the Article 29 Working Party recalls the criteria used in Article 17 of the current Directive[8] to determine the type of security measures to be applied: namely, the risks represented by the data processing and the nature of data. These two factors could be used analogically to determine the general types of measures to apply. More concretely, aspects such as the size of the data processing operation/s, the intended purposes of the processing and the number of envisaged data transfers may determine the level of risk. The type of data, including whether they are sensitive or not, should also be considered. A reflection on the need to impose certain obligations to the data processor or to the designers and/or manufacturers of ICT (information and communication technologies) could also be developed at the light of this accountability principle.

47. While in accordance with these criteria, in principle, large data controllers should implement stringent measures. In some cases, small or medium controllers, for instance if they are engaged in risky data processing operations, take for example some eHealth data processing operations, may also be required to put in place rigorous safeguards. For example, a local government (city hall), a multinational, a small (Internet) business, an organisation for which data processing is its core activity, or an organisation with a history of contravening the law would all require their own specific measures, in order to ensure credible and effective information governance. As a result, in simple and basic cases, such as for the processing of personal data related to human resources for the establishment of a

---

8 "*Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of assurance appropriate to the risks represented by the processing and the nature of the data to be protected*".

corporate directory, the "obligation to demonstrate", referred to under paragraph 2 of the provision on accountability, could be fulfilled easily (through for instance the information notices that were used; the description of basic security measures etc). On the contrary, in other more complex cases, such as for instance the use of innovative biometric devices, fulfilling the "obligation to demonstrate" could need further requirements. The controller may have for instance to demonstrate that it undertook a privacy impact assessment, that the staff involved in the processing are trained and informed regularly, etc.

48. Transparency is an integral element of many accountability measures. Transparency vis-à-vis the data subjects and the public in general contributes to the accountability of data controllers. For example, a greater level of accountability is achieved by publishing privacy policies on the Internet, by providing transparency in regard to internal complaints procedures, and through the publication in annual reports.

Guidance and legal certainty

49. Whereas the need for scalability and hence flexibility supports the use of open language, the Article 29 Working Party is aware that a broad provision giving room for flexibility and scalability may also result in uncertainty. Controllers may consider that the provision is not sufficiently detailed to provide legal certainty. For example, they may be uncertain about the level of detail expected from privacy policies and procedures, when and how to designate a data protection officer, when training sessions need to be organised, etc. The uncertainty may also relate to the type of verification that may be necessary, whether third party or internal. Furthermore, data controllers may also fear being subject to divergent and arbitrary national interpretations regarding the scope and nature of their obligations.

50. The Article 29 Working Party understands this concern. However, for the reasons noted above regarding the need for flexibility and scalability, the solution to achieve legal certainty cannot be provided in the Directive itself. To achieve the needed legal certainty, the Article 29 Working Party considers that harmonising guidance issued by the Commission (for example, through technical implementing measures) or/and the Article 29 Working Party could serve as a useful tool to provide more certainty and eliminate potential differences at implementation level.[9] The Article 29 Working Party could also prepare general guidance providing a baseline of necessary elements for a standard data controller. This baseline could be tailored to the specific needs of each data controller.

[9] An example of such type of guidance is PIPEDA Self-assessment tool, published by the Office of the Privacy Commissioner of Canada to help medium and large data controllers develop and implement good privacy governance and management. The self assessment tool is available at: http://www.priv.gc.ca/information/pub/ar-vr/pipeda_sa_tool_200807_e.pdf .

51. It may also be useful to develop a *model data compliance program*, which could be used by medium and large data controllers as a baseline upon which to draft their particular programs as it has been done for BCRs with the guidance developed by the WP29[10]. These models should be created after a careful review of the current practices, available models, and with the consultation of all appropriate stakeholders. This is an area that will need serious investment from all stakeholders.

Effectiveness of measures

52. The same issues discussed above regarding the applicable measures arise in the context of ensuring the effectiveness of the measures. Depending on the type of data processing, the way effectiveness can be ensured will differ.

53. There are many different ways for data controllers to assess the effectiveness (or ineffectiveness) of the measures. For larger, more complex and high risk processing, internal and external audits are common verification methods. The way in which audits are conducted may also vary and may range from full audits to negative audits (which may also adopt different forms and shapes). In deciding how to ensure the effectiveness of the measures, the Article 29 Working Party suggests using the same criteria as for deciding on the measures, which derive from Article 17 of Directive 95/46/EC namely, the risks represented by the data processing and the nature of data. Therefore, how a controller should ensure the effectiveness of measures will depend on the sensitivity of the data, the amounts of data processed and the particular risks posed by the data processing. Article 29 Working Party guidance on the measures may also include guidance on this aspect.

IV.3 Link with other requirements

Prior notifications

54. A reflection could be undertaken on the possible impact on prior notifications when appropriate safeguards are defined at the level of the controller. One may envisage that certain accountability mechanisms could replace or diminish administrative requirements of current data protection legislation as already suggested by the Article 29 Working Party in its opinion on the Future of Privacy.

International data transfers

55. Binding corporate rules is an example of a way to implement data protection principles on the basis of the accountability principle. It is a way identified and accepted by the Article 29 Working Party to provide adequate safeguards for transfers outside the European Union.

---

[10] Article 29 Working Party Document 153 setting up a table with the elements and principles to be found in Binding Corporate Rules, and Working Document 154 setting up a framework for the structure of Binding Corporate Rules.

56. This is an area which would benefit from further analysis in light of the revision of Directive 95/46. In particular, it would be important to consider whether Article 26.2 of the Directive (*a Member State may authorize a transfer.....where the controller adduces adequate safeguards; such safeguards may in particular result from appropriate contractual clauses")* fully covers binding corporate rules and eventually other similar binding accountability mechanisms as tools to provide adequate safeguards.

57. In this context, it is highly relevant to assess, among others, the mechanisms used to put the data protection principles and obligations into effect internally within data controllers and the systems for verification. It is also relevant to discuss the mechanisms to streamline the current system based on authorisation of data transfers by national data protection authorities.

IV.4 The Role of Data Protection Authorities

58. A question to address is whether the accountability principle proposed in this opinion will affect the powers of data protection authorities, particularly in the area of enforcement. As further described below, the principle does not take away any powers from data protection authorities. On the contrary, it will bring benefits to data protection authorities.

59. As far as enforcement is concerned, the principle as proposed recognises the data protection authorities' competence to request evidence of compliance with the accountability principle from the data controller, and thereby adds to the enforcement activities of the authorities. This ensures that authorities remain empowered, at any time, to carry out enforcement actions. It should be made clear that in any case data protection authorities would remain competent to supervise not only the measures taken by data controllers, but first and foremost to supervise compliance with the underlying principles and obligations.

60. Furthermore, putting the accountability principle into effect will provide useful information to data protection authorities to monitor compliance levels. Indeed, because data controllers will have to be able to demonstrate to the authorities whether and how they have implemented the measures, very relevant compliance related information would be available to authorities. They will then be able to use this information in the context of their enforcement actions. Moreover, if such information is not provided upon request, data protection authorities will have an immediate cause of action against data controllers, independently of the alleged violation of other underlying data protection principles.

61. The principle should also be instrumental for data protection authorities insofar as it would help them to be more selective and strategic, enabling them to invest their resources in a way as to generate the largest possible scale of compliance.

62. The Article 29 Working Party notes that the accountability principle may contribute to the development of legal and technical expertise in the area of implementing data protection requirements. Highly knowledgeable individuals with technical and legal understanding in the field of data protection, with abilities

to communicate, train staff, set up and implement policies, and audit will be indispensable in this area. Such expertise will be necessary both in-house and as an external service for companies to hire. This development will be vital in ensuring that data controllers can carry out their obligations, including if need be performing internal and external/internal audits. At the same time, this development will be beneficial to Data Protection Authorities as the system will contribute to overall compliance, authorities will have at their disposal more sound information about the internal practices of companies, and the development of highly knowledgeable and skilled data protection professionals will certainly help in their interaction with data controllers.

63. It can be concluded that the activity of data protection authorities is more focused on an ‘ex post’ role rather than an ‘ex ante’ one. Because accountability puts emphasis on certain outcomes to be achieved in terms of good data protection governance it is said to be result-focused; its emphasis is 'ex post' (i.e., after the data processing has started).

IV. 5 Sanctions

64. The proposed system can only work if data protection authorities are endowed with meaningful powers of sanction. In particular, when and if data controllers fail to fulfil the accountability principle, there is a need for meaningful sanctions. For example, it should be punishable if a data controller does not honour the representations it made in binding internal policies. Obviously, this is in addition to the actual infringement of substantive data protection principles.

65. In addition to the above, the Article 29 Working Party considers that the powers of national data protection authorities should include the possibility to impose precise instructions upon data controllers regarding their compliance system.

IV.6 The development of certification schemes

66. In the longer term, the provision on accountability may foster the development of certification programs or seals. Such programs would contribute to prove that a data controller has fulfilled the provision; hence, that it has defined and implemented appropriate measures which have been periodically audited. Various factors may promote such development:

67. In general one can anticipate that to differentiate themselves, data protection/auditing/privacy impact assessment services are likely to increasingly offer certificates/seals to single themselves out in the market and also as a competitive advantage. Data controllers may decide to use the option of trustworthy services delivering certificates. As certain seals become known for their rigorous testing, data controllers are likely to favour them insofar as they would give more compliance 'comfort' in addition to offering a competitive advantage.

68. The use of BCRs as legal grounds for international data transfers require that data controllers show that they have put in place adequate safeguards, in which case data protection authorities may authorise the transfers. This is an area where certification services could be helpful. Such services would analyse the assurances provided by the data controller and, if appropriate, issue the relevant seal. A data protection authority could use the certification provided by a given certification program in its analysis of BCRs of whether a data controller has provided sufficient safeguards for the purposes of international data transfers. Thus, contributing to streamlining the process for authorisation of international data transfers.

IV.7 The regulation of certification schemes

69. The same reasons that favour the development of certification services also support the need for such services to be regulated. Indeed, if such services are intended to provide reliable evidence of data protection compliance (to DPAs, to controllers and to consumers in general) and operate smoothly in the internal market, rules setting forth requirements for the provision of the services seem necessary. Data protection authorities should play a key role in the development of those rules (e.g. referential, models, etc) and should be able to enforce their implementation. This also requires they are provided with sufficient resources. Moreover data protection authorities should play a role in certifying the certifiers. This may be particularly relevant in the area of international data transfers. Because the quality of the services and the need for them to operate in the internal market are a key criterion, the law will have to set up the conditions that will serve to achieve such quality. It does not seem possible to leave this to the market. Experience in other areas such as in certification of goods has shown a tendency towards the bottom. Competition among service providers may lead to a reduction of prices and also to certain flexibility or relaxation of the procedures. In sum, whether or not in a cross border basis, rules seem necessary to ensure good quality of the services and a level playing field.

70. The Article 29 Working Party notes that existing legislation on accreditation[11] may be applicable in the area of certification services in the data protection field. Such legislation already provides the necessary structure laying down rules on the organisation and operation of accreditation bodies. These rules apply to voluntary accreditation and also in the specific cases were accreditation is mandatory.

71. Obviously, this type of service would also push towards the harmonisation of the underlying standards against which entities would be tested. The guidance mentioned (from the Article 29 Working Party or from the Commission) setting forth model data compliance programs would be highly relevant.

[11] Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93.

V. CONCLUSIONS

72. The development of new technologies and the continued globalization of the economy and the society have led to a proliferation of the personal information that is collected, sorted, transferred or otherwise retained. The risks to such data therefore multiply.

73. The Article 29 Working Party is convinced that the increase of both the risks and the value of personal data *per se* support the need to strengthen the role and responsibility of data controllers. A regulatory framework that caters for this new reality must contain the necessary tools to encourage data controllers to apply in practice appropriate and effective measures that deliver the outcomes of the data protection principles. Procedures to ensure the identification of all data processing operations, to respond to access requests, the allocation of resources including the designation of individuals who are responsible for the organisation of data protection compliance are examples of such measures.

74. To encourage data protection in practice, the Article 29 Working Party suggests first and foremost to include in the proposals amending the Data Protection Directive a new provision requiring data controllers to implement appropriate and effective measures to ensure that the principles and obligations of the Data Protection Directive are complied with and demonstrate this to authorities upon request. These measures should foster compliance with data protection principles and obligations while minimizing risks of unauthorized access, misuse, loss, etc. The obligation to demonstrate the setting up of the necessary measures upon request should be a useful tool for data protection authorities in their enforcement tasks.

75. The obligation to implement these measures should apply to data controllers of all sectors (public and private) and should be scalable so that the type of measures should be coherent with the risks represented by the data processing and the nature of data.

Done at Brussels, on 13 July 2010

For the Working Party
The Chairman
Jacob KOHNSTAMM