Centre for Information Policy Leadership
Hunton & Williams

**23 November 2014**

# THE ROLE OF RISK MANAGEMENT IN DATA PROTECTION

*Paper 2 of the Project on Privacy Risk Framework and Risk-based Approach to Privacy*

## Executive Summary

Data protection has long relied on risk management as a critical tool for complying with data protection laws and ensuring that data are processed appropriately and the fundamental rights and interests of individuals are protected effectively. Yet these risk management processes, whether undertaken by businesses or regulators, have often been informal, unstructured and failed to take advantage of many of the widely accepted principles and tools of risk management in other areas.

In addition, institutional risk management in the field of data protection has suffered from the absence of any consensus on the harms for individuals or negative impacts that risk management is intended to identify and mitigate in the area of data protection. This is the starting point for effective risk assessment in other fields. As a result, despite many examples of specific applications, a risk-based approach still does not yet provide a broad foundation for data protection practice or law.

This presents both an opportunity and a challenge. The opportunity is to develop modern, effective risk management tools and a framework of impacts—both harms and benefits—building on decades of experience with risk management broadly. The challenge is to do so quickly to keep pace with dramatic changes in technology and human and institutional behaviour.

Risk management involves three key elements—(1) the systematic process of identifying and assessing harms and other negative impacts, (2) avoiding or mitigating those that cannot be justified by the benefits and other positive impacts, and then (3) accepting and managing the remaining risks. This paper addresses the role of risk management in data protection as implemented into legal requirements, interpreted by regulators and put into practice by responsible organisations. It also highlights the growing consensus around risk management as an essential tool for effective data protection, and addresses key considerations that affect the role of risk in data protection law and practice, including:

a. **The role of risk management**—Risk management does not alter rights or obligations. Rather, it is a valuable tool for calibrating the implementation of and compliance with privacy requirements, prioritising action, raising and informing awareness about risks, identifying appropriate mitigation measures and, in the words of the Article 29 Working Party, providing a "scalable and proportionate approach to compliance".

b. **A balancing test**—Risk management is fundamentally a balancing test that takes into account many factors, including the fundamental rights and interests of individuals, the likelihood that the proposed processing will harm individuals, the severity of the harm if it occurs, the measures available to mitigate risk, the rights and interests of data controllers, the likelihood that benefits will result from the proposed processing, and the magnitude of those benefits.

c. **Severity *and* likelihood**—It is universally recognised that the balancing inherent in risk management must take into account both the *magnitude* of potential impacts—positive and negative—and their *likelihood* of occurring.

d. **Identify impacts**—Making risk management work effectively and consistently requires that there be a widely shared classification and taxonomy of impacts—positive and negative—on individuals, organisations and third parties. Specific categories might differ from country to country or culture to culture, but the absence of a common understanding as to what impacts should be minimised (or maximised) threatens not only quality risk management and meaningful accountability, but also effective data protection.

e. **Mitigating measures in risk management**—To manage risk effectively it is necessary to include mitigation measures in the balance.

f. **The goal of risk management: the role of proportionality**—Rarely can risk be eliminated entirely. Therefore, the goal of the risk management process is to provide for proportional responses that reduce the risk as fully as practical and identify the remaining risks and how they will be managed.

g. **Efficient, scalable and flexible risk management**—Unnecessarily burdensome risk management requirements can be costly and stifle innovation. The requirements for risk management, therefore, should be scalable and flexible.

h. **Integration with other risk management approaches**—It is important that data protection risk management tools fit within existing risk management methodologies and programs to allow these tools to take advantage of expertise developed in other areas, ensure that data protection risk management takes advantage of the considerable resources already being devoted by organisations to risk management in other areas, and enhance the efficiency (and reduce the cost) of data protection risk management.

i. **The scope of risk management**—There is widespread agreement that risk management must have a broad scope that includes the entire lifecycle of data-based products and services, including from data collection to use, sharing, transfers and destruction.

j. **Assessment of risk management**—Risk management itself must be assessed to ensure that the methodologies being employed continue to be valid, the range of impacts—positive and negative—and possible mitigation tools remain current, the outcomes are reasonable and the conclusions of those assessments are being complied with.

k. **Organisational support for risk management**—Effective risk management requires significant organisational support including tangible resources and management buy-in.

Despite the wide and growing consensus around risk management as an essential tool for effective data protection, there are still important issues to be resolved. These include the need to:

- Develop and build multinational consensus around a taxonomy of data protection harms or other negative impacts and benefits, and a framework for assessing them;

- Develop and build consensus around risk management models, technical standards, best practices and tools that are both flexible and scalable for risk management in data protection;

- Draw upon extensive experience in risk management in other areas, to both enhance risk management in data protection and ensure that it is well integrated with existing, widely used risk management processes;

- Practise greater consistency and precision in the use of risk management terms and processes (for example, to avoid confusing "risks" with "threats" and to ensure that risks are assessed in terms of both impact and likelihood);

- Develop a deeper understanding of proportionality and the conditions under which risks may be tolerated or accepted; and

- Explore further how, as a step towards greater interoperability, organisations can use risk management as a critical tool to manage compliance in the face of divergent national and sectoral legal requirements.

Risk management does not alter rights or obligations, nor does it take away organisational accountability. On the contrary, it has proven a valuable tool for calibrating accountability, prioritising action, raising and informing awareness about risks, and identifying appropriate mitigation measures.

The Centre for Information Policy Leadership looks forward to continuing to work on these and other issues with all stakeholders to ensure that risk management achieves its full potential as a tool for protecting individuals from harm or negative impacts that affect their privacy and other fundamental rights.

## 1. Introduction

Risk is an inherent part of all human activities so, not surprisingly, assessing risk and making decisions about how to avoid or minimise it are activities fundamental to human existence. Whether evaluating whether to walk down an unfamiliar street at night or undergo a medical procedure, the process of assessing and managing risk is so fundamental and engrained that individuals do it intuitively and often without any conscious awareness.

Not surprisingly, risk management also has become a critical component of most institutional activities as well. Deciding what to buy or sell, whom to hire and where to locate are just a few examples of the many decisions that are based on an evaluation of the risks and benefits involved. As PricewaterhouseCoopers has noted in its *Practical Guide to Risk Assessment*, identifying and managing risk are "increasingly important to the success and longevity of any business".[1]

In recent years, many countries have enacted laws and regulations requiring or encouraging more formal risk management. Today formal, documented risk assessments and other risk management tools are required in an expansive range of laws ranging from workplace safety to financial reporting. Along with these legal requirements has come a professional practice of risk management, including specialised research, international and sectoral standards, a common vocabulary and agreed-upon principles and processes.

Data protection has long relied on risk management as a critical tool for ensuring that data are processed appropriately and that the fundamental rights and interests of individuals are protected effectively. Risk management has become an increasingly prominent feature of legal requirements over the past two decades. Even beyond those legal requirements, however, organisations have employed risk management as a logical, familiar and effective tool for protecting privacy. Risk management does not alter rights or obligations, nor does it take away organisational accountability. To the contrary, it is an integral part of accountability and what accountable organisations should be doing. It has proven a valuable tool for calibrating accountability, prioritising action, raising and informing awareness about risks, and identifying appropriate mitigation measures. Furthermore, it is especially valuable as a step towards greater interoperability in the face of divergent national and sectoral legal requirements, helping organisations to manage compliance on a more global basis as they work with regulators to identify mutually accepted approaches and values, thus driving common outcomes, despite the lack of common legal rules. Data protection regulators themselves are also increasingly employing risk management as a way of targeting scarce resources where they are most needed and can have the greatest impact.

Yet risk management in data protection, whether undertaken by businesses or regulators, has often been informal and unstructured and failed to take advantage of many of the widely accepted principles and tools of risk management in other areas. In addition, risk management in the field of data protection has suffered from the absence of any widely accepted framework of harms or negative impacts and so, at best, has been idiosyncratic and, at worst, has not taken into account the full range of risks to individuals. As a result, despite many examples of specific applications, risk management still does not achieve its full potential as a critical tool in data protection practice and law.

In January 2014, the Centre for Information Policy Leadership launched a multiyear project on the role of risk management in data protection. This project elaborates on the Centre's earlier work on organisational accountability, particularly in seeking to develop the analytical framework and tools needed to implement key aspects of accountability. The Centre's risk project is designed to help "bridge the gap between high-

[1] PricewaterhouseCoopers, *A Practical Guide to Risk Assessment* (2008), 3.

level privacy principles on the one hand, and compliance on the ground on the other".[2] In its first paper, *A Risk-based Approach to Privacy: Improving Effectiveness in Practice*, the project sought to understand "what is meant by privacy risks to individuals (and society) and to create a practical framework to identify, prioritise and mitigate such risks so that principle-based privacy obligations can be implemented appropriately and effectively".[3]

In this paper, the project addresses the role of risk management—the systematic process of identifying and assessing risks, avoiding or mitigating them where possible, and then accepting and managing the remaining risks—in data protection as implemented into legal requirements, interpreted by regulators and put into practice by responsible organisations. This paper highlights the growing consensus around risk management as an essential tool for effective data protection, and addresses key considerations that affect the role of risk in data protection law and practice.

A draft of this paper was provided to the participants in the Centre's second workshop on the Privacy Risk Framework and the Risk-based Approach to Privacy, held in Brussels on 18 November 2014. This final version reflects both the thoughtful comments of those participants[4] and the wide-ranging discussion at the workshop.[5]

## 2. Risk Management in Data Protection Regulation

Companies are subject to hundreds of laws and regulations requiring that they identify, assess and manage risks. Many of these requirements, for example, Sarbanes-Oxley and the broad obligations on publicly traded companies to identify and disclose in their quarterly or annual filings material risks, are longstanding. Others, such as Basel III and the numerous national requirements imposed on financial institutions to assess and avoid or otherwise respond to risks to their solvency, have been enacted or strengthened more recently.

Today, whether as a result of legal requirements, professional or self-regulatory obligations, or internal risk management policy, the types of risk assessments routinely performed within organisations include:

- Strategic risk assessment
- Operational risk assessment
- Compliance risk assessment
- Internal audit risk assessment
- Financial statement risk assessment
- Fraud risk assessment
- Market risk assessment
- Credit risk assessment
- Customer risk assessment
- Supply chain risk assessment
- Product risk assessment
- Security risk assessment
- Information technology risk assessment

---

[2] Centre for Information Policy Leadership at Hunton & Williams LLP, *A Risk-based Approach to Privacy: Improving Effectiveness in Practice* (2014), 1.

[3] Id.

[4] See attached Appendix.

[5] The workshop was conducted under the Chatham House Rule, so it is not possible to attribute specific contributions by name. The Centre thanks all participants, but is alone responsible for the contents of this paper.

- Project risk assessment[6]

Given the long history and widespread reliance on risk management in other areas, it is no surprise that many organisations had begun applying similar tools to the processing of personal data, even before there were any legal obligations to do so.

Over the past decade data protection laws around the world have come increasingly to rely on risk management as a key tool to protect personal privacy. Today, the legal obligation to manage risks around data processing as part of compliance with data protection law is well established. For example,

- Privacy Impact Assessments (PIAs) are a critical part of organisational risk management and one of the earliest examples of risk management being applied to data protection. US federal government agencies have been required to conduct PIAs ever since the E-Government Act of 2002 took effect in 2003.[7] The UK Information Commissioner's Office (ICO) published the first European *Privacy Impact Assessment Handbook* in 2007, and the Cabinet Office adopted PIAs as a "mandatory minimum measure" for all UK government agencies in 2008.[8] The Treasury Board of Canada issued a Directive on Privacy Impact Assessment that took effect in 2010, under which all government departments must conduct a PIA in a manner that is commensurate with the level of privacy risk identified before establishing any new or substantially modified program or activity involving personal information.[9] Other nations and provinces have followed suit, with the Spanish La Agencia Española de Protección de Datos issuing one of the most recent guides, the *GUÍA para una Evaluación de Impacto en la de Protección Datos Personales*, in 2014.[10]

- The broad authority of the US Federal Trade Commission (FTC) to stop "unfair … acts or practices in or affecting commerce", which it has applied with increasing frequency in the area of data protection and data security, requires a risk assessment by both industry and the Commission. The FTC's unfairness authority applies only to practices that cause "substantial" injury to consumers that are "not reasonably avoidable by consumers themselves" and are "not outweighed by countervailing benefits to consumers or to competition".[11] As a result, the FTC must consider both "injuries" and "benefits" and must explicitly balance them. Similarly, to avoid their privacy and security practices' being subject to an unfairness claim, businesses must engage in a similar risk assessment.

- Security breach notification laws in Europe, Australia, Canada, New Zealand, the United States and other countries require an assessment of the risk posed by the exposure or loss of covered information on individuals. Under those laws, the determination as to whether organisations must provide notice often depends on an assessment of the risk to individuals posed by the breached information. As the Article 29 Data Protection Working Party has noted, for notification to be effective "it is important to have an appropriate risk management framework in place."[12]

---

[6] PricewaterhouseCoopers, at 9-11.

[7] Executive Office of the President, Office of Management and Budget, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, M-03-22 (2003).

[8] Cabinet Office, *Cross Government Actions: Mandatory Minimum Measures* (2008), ¶ 4.4.

[9] Treasury Board of Canada Secretariat, *Directive on Privacy Impact Assessment* (2010), § 3.3.

[10] La Agencia Española de Protección de Datos, *GUÍA para una Evaluación de Impacto en la de Protección Datos Personales* (2014).

[11] 15 USC § 45(n).

[12] Article 29 Data Protection Working Party, *Opinion 03/2014 on Personal Data Breach Notification*, 693/14/EN WP 213 (2014), 4.

- The EU data protection directive, like many data protection laws around the world, is focused on protecting data in *context*, with "context" necessarily requiring sensitivity to factors affecting risk. As a result, the directive requires "appropriate safeguards", "appropriate guarantees", "appropriate technical and organizational measures", "reasonable steps", "necessary measures" and similar language requiring sensitivity to the context in which data are processed and the risks that such processing presents.[13] In addition, the directive includes many provisions that explicitly require risk management. For example, the directive requires that security measures must "ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected"[14]; that "processing operations likely to present specific risks to the rights and freedoms of data subjects" be subject to "prior checking" by Member States[15]; that personal data may be processed when "necessary for the purposes of the legitimate interest pursued by the controller or by the third party or parties to whom data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subjects,"[16] and that access rights to data processed for scientific research may be limited "where there is clearly no risk of breaching the privacy of the data subject".[17]

- Many US privacy and security laws require risk assessments. For example, the 1988 Computer Matching and Privacy Protection Act requires government agencies to perform a cost-benefit analysis of proposed data matching.[18] The Security Rule adopted under the Health Insurance Portability and Accountability Act requires "covered entities" to "conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information" held by the organisation.[19]

- Risk assessment is also critical to "privacy by design", a concept developed by Dr. Ann Cavoukian, former Information and Privacy Commissioner of Ontario, Canada, that is increasingly reflected in modern privacy laws and organisational behaviour. To build protections for privacy into new technologies and systems, it is first necessary to understand the risks that those technologies or systems pose to privacy and how they can be reduced or controlled.[20]

In recent years, however, risk management has started to take on a more prominent role in data protection as information technologies have advanced and proliferated, and regulators and organisations have focused more attention on accountability for data processing, in addition to compliance with data protection regulations. There are numerous examples, but some of the most prominent include:

[13] *Directive 95/46/EC of the European Parliament and of the Council 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*, No. L 281/31, arts. 6(1), 11(2), 20(3), 8(2), 17(1), 6(1), 4(1), 13(1), 14, 25.

[14] Id, at art. 17.

[15] Id, at art. 20.

[16] Id, at art. 7.

[17] Id, at art. 12.

[18] 5 USC § 552a(o).

[19] 45 C.F.R. § 164.308(a)(1)(ii)(A).

[20] Information and Privacy Commissioner, Ontario, Canada, *Privacy Risk Management* (2010).

### a. CNIL *Methodology for Privacy Risk Management*

The French Commission Nationale de l'informatique et des Libertés (CNIL) led the way with its *Methodology for Privacy Risk Management*, revised most recently in 2012, which "describes *a method for managing the risks* that the processing of personal data can generate to individuals".[21] There the CNIL writes: "Using a risk management method is the safest way to ensure objectivity and relevance of the choices to make when setting up a processing of personal data".[22]

### b. FTC *Protecting Consumer Privacy in an Era of Rapid Change*

The FTC in 2012 published a report concluding a two-year process examining ways of updating privacy protection to keep pace with significant changes in technologies, markets and behaviour. In that report, the Commission recommended that companies should "implement accountability mechanisms and conduct regular privacy risk assessments to ensure that privacy issues are addressed throughout an organization".[23] The Commission stressed that its orders settling cases brought against companies for inadequate privacy protection require not merely "risk assessment", but also "the implementation of controls designed to address the risks identified" and evaluation and ongoing "adjustment of the privacy program in light of regular testing and monitoring".[24]

### c. UK ICO *Privacy Impact Assessment and Risk Management*

In 2013, the UK ICO published an exhaustive report on *Privacy Impact Assessment and Risk Management*. Prepared by Trilateral Research & Consulting, the report reflects an effort to promote a better "fit" between PIAs and "risk management standards and methodologies".[25] In addition to changes in the law and the ICO's activities, the report recommended that "senior management take privacy impacts into consideration as part of all decisions involving the collection, use and/or sharing of personal data", include "identified privacy risks in their corporate risk register", and "develop practical and easy guidance on the techniques for assessing privacy risks and actions to mitigate them".[26]

The ICO subsequently published a comprehensive PIA Code of Conduct in February 2014, which provides organisations with step-by-step guidance on how to conduct PIAs and advises them to consider privacy and related risks to individuals.[27]

---

[21] Commission Nationale de l'informatique et des Libertés, *Methodology for Privacy Risk Management* (2012), 4.

[22] Id, at 9.

[23] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change* (2012), 30.

[24] Id, at 31.

[25] Trilateral Research & Consulting, *Privacy Impact Assessment and Risk Management* (2013), 15-16.

[26] Id, at 17-18.

[27] UK Information Commissioner's Office, *Conducting Privacy Impact Assessment Code of Conduct* (2014).

### d. OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data

In 2013 the Council of Ministers of the Organisation for Economic Co-operation and Development (OECD) revised the *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, first adopted in 1980, to "implement a risk-based approach".[28] In the accompanying Explanatory Memorandum, the drafters noted the "importance of risk assessment in the development of policies and safeguards to protect privacy".[29] The scope of the revised guidelines is limited at the outset to personal data that "because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a risk to privacy and individual liberties".[30]

According to the revised guidelines, a data controller should have in place a "privacy management programme that …. provides for appropriate safeguards based on privacy risk assessment".[31] Notice to individuals of information security breaches is only required "[w]here the breach is likely to adversely affect data subjects",[32] an approach the drafters of the Guidelines describe as a "risk-based approach to notification".[33] And under the Guidelines, any restrictions to transborder data flows should be "proportionate to the risks presented, taking into account the sensitivity of the data, and the purpose and context of the processing".[34]

### e. The APEC Privacy Framework

In 2005, the Asia-Pacific Economic Cooperation forum (APEC), finalized the APEC Privacy Framework containing nine high-level privacy principles. The first principle in the Framework is the principle of "preventing harm", which is intended to ensure that privacy protections are based on the risk of harm that may flow from the misuse of data.[35]

### f. Draft Text of the European Union General Data Protection Regulation

The text of the draft European Union General Data Protection Regulation that emerged from the Parliament also stresses the need for "the controller or processor" to "evaluate the risks inherent to the processing and implement measures to mitigate those risks".[36]

The draft regulation would require data controllers to demonstrate compliance with the regulation "having regard to 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".[37] Under a wide variety of circumstances the controller would be required to "carry out a risk analysis of the

---

[28] Organisation for Economic Co-operation and Development, *Supplementary Explanatory Memorandum to the Revised Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (2013), 30.

[29] Organisation for Economic Co-operation and Development, *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, C(80)58/FINAL, as amended by C92013)79 (2013), 12.

[30] Id, at ¶ 2.

[31] Id, at ¶ 15(a).

[32] Id, at ¶ 15(c).

[33] OECD, *Supplemental Explanatory Memorandum*, at 27.

[34] *OECD Guidelines*, at ¶ 18.

[35] Asia Pacific Economic Cooperation, *APEC Privacy Framework* (2005), 11.

[36] *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)* (unofficial consolidated version after LIBE Committee vote, provided by the rapporteur, 22 October 2013), ¶ 66.

[37] Id, at art. 22.

potential impact of the intended data processing on the rights and freedoms of the data subjects, assessing whether its processing operations are likely to present specific risks".[38]

The draft of a "partial general approach" to chapter IV that has been circulated by the Council Presidency further builds on the risk-based approach, conditioning the obligations of the data controller to implement appropriate measures and be able to demonstrate compliance with the regulation on "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".[39]

More specifically, the risk-based approach is further reflected throughout the Council's text:

- The requirements of privacy by design and by default have been made more adaptable to the context of the data controller's business by taking into account the nature, scope, context and purposes of the data controller's processing activities, as well as the likelihood and magnitude of the risks to the rights and freedoms of individuals.[40]

- Data controllers established outside the EU do not need to appoint a representative in the EU for processing activities that are "occasional" and "unlikely to result in a risk" to the rights and freedoms of individuals.[41]

- The level of security measures that are considered "appropriate" is determined by analysing a broad range of factors, including the available technology; the cost of implementation; the nature, scope, context and purpose of the data controller's processing activities; and the likelihood and magnitude of the risks involved.[42]

- Data protection impact assessments are required only for processing activities that likely involve "high risk" to the rights and freedoms of individuals, such as discrimination, identity theft, fraud, or financial loss..[43]

- The requirement to consult with data protection authorities prior to commencing certain processing activities is limited to processing that "would result in a high" degree of risk "in the absence of measures to be taken by the controller to mitigate the risk".[44]

- The obligation to report data breaches extends only to those breaches that are "likely to result in a high risk for the rights and freedoms of individuals". If the compromised data are encrypted or otherwise protected so that it remains unintelligible, the data controller is not required to report the breach.[45]

---

[38] Id, at art 32a.

[39] *Note 13772/14, 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)* [First reading]—Chapter IV (2014), at 13 [art. 22.1].

[40] Id, at art. 23.

[41] Id, at recital 63, art. 25.

[42] Id, at art. 30.

[43] Id, at art. 33.

[44] Id, at art. 34.

[45] Id, at arts. 31-32.

- One of the conditions under which personal data may be transferred to a third country or international organisation is if "the data subject has consented to the proposed transfer, after having been informed of the risks of such transfers".[46]

### g. NIST Privacy Risk Model discussion draft

The US National Institute of Standards and Technology (NIST) in 2014 issued a Privacy Risk Model discussion draft to help organisations to "assess the privacy impact on individuals whose information is collected, used, stored, and transmitted by information systems, and how organizations can prevent adverse impact on those individuals".[47] NIST is developing this standard in response to a presidential executive order, and while no law requires use of the NIST model, many NIST standards and tools are used voluntarily by industry.

### h. Article 29 Working Party *Statement on the role of a risk-based approach in data protection legal frameworks*

In 2014 the Article 29 Working Party issued a *Statement on the role of a risk-based approach in data protection legal frameworks* in which it noted support for "the inclusion of a risk-based approach in the EU data protection legal framework".[48] The Working Party stressed that the role of risk management in data protection is "not a new concept, since it is already well known under the current Directive 95/46/EC", and that "the risk-based approach has gained much more attention in the discussions at the European Parliament and at the Council on the proposed General Data Protection Regulation".[49]

The Statement also notes that the role of the risk-based approach, properly understood, is to effect "scalable and proportionate … compliance"[50] and that data protection authorities under the forthcoming proposed EU Data Protection Regulation will be "targeting compliance action and enforcement activity on areas of greatest risk".[51]

### i. Article 29 Working Party *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*

Perhaps the most detailed analysis of the benefits and requirements of risk management is found in the Article 29 Working Party's 2014 opinion on the role of the "legitimate interests of the data controller" under Article 7(f) of the EU Data Protection Directive. There, while focused on the context of applying Article 7(f) as one of the grounds to legitimise processing of personal data, the Working Party proposes a classic risk management "balancing test" for data processing based on "legitimate interest" that includes:

- the nature and source of the legitimate interest and whether the data processing is necessary for the exercise of a fundamental right, is otherwise in the public interest or benefits from recognition in the community concerned;
- the impact on the individual and their reasonable expectations about what will happen to their data, as well as the nature of the data and how they are processed;

---

[46] Id, at art. 44, ¶ 1(a).

[47] National Institute of Standards and Technology, *NIST Privacy Engineering Objectives and Risk Model Discussion Draft* (2014), 3.

[48] Article 29 Data Protection Working Party, *Statement on the role of a risk-based approach in data protection legal frameworks*, 14/EN, WP218 (2014), 2.

[49] Id.

[50] Id.

[51] Id, at 4.

- additional safeguards that could limit undue impact on the individual, such as data minimisation, privacy-enhancing technologies, increased transparency, general and unconditional right to opt-out, and data portability.[52]

### j. Article 29 Working Party Opinion 03/2013 on purpose limitation

Another current application of risk analysis can be found in the Article 29 Working Party's 2013 opinion on purpose limitation.[53] Article 6(1)(b) of the EU Data Protection Directive provides that personal data collected for one or more purposes shall "not be further processed in a way incompatible with those purposes".[54] The Article 29 Working Party distinguishes between two types of "compatibility tests" or "compatibility assessments"—the more objective and legalistic "formal assessments" and "substantive assessments", which the Working Party describes as the more "flexible and pragmatic, but also more effective" type of compatibility assessment.[55] The Working Party set forth specific "key factors" to be considered during this type of substantive compatibility assessment, one of which is "the nature of the data and the impact of the further processing on the data subjects".[56] The types of "impacts" of the proposed further processing that should be considered include "both positive and negative consequences" as well as "emotional impacts [ ] such as the irritation, fear and distress that may result …".[57] According to the Working Party, "the more negative or uncertain the impact of further processing might be, the more unlikely it is to be considered a compatible use".[58] Thus, under the Working Party's opinion on purpose limitation, in order to determine if a subsequent purpose of processing satisfies the purpose limitation principle and the compatibility test, organisations are expected in appropriate circumstances to conduct risk assessments regarding the impact of the proposed further processing.

### k. Article 29 Working Party Opinion on the revised industry proposal for a privacy and data protection impact assessment framework for RFID applications

Working Party Opinion 9/2011 on the revised Industry Proposal for Privacy and Data Protection Impact Assessment Framework for RFID Applications[59] is the Working Party's response to a revised industry framework for RFID (Revised Framework) submitted by industry to amend the Working Party's earlier Opinion 5/2010 (WP 175) on the subject. Per request of the Article 29 Working Party, the Revised Framework included a "clearly defined risk assessment approach", which was missing from the earlier proposal.[60] The Working Party's Opinion endorses the Revised Framework's description of the "risk assessment phase" of Privacy Impact Assessments for RFID, including the need for the identification of risks and their potential privacy impacts as well as the appropriate controls in response to such risks. The opinion notes that the Revised Framework is based on a risk management approach, which is "an essential component of any Privacy and Data Protection Impact Assessment Framework".[61]

---

[52] 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,* 844/14/EN, WP 217 (2014), 3.

[53] Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation*, 00569/13/EN, WP 203 (2013).

[54] Id, at 20.

[55] Id, at 21.

[56] Id, at 25.

[57] Id, at 25-26.

[58] Id, at 26.

[59] Article 29 Data Protection Working Party, *Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications*, 00327/11/EN, WP 180 (2011).

[60] Id, at 3.

[61] Id, at 5.

## 3. Key Considerations for Risk Management in Effective Data Protection

Despite the longstanding role of, and intensified recent attention to, risk management in data protection, it is still a developing field that lacks many of the widely accepted principles and tools of risk management in other areas. As NIST noted recently:

> In the security field, risk management models, along with technical standards and best practices, are key components of improving security. Similarly, the safety risk management field also has well-developed models, technical standards and best practices. To date, the privacy field has lagged behind in the development of analogous components.[62]

One of the most obvious omissions is a clear understanding of the harms or negative impacts that risk management is intended to identify and mitigate in the area of data protection. As discussed in greater detail below, this is the starting point for effective risk management in other fields, yet in data protection, organisations and regulators alike have failed to articulate any comprehensive framework of harms or other impacts, much less to reach consensus regarding those that should be part of effective risk management.

This presents both an opportunity and a challenge. The opportunity is to develop modern, effective risk management tools and a framework of impacts—both harms and benefits—building on decades of experience with risk management broadly. The challenge is to do so quickly to keep pace with dramatic changes in technology and human and institutional behaviour.

Fortunately, a number of key themes for maximising the contribution of risk management to effective data protection have emerged out of the many recent government pronouncements on the subject, as well as academic and private-sector initiatives and the rich literature on risk management generally. This section addresses eleven of the most important of these considerations.

### a. The role of risk management

Risk management does not alter rights or obligations. If a law conveys a right to data protection, or provides individuals with specific rights, such as rights of access, correction or deletion, risk management cannot alter those rights; just as the law imposes obligations on controllers or processors, risk management does not change those obligations. Rather, risk management is a valuable tool for calibrating accountability, prioritising action, raising and informing awareness about risks, identifying appropriate mitigation measures and, in the words of the Article 29 Working Party, providing a "scalable and proportionate approach to compliance".[63]

While risk management does not alter rights or obligations, it may be helpful—especially for those who are not data protection experts—as a means to make those rights or obligations more concrete and decide when they are implicated. For example, under the Parliamentary text of the draft General Data Protection Regulation, "indiscriminate general notification" of security breaches would be abolished and "replaced by effective procedures and mechanism which focus instead on those processing operations which are likely to present specific risks to the rights and freedoms of data subjects".[64] Under this regime, risk assessment therefore would be necessary to know when notification or other obligations might apply.

---

[62] *NIST Privacy Engineering Objectives and Risk Model Discussion Draft*, at 1.

[63] Article 29 Data Protection Working Party, *Statement on the role of a risk-based approach in data protection legal frameworks*, at 2.

[64] Id, at ¶ 70.

Similarly, the revised *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* are limited in their scope to personal data that "because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a risk to privacy and individual liberties".[65] Absent an assessment of that risk, it is impossible to know whether the guidelines even apply.

Equally, risk management does not take away, or reduce, accountability. In fact, it is an integral component of organisational accountability and what organisations should do as part of their privacy management programs. All organisations should be accountable for their data processing activities, and therefore have in place privacy management programs that include all the agreed-upon elements of accountability (e.g. a data protection officer, effective oversight, policies and procedures, training, assessment and verification, enforcement, redress *and* risk management). How these programs are built and how they are implemented will very likely depend on the risks presented by the data processing. Risk assessment can help determine the program, its elements and the specific controls necessary, but it does not alter the obligation for controllers to be accountable and to have in place privacy management programs with all the above elements. Quite the contrary, risk management is necessary to make accountability effective and appropriate.

Risk management is also a valuable tool for prioritising organisational action. It is impossible, as well as undesirable, for any organisation—whether a controller or a regulator—to pursue everything at once and with the same commitment of resources. Risk management can help prioritise where to focus first or where to devote the greatest resources.

But whether necessary to provide a "scalable and proportionate approach to compliance," to identify when specific obligations apply, or as a tool for fine-tuning accountability or prioritising organisational action, risk management is critical in data protection. "Regardless of the size, structure or nature of an organization, its management of personal information unavoidably gives rise to risk".[66] As a result, managing those risks is critical to effective data protection.

### b. A balancing test

Risk management is fundamentally a balancing test that takes into account many factors. In the words of the Article 29 Working Party, discussing application of Article 7(f) of the EU data protection directive: "it requires a balancing of the legitimate interests of the controller, or any third parties to whom the data are disclosed, against the interests or fundamental rights of the data subject".[67]

As the Article 29 Working Party goes on to note, however, the "assessment is not a straightforward balancing test consisting merely of weighing two easily quantifiable and comparable 'weights' against each other".[68] For example, the individual, as well as the controller and third parties, may enjoy substantial benefits that result from the processing of personal data. The balancing process must therefore reflect sensitivity to a wide range of competing factors. It must also reflect "the need for some flexibility [which] comes from the very nature of the right to the protection of personal data and the right to privacy".[69]

---

[65] *OECD Guidelines*, at ¶ 2.

[66] Cavoukian, at 3.

[67] 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*, at 3.

[68] Id.

[69] Id, at 11.

Indeed, as the Article 29 Working Party stresses, data protection and privacy rights, "along with most (but not all) other fundamental rights, are considered relative, or qualified, human rights. These types of rights must always be interpreted in context. Subject to appropriate safeguards, they can be balanced against the rights of others. In some situations—and also subject to appropriate safeguards—they can also be restricted on public interest grounds".[70]

In fact, "important and compelling legitimate interests may in some cases and subject to safeguards and measures justify even significant intrusion into privacy or other significant impact on the interests or rights of the data subjects".[71] Risk management is therefore critical to determining how to balance those competing interests and rights, and also operates with wide scope precisely because those interests and rights can be balanced.

The range of factors to be considered in risk management in the data protection context include the fundamental rights and interests of individuals, the likelihood that the proposed processing will harm individuals, the severity of the harm if it occurs, the measures available to mitigate risk, the rights and interests of data controllers, the likelihood that benefits will result from the proposed processing, and the magnitude of those benefits. Other factors may influence that balance, and the specific elements of the balance are discussed in greater detail below.

### c. Severity *and* likelihood

It is universally recognised that the balancing inherent in risk management must take into account both the *magnitude* of potential impacts—positive and negative—and their *likelihood* of occurring. The default global risk management standard ISO 31000, maintained by the International Organization for Standardization, defines "level of risk" as the "magnitude of a risk or combination of risks" and "their likelihood".[72]

The point is that a risk is not a mere possibility of a consequence occurring, but rather must be understood in terms of its probability of occurring and its impact if it does occur. As the ISO writes in its definition of "risk analysis": "Risk analysis involves consideration of the causes and sources of risk, their positive and negative consequences, and the likelihood that those consequences can occur".[73]

The CNIL's *Methodology for Privacy Risk Management* adopts similar language for the data protection context:

> The **risk level** is estimated in terms of severity and likelihood.
> **Severity** represents the magnitude of a risk. It essentially depends on the level of identification of personal data and the level of consequences of the potential impacts.
> **Likelihood** represents the feasibility of a risk to occur. It essentially depends on the level of vulnerabilities of the supporting assets facing the level of capabilities of the risk sources to exploit them.[74]

---

[70] Id, at 11-12 (citation omitted).

[71] Id, at 30 (citation omitted).

[72] International Organization for Standardization, *ISO 31000:2009 Risk management—Principles and guidelines*, definition 3.6.1.8. Interestingly, in a footnote to the definition of "likelihood", the ISO notes that "the English term 'likelihood' does not have a direct equivalent in some languages; instead, the equivalent of the term 'probability' is often used. However, in English, 'probability' is often narrowly interpreted as a mathematical term. Therefore, in risk management terminology, 'likelihood' is used with the intent that it should have the same broad interpretation as the term 'probability' has in many languages other than English". Id, at definition 3.6.1.1.

[73] Id.

[74] CNIL, *Methodology for Privacy Risk Management*, at 8 (emphasis in original).

The Article 29 Working Party has expanded on this approach in the context of application of Article 7(f) of the EU data protection directive, and, in keeping with risk assessment methodologies in other areas, talks in terms of "impacts", which it defines broadly as "any possible (potential or actual) consequences of the data processing".[75] Impacts, in turn, are assessed by "two key elements—the likelihood that the risk materializes on the one hand, and the severity of the consequences on the other hand—each [of which] contribute to the overall assessment of the potential impact".[76]

Not all discussions of risk in the data protection environment are as punctilious as the CNIL and the Article 29 Working Party in recognising that understanding risks necessarily requires understanding both the potential impact and the likelihood of that impact occurring. The draft text from the Parliament of the General Data Protection Regulation, for example, requires supervisory authorities to help make the public aware of "risks", a term the drafters seem to use generically, like "threats". This is a common and understandable mistake, but one that tends to obscure the importance of evaluating both impact and likelihood when assessing "risk", and that may waste both attention and resources on threats that are unlikely to materialise or affect individuals if they do.

### d. Identify impacts

#### i. The need for a framework

One key requirement of all risk management tools is to identify impacts—both harms and other negative impacts that effective data protection is intended to avoid or mitigate, and benefits and other positive impacts. In the terms of ISO 31000, the "organization should identify sources of risk, areas of impacts, events (including changes in circumstances) and their causes and their potential consequences. The aim of this step is to generate a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives".[77]

Historically, this has been one of the weakest links in data protection risk management. For example, many laws requiring PIAs fail to specify what "impacts" the PIA is to be assessing, or to require that organisations conducting PIAs identify those impacts.

The Centre for Information Policy Leadership's 2014 paper, *A Risk-based Approach to Privacy: Improving Effectiveness in Practice*, focuses on this critical issue: "Data protection and privacy laws are meant to protect people, not data. But from what exactly are people being protected? What threats? What harms? What risks?"[78] The Centre proposed a matrix of these harms in an effort to move the process of creating, vetting and ultimately building consensus around a framework of harms and other negative impacts. Much work remains to be done on the critical issue of identifying the relevant impacts that should be considered in risk management.

As NIST has noted: "Harms from security breaches are generally well understood. In privacy, consensus is still being developed around what constitutes harms. However, if the privacy engineering objectives are intended to mitigate the risk of privacy harms, then the underlying harms need to be explicated in order to assess the utility of the objectives".[79]

---

[75] 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*, at 37.

[76] Id, at 38.

[77] *ISO 31000:2009*, at 5.4.2.

[78] CIPL, *A Risk-based Approach to Privacy*, at 2.

[79] *NIST Privacy Engineering Objectives and Risk Model Discussion Draft*, at 3, n.9.

### ii. A broad concept of "impacts"

There is general agreement, in the words of the OECD, that " '[r]isk' is intended to be a broad concept, taking into account a wide range of possible harms to individuals".[80] But there has been little progress beyond this.

The CNIL has observed that "damage to data subjects" may be:

- physical (loss of amenity, disfigurement or economic loss related to physical integrity);
- material (loss incurred or lost revenue with respect to an individual's assets);
- moral (physical or emotional suffering, disfigurement or loss of amenity, etc.).[81]

NIST has identified as "privacy harms":

- Harms to individuals that result from problematic data actions;
- Loss of self-determination;
- Discrimination;
- Loss of trust;
- Economic loss.[82]

The Centre for Information Policy Leadership's 2014 paper provides a catalogue of possible "harms" under three headings: "tangible damage to individuals, intangible distress to individuals, and societal harm".[83] The paper provides the following illustrative examples of each:

> **Tangible damage,** normally physical or economic, includes:
>
> - bodily harm;
> - loss of liberty or freedom of movement;
> - damage to earning power; and
> - other significant damage to economic interests, for example arising from identity theft.
>
> **Intangible distress,** assessed objectively, includes:
>
> - detriment arising from monitoring or exposure of identity, characteristics, activity, associations or opinions;
> - chilling effect on freedom of speech, association, etc.;
> - reputational harm;
> - personal, family, workplace or social fear, embarrassment, apprehension or anxiety;
> - unacceptable intrusion into private life; and
> - discrimination or stigmatisation.

[80] OECD, *Supplemental Explanatory Memorandum*, at 24.
[81] CNIL, *Methodology for Privacy Risk Management*, at 13, n.21.
[82] NIST, *Privacy Engineering Objectives and Risk Model—Discussion Deck*, 2014, at 25-29.
[83] CIPL, *A Risk-based Approach to Privacy*, at 6-7.

**Societal harm** can arise directly from business activity. But it is more likely where the personal information, quite possibly obtained legally or otherwise from businesses, is used by governmental bodies. It includes:

- damage to democratic institutions, for example excessive state or police power; and
- loss of social trust ("who knows what about whom?").[84]

The most recent text of the Council's "partial general approach" to chapter IV of the draft EU General Data Protection Regulation reflects another recent effort to identify possible negative impacts. The proposed Article 31 provides for prompt notification of supervisory authorities about any security breach "which is likely to result in a high risk for the rights and freedoms of individuals, such as discrimination, identity theft or fraud, financial loss, breach of pseudonymity, damage to the reputation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage".[85]

### iii. Positive impacts

Impacts also include positive impacts. The Article 29 Working Party has provided a "non-exhaustive list of some of the most common contexts in which the issue of legitimate interest in the meaning of Article 7(f) may arise".[86] There are close links here between these contexts and positive impacts of specific processing. The Working Party's list includes:

- exercise of the right to freedom of expression or information, including in the media and the arts;
- conventional direct marketing and other forms of marketing or advertisement;
- unsolicited non-commercial messages, including for political campaigns or charitable fundraising;
- enforcement of legal claims including debt collection via out-of-court procedures;
- prevention of fraud, misuse of services or money laundering;
- employee monitoring for safety or management purposes;
- whistle-blowing schemes;
- physical security, IT and network security;
- processing for historical, scientific or statistical purposes; and
- processing for research purposes (including marketing research).[87]

There are obviously other impacts that may result from processing data. It is critical that risk management processes take those into account.

---

[84] Id (emphasis in original) (numbering and punctuation altered).

[85] *Note 13772/14, 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)* [First reading]—Chapter IV (2014), at 24 [art. 31.1].

[86] 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*, at 24.

[87] Id, at 25.

### iv. Need for consensus and predictability

Making risk management work effectively and consistently requires that there be a widely shared classification of impacts—positive and negative—on individuals, organisations and society. Specific categories might differ from country to country or culture to culture. But the absence of a common understanding—transcending the detail of regional differences—as to what impacts should be minimised (or maximised) threatens not only quality risk management and meaningful accountability, but also effective data protection.

As the Centre for Information Policy Leadership has noted: "There is a particular benefit in developing a common and objective approach to risk management and an objective notion of harm or adverse impact to individuals that are acceptable and useful to as many businesses and regulators as possible".[88]

Moreover, the approach to impacts needs to be based on "*objective* descriptors of harm—it is harm imposed on the reasonable man or woman in this context. In the same way as tort law ignores the 'egg-shell skull', the test is not, and cannot be, concerned with the impact on each particular individual, let alone an individual with particular sensibilities".[89]

The fact that privacy is a fundamental right does not answer this urgent need for a common approach to risk management and a widely shared understanding of the relevant harms and impacts. After all, as the Article 29 Working Party has noted, risk management does not alter the nature of rights, but rather the way in which their protection is implemented.

Similarly, some guidance documents focus on "specific objective criteria" that might affect risk, such as "the nature of personal data (e.g. sensitive or not), the category of data subject (e.g. minor or not), the number of data subjects affected, and the purpose of the processing".[90] These may or may not result in negative impacts, but they are not in and of themselves impacts at all that the risk management is intended to help avoid or mitigate. Nor are they necessarily to be avoided. For example, processing personal data about a child or a large number of people may result in no negative impacts if done appropriately and subject to specified protections.

### v. Impacts affecting organisations

When identifying specific impacts, it is important to remember that privacy-related negative impacts may affect organisations as well as individuals. The prospect of economic and/or reputational damage is likely to be one of the most powerful motivations for organisations to adopt a risk management approach as a matter of enlightened self-interest. The UK ICO has noted that "[p]rivacy risks fall into two categories".[91] The first is "[r]isks to the individual as a result of contravention of their rights in relation to privacy, or loss, damage, misuse or abuse of their personal information".[92] The second is:

> Risks to the organisation as a result of:
>
> - perceived harm to privacy;
> - a failure to meet public expectations on the protection of personal information;

---

[88] CIPL, *A Risk-based Approach to Privacy*, at 4.
[89] Id, at 7.
[90] Article 29 Data Protection Working Party, *Statement on the role of a risk-based approach in data protection legal frameworks*, at 4.
[91] UK Information Commissioner's Office, *Privacy Impact Assessment Handbook 2.0*, ch. 2.
[92] Id.

- retrospective imposition of regulatory conditions;
- low adoption rates or poor participation in the scheme from both the public and partner organisations;
- the costs of redesigning the system or retrofitting solutions;
- collapse of a project or completed system;
- withdrawal of support from key supporting organisations due to perceived privacy harms; and/or
- failure to comply with the law, leading to:
  - enforcement action from the regulator; or
  - compensation claims from individuals.[93]

### vi. Risks of inaction and uncertainty

There are often substantial impacts caused by not processing data and, as the ISO has noted, it is "important to identify the risks associated with not pursuing an opportunity"[94]—what are sometimes called "reticence risks". Moreover, there also may be substantial impacts caused by ambiguity as to whether specific data processing is permissible, what the Japanese government has recently described as the "Gray Zone" where it is unclear as to whether the free use of information is allowed.[95] Whether the result of a clear choice or uncertainty, the effects of not using data can be significant. The lack of a clear, broadly accepted framework of impacts can contribute to the existence of the "Gray Zone", leaving controllers on their own when assessing risk or unwilling to accept even minor risks that may be justified by significant benefits to individuals, organisations or societies. Whatever the cause, failure to process information can significantly affect the fundamental rights, health, safety and other interests of both individuals and organisations.

The risks of both inaction and uncertainty were recently clearly demonstrated in a 12 November 2014 report by the Brookings Institution. The report stresses the potential of anonymised data from burgeoning mobile communication in the developing world for "unprecedented insights" for both "individuals and societies" into "migration patterns, economic transactions, and even importation routes of infectious diseases like Ebola".[96]

In the case of Ebola, the need is as urgent as the potential is great. According to the *Economist*:

> Until recently the standard way to model the spread of a disease relied on extrapolating trends from census data and surveys. CDRs [call data records], by contrast, are empirical, immediate and updated in real time. You do not have to guess where people will flee to or move …. If researchers could track population flows from an area where an outbreak had occurred, they could see where it would be likeliest to break out next—and therefore where they should deploy their limited resources.[97]

"Yet", the *Economist* continues, "despite months of talks, and the efforts of the mobile-network operators' trade association [the GSMA] and several smaller UN agencies, telecoms firms have not let

---

[93] Id.

[94] *ISO 31000:2009*, at 5.4.2.

[95] Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society, *Outline of the System Reform Concerning the Utilization of Personal Data* (2014), 4.

[96] Yves-Alexandre de Montjoye, Jake Kendall & Cameron F. Kerry, *Enabling Humanitarian Use of Mobile Phone Data*, Brookings Institution Issues in Technology Innovation, no. 26, (2014).

[97] "Waiting on Hold", *Economist*, 25 October 2014.

researchers use the data".[98] The reason is "the absence of a common framework for sharing mobile phone data in privacy-conscientious ways and an uncertain regulatory landscape".[99] A solution will "require government action" to resolve the uncertainty about the privacy issues.[100] This example highlights the broader issue of ensuring that risk management takes into account risks associated with not processing data, whether the result of a deliberate choice or a regulatory "Gray Zone".

The Ebola example also highlights the important roles that regulators and enforcement officials fill in the data protection risk management process to help resolve ambiguity and enhance predictability and consistency through not only enforcement actions, but also guidance documents, workshops, transparent consultations, collections of best practices and other measures. Without question, the ultimate responsibility, the burden of proof and liability for making specific risk management determinations, rests with individual controllers, but there is much data protection authorities can and should do to enhance the quality and consistency of those decisions while also ensuring that the interests of individuals and society are both represented and protected.

### e. Mitigating measures in risk management

To manage risk effectively, it is necessary to include mitigation measures in the balance. ISO 31000 notes that risk analysis includes not only "consideration of the causes and sources of risk, their positive and negative consequences, and the likelihood that those consequences can occur", but also "[e]xisting controls and their effectiveness and efficiency".[101]

The Parliamentary text of the draft General Data Protection Regulation implements this fundamental principle of risk management:

> Data protection impact assessments should consequently have regard to the entire lifecycle management of personal data from collection to processing to deletion, describing in detail the envisaged processing operations, the risks to the rights and freedoms of data subjects, *the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure compliance with the regulation*.[102]

The consideration of mitigation measures, safeguards and other controls is often an iterative process. Some safeguards may be in place from the beginning of the risk management and so should be considered from the start of the process. For example, a bank that encrypts all its customer financial data at all times—at rest and in transit—would certainly consider that when assessing the likelihood that a specific harmful impact (for example, financial fraud or identify theft) might occur.

At the same time, sometimes a risk assessment is used to identify specific risks that only then does the controller determine how to mitigate. In its opinion on the application of "legitimate interests" in Article 7(f) of the EU data protection directive, the Article 29 Working Party refers to this as a "provisional balance", which then may be followed by consideration of "additional safeguards applied by the controller to prevent any undue impact on the data subjects".[103] That outcome of this additional

---

[98] Id.

[99] Montjoye, et al.

[100] "Waiting on Hold".

[101] *ISO 31000:2009*, at 5.4.3.

[102] *Draft EU General Data Protection Regulation* (unofficial consolidated version after LIBE Committee vote), at recital 71a (emphasis added).

[103] 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*, at 33.

consideration is an identification of "residual risk", which, as described below, cannot or perhaps should not be reduced further.

In either case, that privacy risk management explicitly includes measures for mitigating or avoiding the risks. The Article 29 Working Party has identified a number of risk mitigation measures in the context of applying legitimate interests under Article 7(f) of the EU Data Protection Directive:

- technical and organisational measures to ensure that the data cannot be used to take decisions or other actions with respect to individuals ('functional separation' as is often the case in a research context)
- extensive use of anonymisation techniques
- aggregation of data
- privacy-enhancing technologies, privacy by design, privacy and data protection impact assessments
- increased transparency
- general and unconditional right to opt-out
- data portability & related measures to empower data subjects.[104]

The UK ICO considered the role of privacy risk mitigation and risk avoidance in detail in its *Privacy Impact Assessment Handbook*:

> A mitigation measure is a feature that compensates for other, privacy intrusive aspects of a design. A mitigation measure may compensate partially or wholly for a negative impact. Examples include:
>
> - minimisation of personal data retention by not recording it;
> - destruction of personal information as soon as the transaction for which it is needed is completed;
> - destruction schedules for personal information which are audited and enforced;
> - limits on the use of information which has been collected for a very specific purpose, with strong legal, organisational and technical safeguards preventing its application to any other purpose;
> - design, implementation and resourcing of a responsive complaints-handling system, backed by serious sanctions and enforcement powers. Problems must be analysed, to devise acceptable avoidance and mitigation measures.[105]
>
> An avoidance measure is a means of dissipating a risk. It refers to the exclusion of technologies, processes, data or decision criteria in order to avoid particular privacy issues' arising. Examples include:
>
> - minimising the collection of personal information to what is strictly necessary;
> - non-collection of contentious data-items;
> - active measures to stop or block the use of particular information in decision making (a good example of this is ethnic monitoring forms being filled out anonymously when companies are recruiting);

[104] 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*, at 42.

[105] UK Information Commissioner's Office, *Privacy Impact Assessment Handbook 2.0*, at ch. 2.

- active measures to preclude the disclosure of particular data-items, for example screening or hiding of certain services which are being provided to the individual which might disclose other personal information;
- non-adoption of biometrics in order to avoid issues about invasiveness of people's physical selves.[106]

### f. The goal of risk management: the role of proportionality

Rarely can risk be eliminated entirely. As Dr. Cavoukian has noted: "Risk is inherent in any pursuit which seeks to create value. Successful organizations, regardless of size, industry or structure, grow because they continually seek ways to embrace new opportunities and to manage risk—both need to be done effectively".[107]

Therefore, the goal of the risk management process is to reduce the risk as fully as practical and to be explicit about the remaining risks and how they will be managed so that the controller, and ultimately the data subjects and the regulators, understand the risks and undertakings that remain.

The Trilateral Research report for the UK ICO describes this as "accepting the risks", and it is a necessary endpoint because few risks can be eliminated entirely:

> In some instances, because of the nature of the risks, impacts or liabilities, the chances of the risks being realised or the minimal impact they may have, it might be entirely appropriate to simply recognise and accept the privacy risks or certain aspects of the privacy risks. However, this must not be done simply as an alternative to taking action to address risk and must be considered carefully as an option. If considering this option, ensure that a record of the identified risk is made, along with the reasons for accepting the risk.[108]

Risk management can also identify "appropriate" responses, meaning responses that are effective in mitigating risks, but also support the often critical benefits that risk management necessarily involves balancing.

The Explanatory Memorandum that accompanied the 2013 revisions to the OECD Guidelines makes clear that management of "risk" is intrinsically connected with "proportionality", indicating, in the context of transborder data flows for example, that "any restrictions upon transborder data flows imposed by Member countries should be proportionate to the risks presented (i.e. not exceed the requirements necessary for the protection of personal data), taking into account the sensitivity of the data,[and] the purpose and context [of the] processing".[109]

The Article 29 Working Party has recently echoed this theme in the context of applying legitimate interests under Article 7(f) of the EU Data Protection Directive: "The purpose of the Article 7(f) balancing exercise is not to prevent any negative impact on the data subject. Rather, its purpose is to prevent disproportionate impact. This is a crucial difference".[110]

---

[106] Id.
[107] Cavoukian, at 3.
[108] UK Information Commissioner's Office, *Privacy Impact Assessment Handbook 2.0*, at ch. 2.
[109] OECD, *Supplemental Explanatory Memorandum,* at 30.
[110] 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,* at 41.

The Parliamentary text of the draft General Data Protection Regulation makes clear that controllers should "ensure an *appropriate* level of security, taking into account the state of the art and the costs of their implementation in relation to the risks and the nature of the personal data to be protected".[111] One goal of risk management is to identify what level of security or notification or protection for transborder data flows is "appropriate".

The professional risk management literature often describes a tool used to accomplish this as a "heat map" or "risk profile".[112] The CNIL in its *Methodology for Privacy Risk Management* provides an effective example of how this heat map would work in practice. After describing a variety of ways of assessing risks on a scale from "negligible" to "maximum", the *Methodology* sets "objectives" based on where "risks are located on the map (in order of priority):"

1. Risks with a high severity and likelihood absolutely must be avoided or reduced by implementing security measures that reduce both their severity and their likelihood. Ideally, care should even be taken to ensure that these risks are treated by independent measures of prevention (actions taken prior to a damaging event), protection (actions taken during a damaging event) and recovery (actions taken after a damaging event).
2. Risks with a high severity but a low likelihood must be avoided or reduced by implementing security measures that reduce either their severity or their likelihood. Emphasis must be placed on preventive measures.
3. Risks with a low severity but a high likelihood must be reduced by implementing security measures that reduce their likelihood. Emphasis must be placed on recovery measures.
4. Risks with a low severity and likelihood may be taken, especially since the treatment of other risks should also lead to their treatment.[113]

The goal is to focus data protection resources where the severity and likelihood of negative impacts are greatest and, conversely, to recognise that some risks can be tolerated. After all, in the words of PricewaterhouseCoopers: "Overcontrolling risk can be costly and stifle innovation".[114]

### g. Efficient, scalable and flexible risk management

Unnecessarily burdensome risk management requirements can also be costly and stifle innovation, as regulators have recognised. The requirements for risk management, therefore, should be scalable, so that they can be effective in protecting personal privacy across the billions of data processing operations performed around the world every day. Many of these take place in the context of large organisations, but many (perhaps most) are pursued by small organisations with few resources to dedicate to complicated risk management measures. Requirements for risk management must be both scalable and flexible. Equally, where small organisations engage in data practices that may cause harm and negative impact on individuals, they not only have a duty to comply with the law, but also to implement accountability measures, such as risk assessment, to avoid and mitigate such harm.

It is critical to ensure not only that risk management generates well-targeted, appropriate protections, but also that the risk management tools themselves are well targeted and appropriate. This has been a

[111] *Draft EU General Data Protection Regulation* (unofficial consolidated version after LIBE Committee vote), at ¶ 66 (emphasis added).
[112] PricewaterhouseCoopers, at 6.
[113] CNIL, *Methodology for Privacy Risk Management*, at 19 (emphasis in original).
[114] PricewaterhouseCoopers, at 33.

particular focus of the ongoing negotiation over the EU General Data Protection Regulation. In its 3 October 2014 note to the Council detailing efforts to reach agreement on a "partial general approach" to Article IV, the Presidency noted "the need to further reduce the administrative burden/compliance costs flowing from this Regulation by sharpening the risk-based approach".[115] As one step towards that end, the draft text suggests that "best practices to mitigate the risk" could be provided by "approved codes of conduct, approved certifications, guidelines of the European Data Protection Board or through the indications provided by a data protection officer".[116]

In addition, the regulation of risk management should avoid unnecessary or duplicative risk assessments. For example, the Parliamentary text of the draft EU General Data Protection Regulation provides that a "single assessment shall be sufficient to address a set of similar processing operations that present similar risks".[117]

### h. Integration with other risk management approaches

As noted, most large organisations have been engaged in risk management for decades and already face a wide array of legal and professional requirements to perform risk assessment and mitigation in many areas. It is therefore important that data protection risk management tools fit within existing risk management methodologies and programs. This is necessary for many reasons, including allowing data protection risk management to take advantage of expertise developed in other areas, ensuring that data protection risk management takes advantage of the considerable resources already being devoted by organisations to risk management in other areas, and enhancing the efficiency (and reducing the cost) of data protection risk management.

Former Canadian Privacy Commissioner Jennifer Stoddart stresses the importance of integration with existing risk management practice in the context of PIAs:

> In order to better encourage the early consideration of privacy risks, we believe there is a need to integrate PIA practices with an organisation's overall approach to risk management. This occurs not only at an operational level—that is, through the PIA triggers or screening devices previously discussed—but by linking existing regulatory requirements with other program activities and their administrative processes. Ideally, senior managers should be using privacy impact assessment, in conjunction with other social and economic analyses, to influence the subsequent development of programs, services, plans and policies.[118]

One of the advantages that the CNIL notes of its *Methodology for Privacy Risk Management* is that it "naturally fits into global risk management approaches".[119]

---

[115] *Note 13772/14, 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)* [First reading]—Chapter IV (2014), at 1.

[116] Id, at 4.

[117] *Draft EU General Data Protection Regulation* (unofficial consolidated version after LIBE Committee vote), at art. 33, ¶ 1.

[118] Stoddart, Jennifer, "Auditing Privacy Impact Assessments: The Canadian Experience," in David Wright & Paul De Hert, eds., *Privacy Impact Assessment* (2012), 430.

[119] CNIL, *Methodology for Privacy Risk Management*, at 6.

ISO 31000 highlights another advantage of integrating risk management fully into organisational processes—namely, ensuring that it includes all the relevant information from all the organisation's activities:

> Risk management should be embedded in all the organization's practices and processes in a way that it is relevant, effective and efficient. The risk management process should become part of, and not separate from, those organizational processes. In particular, risk management should be embedded into the policy development, business and strategic planning and review, and change management processes. There should be an organization-wide risk management plan to ensure that the risk management policy is implemented and that risk management is embedded in all of the organization's practices and processes.[120]

### i. The scope of risk management

There is widespread agreement that risk management must have a broad scope that includes, in the words of the Parliamentary text of the draft General Data Protection Regulation, the "entire lifecycle management of personal data from collection to processing to deletion".[121] The FTC made a similar point in its 2012 report, *Protecting Consumer Privacy in an Era of Rapid Change*: "Companies should maintain comprehensive data management procedures throughout the life cycle of their products and services".[122]

This has two significant corollaries. The first is that while a controller can assess risk around specific processing activities (e.g. data collection, data use, data sharing, etc.), it must also ensure that the risk assessments are valid, and the mitigation measures effective, in light of all the organisation's processing activities. For example, an organisation may correctly conclude that there is little risk to individuals posed by a specific use of personal data, but if those data are stored or retained inappropriately, there may still be risks that need to be addressed.

The second implication of the broad scope of risk management is that it must continue over time as long as the data are being stored, used or processed in any way. The Parliamentary text of the draft General Data Protection Regulation, for example, would require that the "risk analysis shall be reviewed at the latest after one year, or immediately, if the nature, the scope or the purposes of the data processing operations change significantly".[123]

### j. Assessment of risk management

Risk management itself must be assessed to ensure that the methodologies being employed continue to be valid, the range of impacts—positive and negative—and possible mitigation tools remain current, the outcomes are reasonable and the conclusions of assessments are being complied with.

This is a requirement of responsible risk management generally, as PricewaterhouseCoopers notes in its *Practical Guide to Risk Assessment*: "Risk management discipline then ensures that risk assessments

---

[120] *ISO 31000:2009*, 4.3.4.

[121] *Draft EU General Data Protection Regulation* (unofficial consolidated version after LIBE Committee vote), at art. 33, ¶ 3.

[122] FTC, *Protecting Consumer Privacy in an Era of Rapid Change*, at 32.

[123] *Draft EU General Data Protection Regulation* (unofficial consolidated version after LIBE Committee vote), at art. 32a, ¶ 4.

become an ongoing process, in which objectives, risks, risk response measures, and controls are regularly re-evaluated".[124]

Ongoing assessment is explicitly required by ISO 31000:

> 4.5 Monitoring and review of the framework
>
> In order to ensure that risk management is effective and continues to support organizational performance, the organization should:
>
> - measure risk management performance against indicators, which are periodically reviewed for appropriateness;
> - periodically measure progress against, and deviation from, the risk management plan;
> - periodically review whether the risk management framework, policy and plan are still appropriate, given the organizations' external and internal context;
> - report on risk, progress with the risk management plan and how well the risk management policy is being followed; and
> - review the effectiveness of the risk management framework.
>
> 4.6 Continual improvement of the framework
>
> Based on results of monitoring and reviews, decisions should be made on how the risk management framework, policy and plan can be improved. These decisions should lead to improvements in the organization's management of risk and its risk management culture.[125]

And the importance of ongoing review is highlighted in all the recent data protection risk management regulatory documents. For example, paragraph 15(a)(vi) of the revised OECD Guidelines "stipulates that privacy management programmes should be routinely reviewed and updated to ensure that they remain appropriate to the current risk environment".[126]

### k. Organisational support for risk management

Effective risk management requires significant organisational support. This requires appropriate resources, such as those suggested by ISO 31000:

- people, skills, experience and competence;
- resources needed for each step of the risk management process;
- the organization's processes, methods and tools to be used for managing risk;
- documented processes and procedures;
- information and knowledge management systems; and
- training programmes.[127]

---

[124] PricewaterhouseCoopers, at 6.
[125] *ISO 31000:2009*, at 4.5-4.6.
[126] OECD, *Supplemental Explanatory Memorandum*, at 25.
[127] *ISO 31000:2009*, at 4.3.5.

Beyond tangible resources, however, risk management requires consistent support from an organisation's top management. Even if risk can be assessed from within a risk management or privacy group, it cannot be mitigated or avoided without strong support from the board and senior management. As professional risk managers often note, risk management reflects the cultures of organisations and the commitment of organisational leaders.

## 4. Conclusion

Legislators and regulators are focusing new and valuable attention on expanding and standardising the practice of risk management in data protection. This new attention builds on longstanding legal requirements and behaviour by responsible organisations, a wide range of other legal requirements for risk management, and a rich literature illuminating professional risk management.

There is a growing consensus around risk management as an essential tool for effective data protection. While risk management does not alter rights or obligations, it is a valuable tool for calibrating accountability, prioritising action, raising and informing awareness about risks and identifying appropriate mitigation measures. This paper has sought to highlight key principles about which there is widespread agreement. There are still, however, key issues to be resolved. These include the need to:

- Develop and build multinational consensus around a taxonomy of data protection harms or other negative impacts and benefits, and a framework or categories for assessing them;

- Develop and build consensus around risk management models, technical standards, best practices and tools that are both flexible and scalable for risk management in data protection;

- Draw upon extensive experience in risk management in other areas, both to enhance risk management in data protection and to ensure that it is well integrated with existing, widely used risk management processes;

- Practise greater consistency and precision in the use of risk management terms and processes (for example, to avoid confusing "risks" and "threats" and to ensure that risks are assessed in terms of both impact and likelihood);

- Develop a deeper understanding of proportionality and the conditions under which risks may be tolerated or accepted; and

- Explore further how, as a step towards greater interoperability, organisations can use risk management as a critical tool to manage compliance in the face of divergent national and sectoral legal requirements.

The Centre for Information Policy Leadership looks forward to continuing to work on these and other issues with all stakeholders to ensure that risk management achieves its full potential as a tool for ensuring compliance with data protection laws and protecting fundamental rights.

**Appendix**
**Centre for Information Policy Leadership**
**Privacy Risk Framework and the Risk-based Approach to Privacy**
**Workshop II**
**18 November 2014**
**Brussels**
**Attendee List**

**Centre for Information Policy Leadership**
**Privacy Risk Framework and the Risk-based Approach to Privacy**
**Workshop II**
**18 November 2014**
**Brussels**
**Attendee List**

| | |
|---|---|
| Vivienne Artz | Citi |
| Bojana Bellamy | Centre for Information Policy Leadership |
| Julie Brill | US Federal Trade Commission |
| Geff Brown | Microsoft Corporation |
| Emma Butler | LexisNexis |
| Giovanni Buttarelli | European Data Protection Supervisor (EDPS) |
| Fred Cate | Centre for Information Policy Leadership |
| Isabelle Chatelier | European Data Protection Supervisor (EDPS) |
| Helen Crooks | Independent Data Strategy Consultant |
| Gary Davis | Apple Inc. |
| Ted Dean | International Trade Administration, US Department of Commerce |
| Dirk De Bot | Commission for the Protection of Privacy (Belgium) |
| Ulrika Dellrud | Oracle Corporation |
| Luca De Matteis | Permanent Representation of Italy to the EU |
| Michael Donohue | Organisation for Economic Co-operation and Development (OECD) |
| Stephanie Driggers | UPS |
| Nicolas Dubois | European Commission |
| Patrice Ettinger | Pfizer, Inc. |
| Peter Fleischer | Google Inc. |
| Rafael García Gozalo | Agencia Española de Protección de Datos (Spain) |
| Julie Gibson | The Procter & Gamble Company |
| Jennifer Glasgow | Acxiom |
| Lynn Goldstein | Center for Urban Science and Progress (CUSP), NYU |
| Dominique Hagenauw | Dutch Data Protection Authority |
| Ben Hayes | Nielsen |
| Frances Henderson | Council for Better Business Bureaus |
| Markus Heyder | Centre for Information Policy Leadership |
| Hielke Hijmans | Free University Brussels/University of Amsterdam |
| Jörg Hladjk | Hunton & Williams |
| Jane Horvath | Apple Inc. |
| Peter Hustinx | European Data Protection Supervisor (EDPS) |
| Marisa Jimenez | Google Inc. |
| Constantine Karbaliotis | Nymity |

| | |
|---|---|
| Jacob Kohnstamm | Dutch Data Protection Authority |
| Karen Kornbluh | Nielsen |
| Michael Lamb | Reed Elsevier |
| Teena Lee | The Estée Lauder Companies Inc. |
| Naomi Lefkovitz | National Institute of Standards and Technology (NIST) |
| Ilaria Liccardi | MIT Computer Science and Artificial Intelligence Laboratory (CSAIL) |
| Adriana Lopez-Tafall | Merck & Co., Inc. |
| Caroline Louveaux | MasterCard |
| Sophie Louveaux | European Data Protection Supervisor (EDPS) |
| Brendon Lynch | Microsoft Corporation |
| William Malcolm | Google Inc. |
| Josh Maxfield | Garmin |
| Terry McQuay | Nymity |
| John Midgley | Intuit Inc. |
| Wim Nauwelaerts | Hunton & Williams |
| Saira Nayak | TUNE |
| Mikko Niva | Nokia Corporation |
| Marie Olson | The Boeing Company |
| Christina Peters | IBM |
| Daniel Pradelles | Hewlett-Packard Company |
| Florence Raynal | Commission nationale de l'informatique et des libertés (CNIL) |
| David Ritchie | International Trade Administration |
| Marie Charlotte Roques-Bonnet | Microsoft Corporation |
| Eva Salzmann | IBM |
| Sachiko Scheuing | Acxiom |
| Russell Schrader | Visa Inc. |
| Manuela Siano | Garante per la Protezione dei Dati Personali (Italy) |
| David Smith | Information Commissioner's Office (UK) |
| JoAnn Stonier | MasterCard |
| Richard Thomas | Centre for Information Policy Leadership |
| Louise Thorpe | American Express Company |
| Bridget Treacy | Hunton & Williams |
| Vincent Vandepitte | The Procter & Gamble Company |
| Cristina Vela | Telefónica, S.A. |
| Pat Walshe | GSM Association |
| Hilary Wandall | Merck & Co., Inc. |
| Justin Weiss | Yahoo! Inc. |
| Daniel Weitzner | MIT Computer Science and Artificial Intelligence Laboratory (CSAIL) |
| Wojciech Wiewiorowski | Generalny Inspektor Ochrony Danych Osobowych (Poland) |
| Boris Wojtan | Accenture |