Organisation for Economic Co-operation and Development

DSTI/CDEP/DGP(2022)8/FINAL

Unclassified

English - Or. English

13 June 2023

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INNOVATION
COMMITTEE ON DIGITAL ECONOMY POLICY

Working Party on Data Governance and Privacy in the Digital Economy

# OECD Privacy Guidelines Implementation Guidance: Foreword and Chapter on Accountability

JT03521782

# Foreword of the Implementation Guidance for the OECD Privacy Guidelines

1. The objective of this Implementation Guidance is to assist in the interpretation and application of the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (hereafter, the "Privacy Guidelines"), an integral part of the Recommendation concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data [OECD/LEGAL/0188] (hereafter the "Recommendation"). The Implementation Guidance aims to help policy makers, privacy enforcement authorities, public sector bodies and private sector organisations better understand and implement the Privacy Guidelines.
2. The Privacy Guidelines were adopted by the OECD Council in 1980 and amended in 2013. OECD Members and non-Members having adhered to the Recommendation (hereafter, "Adherents") are encouraged to implement the Privacy Guidelines in the pursuit of protecting the privacy and free flow of information.
3. Along with the adoption of the Privacy Guidelines in 1980, an Explanatory Memorandum was prepared as an information document to help in the interpretation and application of the Privacy Guidelines. The 1980 Explanatory Memorandum remains relevant to interpreting the aspects of the 1980 version of the Privacy Guidelines that remain unchanged. In addition, a supplementary Explanatory Memorandum was prepared when the Privacy Guidelines were amended in 2013 to provide the context and rationale for the revisions. It supplements but does not replace the 1980 Explanatory Memorandum.
4. This Implementation Guidance is not intended to vary the meaning of, or replace, the Privacy Guidelines, the original Explanatory Memorandum (1980) or the supplementary Explanatory Memorandum (2013). The explanatory memoranda and this Implementation Guidance are designed to complement each other and should be read and understood in conjunction.
5. In 2021, the Report on the Implementation of the OECD Recommendation concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data [C(2021)42] (hereafter, the "2021 Report") invited the OECD Committee on Digital Economy Policy (CDEP), through the Working Party on Data Governance and Privacy (WPDGP), to support further dissemination and implementation of the Privacy Guidelines, and to support Adherents in addressing the findings and challenges identified in the report, including addressing a proposal to develop additional guidance on the implementation of the Privacy Guidelines. This Implementation Guidance aims to focus on the issues identified in the 2021 Report on a chapter-by-chapter basis.
6. The development of the chapters of this Implementation Guidance has been led by the WPDGP and involved a multi-stakeholder process with OECD Members and partner countries and representatives from academia, business, and civil society. An informal advisory group of experts was composed to support the drafting of the chapters.

# Implementation Guidance for the OECD Privacy Guidelines: Chapter on Accountability

**Implementation Guidance for the OECD Privacy Guidelines**

**Chapter on Accountability**

## *Contents*

# 1. Introduction

## 1.1. Background

1. The **accountability principle** is one of the eight basic principles of national application[1] of the Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (hereafter the "Privacy Guidelines") set out in the Annex to the Recommendation concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data [OECD/LEGAL/0188]. The accountability principle provides that a data controller should be accountable for complying with measures which give effect to the rest of the principles.
2. Additionally, the Privacy Guidelines, as revised in 2013, introduced the concept of "**privacy management programmes**" to flesh out the elements required of data controllers to implement the accountability principle.
3. The 2021 Report on the Implementation of the OECD Recommendation concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data [C(2021)42] noted that the accountability principle remains an important pillar of the Privacy Guidelines, and that there is an opportunity to clarify its meaning and offer some further guidance on this important concept.
4. Specifically, the Report highlighted the need to clarify the following points in relation to the application of the accountability principle:
   a. The role of various actors (e.g., data controllers and their agents, top management of organisations, privacy officers, privacy enforcement authorities) and relevant tools (e.g., privacy risk assessments) related to accountability;
   b. How micro, small, and medium-sized enterprises can better implement the accountability principle; and
   c. The evolving concepts and practices concerning accountability (e.g., so-called Accountability 2.0, data ethics).

## 1.2. Objectives of this Chapter

5. This Chapter on accountability is intended to help policy makers, privacy enforcement authorities, public sector bodies and private sector organisations to better understand and implement the accountability principle of the Privacy Guidelines through privacy management programmes, by further clarifying some of the issues raised above. Although descriptions and examples in the Chapter are mainly of private sector organisations, they are also applicable to public sector bodies engaged in activities concerned with processing of personal data, as relevant.
6. For that purpose, the following sections of this Chapter will revisit the relevant parts of the Privacy Guidelines as well as the two explanatory memoranda accompanying the Privacy

[1] The other basic principles are: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, and individual participation.

Guidelines[2], and provide additional guidance on their interpretation and application, to understand what it means for an organisation to be truly accountable.

7. Specifically, the following sections will first look at the background of discussions on accountability (in Section 2.1), who should be accountable (in Section 2.2), elements of privacy management programmes (in Section 2.3), to whom accountability should be demonstrated (in Section 2.4), the role of privacy enforcement authorities (in Section 2.5), accountability for micro, small, and medium-sized enterprises and local public authorities (in Section 2.6), and accountability 2.0 as well as data ethics (in Section 2.7).

8. Such clarifications and guidance are aimed at enhancing the application of the accountability principle, and contributing to the effective implementation and dissemination of the Privacy Guidelines. The different aspects of accountability addressed in this Chapter should be considered both on their own and in their mutual interactions to ensure effective implementation.

## 2. Strengthening the implementation of the accountability principle

### 2.1. What is accountability?

9. Since the accountability principle was set forth in the Privacy Guidelines in 1980, the notion of accountability has been discussed by experts and addressed in laws and regulations of a host of countries, as well as in regional and international frameworks, as the processing of data pertaining to people has grown in complexity. For example, Canada adopted the Personal Information Protection and Electronic Documents Act in 2000, setting out ten "fair information principles", one of which is accountability. In 2005, the APEC Privacy Framework was modelled upon the Privacy Guidelines, including with respect to the principle of accountability. In 2009, an effort was initiated by an international group of experts from government, industry and academia to define the essential elements of accountability and consider how an accountability approach would work in practice (called the Galway Project).[3] The group reached consensus on the essential elements to guide organisational accountability.[4]

10. In 2013, the Privacy Guidelines were revised to introduce the concept of "privacy management programmes" to flesh out the elements to implement the accountability principle. In some jurisdictions, accountability is accompanied by liability, whereby an organisation could face legal consequences (e.g., sanctions) if it fails to comply with laws requiring accountability. For example, in 2016, the European Union adopted the General Data Protection Regulation (GDPR), which provided the tools for implementation and sanctions in case of non-compliance, also with the accountability principle. In addition, regulatory guidance regarding accountability has been developed across countries and

[2] The original Explanatory Memorandum to the OECD Privacy Guidelines (1980) and the supplementary Explanatory Memorandum to the revised Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (2013). See https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

[3] "Data Protection Accountability: The Essential Elements. A Document for Discussion October 2009", *Prepared by the Centre for Information Policy Leadership at Secretariat to the Galway Project*, https://www.ftc.gov/sites/default/files/documents/public_comments/privacy-roundtables-comment-project-no.p095416-544506-00059/544506-00059.pdf.

[4] Those are: (1) Organisation commitment to accountability and adoption of internal policies consistent with external criteria; (2) Mechanisms to put privacy policies into effect, including tools, training and education; (3) Systems for internal, ongoing oversight and assurance reviews and external verification; (4) Transparency and mechanisms for individual participation; and (5) Means for remediation and external enforcement.

jurisdictions, for example in Canada[5], Australia[6], Hong Kong (China)[7], Singapore[8], Colombia[9], the United Kingdom[10] and Japan.[11]

11. Although the Privacy Guidelines do not provide a definition of accountability[12], there have been global discussions in this regard. For instance:

- The report by the aforementioned Galway Project provided that "*[a]n organisation must demonstrate its willingness and capacity to be both responsible and answerable for its data practices*";
- The 2010 Opinion by the former Article 29 Data Protection Working Party (now the European Data Protection Board), which inspired the introduction of the principle of accountability in the GDPR, provided that *"[i]n general terms […] its emphasis is on showing how responsibility is exercised and making this verifiable*" and that "*[o]nly when responsibility is demonstrated as working effectively in practice can sufficient trust be developed*"[13]. Article 5(2) GDPR reflects this principle: "*The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')*".
- The guidance "Getting Accountability Right with a Privacy Management Program", developed by the Office of the Privacy Commissioner of Canada and their provincial counterparts, explains that "*[a]ccountability in relation to privacy is the acceptance of*

[5] Office of the Privacy Commissioner of Canada (2012), "Getting Accountability Right with a Privacy Management Program", https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-compliance-and-training-tools/gl_acc_201204/.

[6] Office of the Australian Information Commissioner (2015), "Privacy management framework: enabling compliance and encouraging good practice", https://www.oaic.gov.au/privacy/guidance-and-advice/privacy-management-framework-enabling-compliance-and-encouraging-good-practice.

[7] Privacy Commissioner for Personal Data, Hong Kong (2018), "Privacy Management Programme A Best Practice Guide", https://www.pcpd.org.hk//english/resources_centre/publications/files/PMP_guide_e.pdf.

[8] Personal Data Protection Commission, Singapore (Revised 2021), "Guide to Developing a Data Protection Management Programme", https://www.pdpc.gov.sg/help-and-resources/2019/07/guide-to-developing-a-data-protection-management-programme.

[9] Superintendencia de Industria y Comercio, "Guía para la implementación del Principio de Responsabilidad Demostrada (Accountability)", https://www.sic.gov.co/noticias/guia-para-la-implementacion-del-principio-de-responsabilidad-demostrada.

[10] Information Commissioner's Office, "Accountability Framework", https://ico.org.uk/for-organisations/accountability-framework/.

[11] Personal Information Protection Commission Japan (2021), "The Promotion of Privacy Impact Assessment", https://www.ppc.go.jp/files/pdf/pia_promotion.pdf (only available in Japanese) provides business operators with guidance on privacy impact assessments.

[12] The 1980 Explanatory Memorandum, accompanying the Privacy Guidelines, expanded on the accountability principle as follows: "*The data controller decides about data and data processing activities. It is for his benefit that the processing of data is carried out. Accordingly, it is essential that under domestic law accountability for complying with privacy protection rules and decisions should be placed on the data controller who should not be relieved of this obligation merely because the processing of data is carried out on his behalf by another party, such as a service bureau. On the other hand, nothing in the Guidelines prevents service bureaux personnel, "dependent users" […] and others from also being held accountable. For instance, sanctions against breaches of confidentiality obligations may be directed against all parties entrusted with the handling of personal information […]. Accountability […] refers to accountability supported by legal sanctions, as well as to accountability established by codes of conduct, for instance.*"

[13] Article 29 Data Protection Working Party (2010), "Opinion 3/2010 on the principle of accountability", https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf.

*responsibility for personal information protection*" and that "*[t]he outcome is a demonstrable capacity to comply, at a minimum, with applicable privacy laws*".

12. There is therefore a consensus that accountability comprises the taking of *responsibility* for personal data use and a means to *demonstrate* (or answer, verify, or make visible) this to other stakeholders. The taking of responsibility suggests leadership from top management and the cascading of responsibility throughout the organisation. In addition, ethical considerations regarding data are increasingly becoming a necessary part of accountability, particularly given that personal data use has become more complex, entailing impacts on a broad range of stakeholders. Finally, the concept of accountability encompasses the notion that the organisation is legally responsible for its data protection practices including before the judicial system.

13. This Chapter will explore the relationships between accountability and risks (see Section 2.3.3 below). It is important to recall, however, that the risk-based nature of accountability does not mean that the organisation does not need to comply with the basic principles of the Privacy Guidelines even where no risk is identified as a result of privacy risk assessments.

14. The accountability principle gives effect to, and allows the demonstration of compliance with, the (other) principles under the Privacy Guidelines. To that end, all of Part Three of the Privacy Guidelines, introduced in the 2013 revisions of the original Privacy Guidelines, is dedicated to the implementation of accountability through privacy management programmes. Appropriate privacy management programmes can address both responsibility and demonstrability, as discussed above.

15. Therefore, the purpose of accountability – and privacy management programmes – is to ensure compliance with all the data protection rules that give effect to the principles of the Privacy Guidelines. Accountable organisations demonstrate their responsibility in this regard through their privacy management programmes. However, a privacy management programme can do more than ensure and demonstrate that rules are followed; it can also ensure and demonstrate that data processing is legal, fair and just.

16. The rest of this Chapter will explore how an appropriate privacy management programme may be implemented, and the notions of Accountability 2.0 and data ethics to understand what it means for an organisation to be truly accountable.

## 2.2. Who should be accountable?

17. Paragraph 14 of the Privacy Guidelines explicitly provides that "[a] **data controller** should be accountable for complying with measures which give effect to the principles stated above".

18. According to the Privacy Guidelines and the 1980 Explanatory Memorandum,

    a. A data controller means *"a party who, according to national law, is competent to decide about the contents and use of data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf*";

    b. A data controller is "*a subject who, under domestic law, should carry ultimate responsibility for activities concerned with the processing of personal data*".

    c. A data controller *"may be a legal or natural person, public authority, agency or any other body*".

19. Based on these elements, the data controller is usually the public sector body or the private sector organisation itself, provided that it decides about the contents and use of data, and carries ultimate responsibility for activities related to the processing of personal data, and will thus be held accountable.

20. In a real-life setting, the organisation carries out activities related to the processing of personal data through different actors. These actors could be:

    - Top management of the organisation (e.g., CEO, members of the board);
    - Privacy officers, whose main objective is to advise on the activities related to processing of personal data;
    - A particular business unit or department within the organisation;
    - Employees of the organisation, who process personal data for a certain business need; and
    - Service providers who process personal data on behalf of the organisation.

21. There are complementary roles for these actors related to the processing of personal data, and they should enable the data controller to ensure greater compliance with the principles. Accountability can be achieved through a collective effort by all actors involved in the development and implementation of privacy management programmes (as will be outlined in Section 2.3 below). While the organisation as an entity is the data controller and hence legally accountable, it meets its obligations through the contributions of individual actors who play important roles and responsibilities in ensuring that personal data are protected.

22. Notably, various products and services developed with new technologies collect, store, process, and disseminate data. Developers that create products or services used for the processing of personal data are encouraged to aim for a design that helps organisations making use of such products or services to implement effective accountability (see also Section 2.3.3 below on "privacy by design" and Section 2.4.2 below on certification, seals and trustmarks).

## 2.3. Elements of a privacy management programme

23. A data controller should put in place a **privacy management programme** as set out in the Privacy Guidelines and in accordance with all applicable legal requirements. How an organisation implements and is prepared to demonstrate its privacy management programme is an essential element expected to give practical effect to the basic principles of the Privacy Guidelines. Privacy management programmes offer a means of demonstrating how organisations are accountable for data use.

24. Since the data controller is usually the organisation itself, a privacy management programme should concern all actors that are part of the organisation (see Section 2.2 above), and requires an appropriate governance structure and mechanisms concerning those actors. Paragraph 15 of the Privacy Guidelines provides the elements of privacy management programmes, to ensure such structure and mechanisms. The 2013 Supplementary Explanatory Memorandum provides further guidance in this regard. This Section revisits that guidance and complements it by elaborating on the elements of privacy management programmes.

### *2.3.1. Putting all personal data under control of the data controller*

Privacy Guidelines

15. A data controller should:
    a) Have in place a privacy management programme that:
        i. gives effect to these Guidelines for all personal data under its control;

2013 Supplementary Explanatory Memorandum

Paragraph 15(a)(i) specifies that a data controller's privacy management programme should give effect to the Guidelines "for all personal data under its control". The term "control" refers back to the definition of a "data controller", as defined in paragraph 1(a). This formulation emphasises that a privacy management programme should not only address the data controller's own operations, but all operations for which it may be accountable - regardless of to whom data is transferred. For example, a privacy management programme should include mechanisms to ensure that agents of the data controller maintain appropriate safeguards when processing personal data on its behalf. Safeguards may also be necessary in relationships with other data controllers, particularly where the responsibility for giving effect to the Guidelines is shared. Appropriate safeguards may include: provisions in contracts that address compliance with the data controller's privacy policies and practices; protocols for notifying the data controller in the event of a security breach; employee training and education; provisions for sub-contracting; and a process for conducting audits.

Paragraph 15(a)(i) refers only to the Guidelines as a source of rules or principles to be implemented through a privacy management programme. In practice, privacy management programmes may need to reflect other sources as well; including domestic law, international obligations, self-regulatory programmes, or contractual provisions.

25. The Privacy Guidelines provide that an organisation's privacy management programme should give effect to the Privacy Guidelines **for all personal data under its control** (paragraph 15(a)(i)). To that effect, the data controller should put in place a privacy management programme that could include:

    a. **Governance measures** concerning:

        i. **Internal oversight**: Putting in place a proper internal oversight structure is the first and most important step of a privacy management programme. Accountability should begin from top management to set the right direction, cascading down to the rest of the organisation (see Section 2.3.4 below);

        ii. **Organisational structure**: This concerns the allocation of responsibility for protecting personal data within the organisation and amongst the agents acting on behalf the organisation or other data controllers (see paragraph 29 below);

        iii. **Process controls**: This concerns having in place policies and procedures to ensure compliance with data protection rules giving effect to the Privacy Guidelines. For example, this could include plans for responding to inquiries or complaints, or plans for responding to incidents (see Section 2.3.5 below). Such policies and procedures should ensure that the organisation keeps appropriate records of its personal data processing operations, and should be reviewed and updated periodically (see Section 2.3.6 below);

        iv. **Defining roles and responsibilities, and training individual actors**: This concerns training and education of employees to foster awareness and a culture of accountability;

    b. **Technical measures**: These could include the development and deployment of privacy-respecting and privacy enhancing technologies (PETs), physical measures,

access control to data, and threat monitoring of unusual activities and responses to them. This relates to the security safeguards principle under the Privacy Guidelines.

26. The privacy management programme should be tailored to the structure, scale, volume and sensitivity of the organisation's operations (see Section 2.3.2 below). The organisation's policies and procedures should be articulated and made readily available to the public through, for example, privacy notices (in any format) to ensure transparency to stakeholders, including individuals. "Readily available" means that individuals should be able to obtain information without unreasonable effort as to time, previous knowledge, travel, any other administrative burden, and without unreasonable cost. Successful communications will enable individuals to understand the organisation's activities related to the processing of personal data. This will enhance the implementation of the openness principle and the individual participation principle under the Privacy Guidelines.

27. A data controller may delegate activities related to data processing to an external organisation (or multiple external organisations), who act on behalf of the data controller. Under the Privacy Guidelines, an agent acting on behalf of the data controller[14] could be understood as a party who is involved in activities related to the processing of personal data on behalf the data controller, but not legally competent to decide on its own about the contents and use of data. In some jurisdictions, this type of agent may be called a data processor[15], contractor (or sub-contractor, as the case may be), third-party service provider, or trustee. If such agents have taken on responsibility to decide about the contents and use of data, it means they are acting as a data controller.

28. In other cases, a data controller may share responsibility for giving effect to the Privacy Guidelines with other data controllers (e.g., in case of data sharing between different organisations in a joint project).

29. In any case, the 2013 Supplementary Explanatory Memorandum provides that a privacy management programme should address all operations regarding the processing of personal data, *regardless of to whom data is transferred*. To that effect, a privacy management programme should include mechanisms to ensure that agents of the data controller maintain appropriate safeguards when processing personal data on its behalf, and/or mechanisms to ensure appropriate safeguards in relation to other data controllers, particularly where the responsibility for giving effect to the Privacy Guidelines is shared. In the context of transborder data flows, it should be recalled that the data controller remains accountable for personal data under its control *without regard to the location of the data* (paragraph 16 of the Privacy Guidelines).

30. Such mechanisms could be implemented by way of contracts or other forms of agreements between the data controller and agents or other data controllers. Such contracts or agreements may include provisions on:

    a. Subject matter of the processing;

    b. Duration of the processing;

    c. Nature and purpose of the processing;

    d. Type of personal data involved;

    e. Categories of data subject;

[14] An agent may be a legal entity.

[15] See, for example, EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, para. 80.

f. Compliance with the data controller's privacy policies and practices, including maintaining appropriate safeguards for data protection;

g. Keeping records of data processing;

h. Protocols in the event of a data security breach, including notification to the data controller;

i. Requirements to support data subjects in exercising their rights;

j. Restriction of data processing for certain cases;

k. Obligations regarding sub-contracting;

l. A process for oversight including through monitoring, regular meetings and audits, and exit management, particularly for longer-term agreements.

31. It should be noted that the nature and extent of the relationship between the data controller and agents or other data controllers could change as the organisation's activities evolve. As such, a privacy management programme needs to be reviewed and updated to reflect such changes[16] (see Section 2.3.6 below).

### *2.3.2. Tailoring to the nature of the operations*

Privacy Guidelines

15. A data controller should:
    a) Have in place a privacy management programme that:
        ii. is tailored to the structure, scale, volume and sensitivity of its operations;

2013 Supplementary Explanatory Memorandum

Paragraph 15(a)(ii) underlines the need for flexibility when putting in place a privacy management programme. For example, large data controllers with locations in multiple jurisdictions may need to consider different internal oversight mechanisms than small or medium sized data controllers with a single establishment. At the same time, paragraph 15(a)(ii) also provides that privacy management programmes should be adapted to the volume and sensitivity of the controller's operations. Programmes for data controllers that deal with large volumes of personal data will need to be more comprehensive than those of data controllers who handle only limited amounts of personal data. The sensitivity of the data controller's operations may also impact the nature of a privacy management programme, as even a very small data controller may handle extremely sensitive personal data.

32. A privacy management programme should be **tailored to the structure, scale, volume and sensitivity** of the organisation's operations concerning personal data (paragraph 15(a)(ii)). As the 2013 Supplementary Explanatory Memorandum further provides, this underlines the need for flexibility when putting in place a privacy management programme.

33. The parameters to consider are as follows:

a. Structure of the operations. For example, the structure may be considered complex if the operations involve multiple locations and multiple agents or other data controllers, making the allocation of responsibilities complex;

[16] For example, Personal Data Protection Commission, Singapore (2020), "Guide to Managing Data Intermediaries", https://www.pdpc.gov.sg/help-and-resources/2020/09/guide-to-managing-data-intermediaries provides guidance on privacy management programmes specific to data processing outsourcing.

b. Scale of the operations. For example, the scale may be considered large if the operations involve a large number and frequency of envisaged data flows, and a long data retention period;

c. Volume of the operations. For example, the volume may be considered large if the operations involve a large number of individuals (data subjects) or a large quantity of data sets;

d. Sensitivity of the operations. For example, the level of sensitivity may be greater depending on the intended purposes, the methods of the processing and uses of the data, the type of data (including sensitive data), the type of data subjects (e.g., children and other groups of vulnerable persons), and the context in which the processing takes place.

34. These parameters need to be considered holistically as they may correlate with each other. For example, an organisation dealing with data that are limited in amount but extremely sensitive in content may need to have a more robust privacy management programme compared to other cases. This also applies to micro, small, and medium-sized enterprises (see Section 2.6 below).

35. Identifying the nature of the organisation's operations will also facilitate privacy risk assessments (see Section 2.3.3 below). In turn, privacy risk assessments with proper compliance can help organisations tailor their policies and practices.

### *2.3.3. Appropriate safeguards based on privacy risk assessments*

Privacy Guidelines

15. A data controller should:
    a) Have in place a privacy management programme that:
        iii. provides for appropriate safeguards based on privacy risk assessment;

2013 Supplementary Explanatory Memorandum

A recurring element in the discussions about privacy management programmes was the need for such programmes to develop appropriate safeguards based on privacy risk assessment. Paragraph 15(a)(iii) contemplates that the determination of the necessary safeguards should be made through a process of identifying, analysing and evaluating the risks to individuals' privacy. This process is sometimes accomplished by conducting a "privacy impact assessment" before a new programme or service is introduced or where the context of the data use changes significantly. "Risk" is intended to be a broad concept, taking into account a wide range of possible harms to individuals. A privacy management programme can also assist in the practical implementation of concepts such as "privacy by design", whereby technologies, processes, and practices to protect privacy are built into system architectures, rather than added on later as an afterthought.

36. A privacy management programme should provide for appropriate safeguards of personal data based on **privacy risk assessments**. Privacy management programmes need to be based on, and developed around, prioritisation of risks, even though data controllers must comply with all principles (collection limitation, data quality, etc.), independently of the risk assessments.

37. First, organisations need to consider the nature, scope, context and purposes of the processing of personal data (see also paragraph 85 below on elements to consider, which concerns micro, small, and medium-sized enterprises, but is relevant for all organisations),

and the magnitude of risks that certain operations related to personal data processing pose for individuals and society. They also need to balance such risks with the benefits that such operations can deliver. Second, organisations need to consider the likelihood of the identified risk occurring, and adopt reasonable measures to avoid or minimise risks that are likely to occur. Privacy risk assessments allow organisations to calibrate their privacy management programmes.

38. Certain kinds of operations of the organisation trigger the need for privacy risk assessments (see Section 2.3.2 above) for their potential impact on individuals and their rights, particularly for vulnerable populations. For instance, organisations should perform privacy risk assessments when introducing new technologies, processes or systems, when making significant changes to existing processes or systems, and when new laws are enacted. Furthermore, periodic reviews should be in place to ensure that privacy risk assessments are up to date.

39. Effective privacy risk assessments will enable the organisation to put in place appropriate safeguards to protect personal data. As the 2013 Supplementary Explanatory Memorandum notes, the determination of the necessary safeguards should be made through a process of identifying, analysing and evaluating the risks to individuals' privacy.

40. As the Supplementary Explanatory Memorandum notes, "risk" is intended to be a broad concept, taking into account a wide range of possible adverse outcomes to individuals. Recent developments of digital technologies may entail a variety of risks to individuals (data subjects) and to society. As an illustration, privacy risks associated with the organisation's operations could include:

    a. financial loss or economic harm, direct or indirect, through, for instance, sanctions or fines;

    b. physical harm;

    c. psychological harm;

    d. inconvenience or expenditure of time;

    e. a negative outcome or decision with respect to an individual's eligibility for a right, privilege, or benefit;

    f. stigmatisation or reputational injury;

    g. disruption and intrusion from unwanted commercial communications or contacts;

    h. psychological manipulation made possible by the handling of massive amounts of data;

    i. discrimination; and

    j. any other detrimental or negative consequences that affect an individual's private life and privacy.

41. Adverse outcomes to individuals could result in business risks for the organisation. To manage such risks for the organisation, the concept of risk management, which is being applied and implemented in various areas, could be likewise applicable here. According to the relevant ISO standard, for example, a risk management framework is described to encompass "*integrating, designing, implementing, evaluating and improving risk*

*management across the organisation*."[17] Box 1 describes the fundamental components of a general risk management cycle.

**Box 1 Risk management cycle components**

1. **Establishing the objectives and the context**. One cannot determine the acceptable risk level in the abstract. It is always contextual. Therefore, the first step is to understand the mission of the organisation, its economic and social objectives, the benefits it is aiming to realise, and its values. It also requires examining the broader context including society's values, laws, regulations and culture, identifying stakeholders and their concerns and other internal and external factors that define what a successful achievement of the objectives means.

2. **Assessing the risk**. This analytical step consists of three distinct tasks:

    a. Identifying risk factors: intentional and unintentional threats (such as a criminal attracted by a company's asset), vulnerabilities (weaknesses such as keys left under the doormat or lack of employee training) and possible events (e.g. incidents such as an intrusion by a thief).

    b. Analysing the risk factors. This involves taking into account the likelihood or probability that an event will occur. It can be described qualitatively – e.g. low, medium or high – or using a numeric value.

    c. Evaluating the risk (impact). This phase involves assessing the severity or magnitude of the estimated consequences of uncertainty on the organisation's objectives defined in stage 1. The impact can be tangible (e.g. money loss, physical harm) or intangible (e.g. reputation).

3. **Treating the risk**. This decision making step aims to determine the most appropriate way to address the risk in order to achieve the anticipated objectives and benefits. This involves one or more of the following:

    a. Accepting the risk.

    b. Reducing the risk to an acceptable level. Risk can be reduced through security measures generally involving people (e.g. training), processes (e.g. legal, organisational, etc.) and technologies (e.g. keys, locks, fences, etc.). Since risk cannot be completely eliminated, the persistence of some residual risk means that undesirable events can occur despite the presence of security measures. Therefore organisations also need to be ready to deal with undesirable events through measures that reduce the impact of incidents when they happen (preparedness measures) to ensure resilience and continuity. Finally, organisations can also use innovation to reduce risk, i.e. designing the activity differently, including its business model and organisational aspects, to reduce its risk exposure.

    c. Sharing the risk or transferring it to another party (e.g. through insurance).

    d. Avoiding the risk by not carrying out the activity and thus forgoing the potential benefits.

[17] ISO (2018), "ISO 31000:2018 Risk management - Guidelines", https://www.iso.org/standard/65694.html.

The choice of risk treatment depends on several factors including the organisation's tolerance of risk, also called "risk appetite".

4. **Ongoing monitoring and review cycle**. Since the environment is constantly changing, a cycle has to be created to ensure that the risk is continuously managed. This includes returning to step 1 and examining, for example, changes in the context (e.g. objectives, market, expected benefits) and the risk level (threats, vulnerabilities, likelihood, possible impact), effectiveness of the risk treatment measures, and accuracy of the risk assessment.

Source: OECD (2016), "Managing Digital Security and Privacy Risk", *OECD Digital Economy Papers*, No. 254, OECD Publishing, Paris, https://doi.org/10.1787/5jlwt49ccklt-en.

42. Although not identical[18], this general risk management cycle resonates with the concept of privacy management programmes in many respects. Specifically in the context of privacy management programmes, the above components of the risk management cycle may be applied as follows:

    a. **Establishing the objectives and the context** relates to applying the basic principles of the Privacy Guidelines (e.g., collection limitation principle, data quality principle, purpose specification principle, use limitation principle) as well as taking into consideration the other rights and interests of individuals potentially impacted, when the data controller decides about the purpose it is pursuing, the necessity and proportionality of processing personal data and the amount and type of data (see also paragraph 85 below on elements to consider, which concerns micro, small, and medium-sized enterprises, but is also relevant for all organisations);

    b. **Assessing the risk** relates to identifying the risks and their impact as illustrated in paragraph 40 above, as well as assessing them against the potential benefits. The assessment should cover risks associated with activities not only by the data controller but also by its agents or employees (see Section 2.3.1 above);

    c. **Treating the risk** concerns establishing appropriate safeguards against the foreseen risks. This may include the implementation of concepts such as "privacy by design", whereby technologies, processes, and practices to protect privacy are built into system architectures, rather than added on later as an afterthought, as the 2013 Supplementary Explanatory Memorandum notes. With particular regard to risk reduction, this may also take the form of a reduction of the scope, extent, and retention period of the intended data processing activity, or of data minimisation;

    d. **Ongoing monitoring and review cycle** concerns monitoring and periodic assessment as discussed in Section 2.3.6 below.

43. To implement this risk management cycle, organisations should, under the leadership of top management, clearly define who is (are) assessing the risk, who is (are) responsible for treating the risk and who is (are) monitoring and reviewing the cycle (see also Section 2.3.6 below).

44. This risk-based approach of privacy management programmes will enhance the organisation's governance of personal data. Risk assessments can help organisations comply more effectively by adjusting their privacy management programme to reflect evolving risks and changes in the environment. The risk-based approach of privacy

[18] For example, the sharing or transfer of risk mentioned in Box 1 will not be appropriate for risks involving personal data, because the responsibility for data controllers to comply with data protection principles cannot be shared with, or transferred to, someone else.

management programmes can address emerging technologies, particularly in building responsible and ethical practices into privacy management programmes.

45. In addition, the risk-based approach of privacy management programmes may reduce the costs borne by the organisation by, for example, reducing the burden arising from excessive notifications for minor data security breaches, as the 2013 Supplementary Explanatory Memorandum notes. Finally, risk assessments can improve overall governance and strengthen trust on the part of customers and other stakeholders.

### *2.3.4. Governance structure and internal oversight mechanisms*

Privacy Guidelines

15. A data controller should:
    a) Have in place a privacy management programme that:
        iv. is integrated into its governance structure and establishes internal oversight mechanisms;

2013 Supplementary Explanatory Memorandum

Paragraph 15(a)(iv) indicates that privacy management programmes should be integrated in the governance structure of a data controller and establish appropriate internal oversight mechanisms. Obtaining support and commitment from senior management is a key factor in ensuring the successful implementation of a privacy management programme. Ensuring the availability of sufficient resources and staff, as well as training programmes, may also improve the effectiveness of the programme. Privacy officers may play an important role in designing and implementing a privacy management programme.

46. A privacy management programme should be integrated into the organisation's governance structure and establish appropriate internal oversight mechanisms.

47. Top management and privacy officer(s) of the organisation play a critical role to ensure that the organisation's privacy management programme is effective, as explained in Sections 2.3.4.1 and 2.3.4.2 below respectively. Any agent acting on behalf the organisation may also need to ensure that its governance structure allows it to demonstrate its compliance to the data controller (see Section 2.3.1 above).

48. Integrating data protection into corporate frameworks, such as incorporating privacy risk management (see 2.3.3 above) into the enterprise risk management framework, can assure senior management commitment and attention. This ensures that data protection concerns and risks are governed and managed holistically by the organisation.

#### *2.3.4.1. Role of top management*

49. Top management (e.g., for large organisations, this would be the CEO or the board; for smaller/medium-sized organisations, this would be senior management staff; for administrative bodies, this would be the corresponding senior officers) plays a critical role to ensure that the organisation's privacy management programme is effective.

50. Top management should consider the different objectives, rights, interests, and benefits at stake, and address their potential misalignment through its governance structure. For example, for privacy risk, the range of consequences of a data security breach can be very different for the organisation as compared to the data subject (affected individual): the organisation may face sanctions for data mismanagement while the data subject may suffer

personal consequences. If their interests are misaligned, organisations may have an incentive to underestimate privacy risk.

51. Top management should ensure that the organisation's privacy management programme is responsive and agile in adapting to changes in the environment, through its governance structure. It needs to ensure its operations are within the range in which the organisation can afford to mitigate the privacy risks identified in the privacy risk assessment, respond to the consequences of an incident, such as loss of consumer trust, damage to reputation, negative impacts on revenue, as well as costs to implement measures to prevent recurrence, and thereby ensure the sustainability of business. If the organisation cannot afford them, top management should reconsider its activities.

52. Furthermore, top management should ensure commitment including sufficient investment and resourcing across the organisation for an effective privacy management programme, explicit support for the privacy officer and staff (including employee education and training), and privacy accountability for functional executives or the corresponding administrative staff. For example, top management may consider appointing a sponsor from the board or top management, and establishing a direct line of reporting from that individual to the board or top management.

53. It is important for top management to have an appropriate corporate governance structure that enables the organisation to achieve these objectives, for example, by having functions within the organisation that can:

    a. **Direct** the privacy management programme in terms of corporate/administrative strategy by:

        i. integrating privacy risk assessments (or risk management) as part of the decision-making process of the organisation (see Section 2.3.3 above);

        ii. assigning the responsibility for the privacy management programme, for example to (one or more) independent members of the board or administrative hierarchy;

    b. **Monitor** the performance of the privacy management programme by:

        i. appointing and engaging with a privacy officer (see Section 2.3.4.2 below);

        ii. ensuring adequate resources and funding;

        iii. introducing mechanisms for whistle-blower protection;

    c. **Evaluate** the results of the privacy management programme by:

        i. having the internal audit cover the privacy management programme (see Section 2.3.6 below);

        ii. having the external audit cover the privacy management programme (see Section 2.3.6 below);

    d. **Update** the privacy management programme as needed based on the aforementioned evaluation (see Section 2.3.6 below);

    e. **Communicate** to stakeholders.

#### *2.3.4.2. Role of privacy officers*

54. The privacy officer plays a critical role to ensure that the organisation's privacy management programme is effective for the organisation to be accountable. The privacy

officer should be appointed from top management of the organisation or have a direct reporting line to top management. The organisation should ensure the resources, authority and independence of the privacy officer necessary to perform their tasks. This is particularly important when the organisation's operations involve a high degree of privacy risks.

55. The role of the privacy officer may, for example, include:

a. Advising the organisation and other actors involved (e.g., the data controller's agents, top management, employees) on solutions that achieve the intended objectives in a way that is respectful of privacy;

b. Monitoring the organisation's compliance with regulations concerning privacy, and report thereon;

c. Monitoring the related actors' compliance with the data protection policies and practices of the data controller;

d. Advising on and monitoring the effectiveness of the privacy risk assessment;

e. Advising on ethical use and management of data by the organisation;

f. Advising senior leadership on privacy trends;

g. Advising on the implementation of privacy by design;

h. Advising the organisation to ensure that data maps and inventories are maintained;

i. Supporting the negotiation and performance of complex contracts with regard to personal data processing;

j. Overseeing or managing privacy inquiries or access requests from data subjects;

k. Supporting training of employees who are involved in activities concerned with personal data processing; and

l. Engaging with privacy enforcement authorities (see Section 2.5 below), particularly in case of data security breaches or violations of privacy laws.

### *2.3.5. Plans for responding to incidents and plans for responding to inquiries*

Privacy Guidelines

15. A data controller should:
    a) Have in place a privacy management programme that:
        v. includes plans for responding to inquiries and incidents;

2013 Supplementary Explanatory Memorandum

Paragraph 15(a)(v) provides that a privacy management programme should also include plans for responding to incidents and inquiries. The increasing frequency of security breaches affecting personal data demonstrates the importance of developing an incident response plan, which includes breach notification (see below). To support the "Individual Participation Principle" in Part Two, data controllers should also be able to provide timely response to inquiries (either in the form of complaints or requests for information) by data subjects.

56. A privacy management programme should include **plans for responding to incidents and plans for responding to inquiries**, including those related to activities by the agents of the

data controller. A proper management of responses to inquiries and to incidents will ensure that data subjects' rights are respected.

57. Plans for responding to inquiries by data subjects can be in the form of complaints or requests for information, or inquiries that may be received outside the context of an incident. Such plans may include internal policies that specify:

    a. A dedicated person or team to manage inquiries;

    b. Procedures to ensure timely handling of inquiries by data subjects;

    c. Reporting structures and procedures within the organisation.

58. Plans for responding to incidents (e.g., data security breaches affecting personal data) may include internal policies that specify:

    a. A dedicated person or team to manage incidents;

    b. Procedures to ensure timely management of incidents, consistently with the cybersecurity plans of the organisation;

    c. Methods for identifying incidents and notifying the responsible employees within the organisation;

    d. Notification to data subjects (see Section 2.3.7 below);

    e. Notification to privacy enforcement authorities (see Section 2.3.7 below);

    f. Training of employees; and

    g. Remedies for affected data subjects: recovery of services and management of relationships with affected data subjects.

59. As noted in Section 2.3.1 above, the organisation's policies and procedures, including plans for responding to inquiries and plans for responding to incidents, should be clearly articulated and made readily available to the public to ensure transparency. This will help individuals exercise their rights, and enhance the implementation of the other principles under the Privacy Guidelines, especially openness and individual participation.

### *2.3.6. Monitoring and periodic assessment*

Privacy Guidelines

15. A data controller should:
    a) Have in place a privacy management programme that:
        vi. is updated in light of ongoing monitoring and periodic assessment;

2013 Supplementary Explanatory Memorandum

Finally, paragraph 15(a)(vi) stipulates that privacy management programmes should be routinely reviewed and updated to ensure that they remain appropriate to the current risk environment.

60. A privacy management programme should be **routinely reviewed and updated**. An outcome-based privacy management programme will ensure that the data controller takes appropriate measures to give effect to the Privacy Guidelines, and adjust to changes in the environment. Thus, a privacy management programme should also be reviewed and updated when there are significant changes in the environment, such as changes in legal or regulatory requirements, organisational changes or changes in outsourcing arrangements.

61. Organisations may leverage their audit arrangements. If the organisation has an internal audit mechanism, the scope of such internal audit should cover the privacy management programme. The internal audit should periodically validate the organisation's compliance with data protection policies and procedures, and test whether its privacy management programme remains effective. The organisation may also utilise an external audit in this regard. Such audits should cover activities not only by the data controller but also by its agents (see Section 2.3.1 above).

62. Monitoring and assessment through certification schemes are also relevant (see Section 2.4.2 below). The process of certification and re-certification helps to ensure that privacy management programmes are updated, and also reviewed by an external auditor.

63. When the internal and/or external audit or certification scheme finds the existing privacy management programme ineffective, the data controller should revise its privacy management programme and make it effective, including through training and education for employees.

### *2.3.7. Data security breach notification*

Privacy Guidelines

15. A data controller should:

> c) Provide notice, as appropriate, to privacy enforcement authorities or other relevant authorities where there has been a significant security breach affecting personal data. Where the breach is likely to adversely affect data subjects, a data controller should notify affected data subjects.

2013 Supplementary Explanatory Memorandum

The "Security Safeguards Principle" of Part Two states that "Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data." Numerous high-profile data breaches have demonstrated that personal data security continues to be a challenge.

Data breaches can result, for example, from actions by careless employees who fail to follow proper procedures; hackers who gain access to inadequately protected databases; or opportunistic thieves who steal unsecured portable devices. However, the underlying causes – lack of employee training and awareness, out-of-date security safeguards, inadequate rules governing access to personal data, over-collection of data and undefined retention periods, or a lack of adequate oversight – can often be attributed to the data controller.

The potential harm to individuals from the misuse of their personal data, whether accidentally lost or purposefully stolen, may be significant. Organisations experiencing a breach often incur significant costs responding to it, determining its cause, and implementing measures to prevent recurrence. The reputational impact can also be significant. A loss of trust or confidence can have serious consequences for organisations. As a result, the security of personal data has become an issue of great concern to governments, businesses and individuals.

Breach notification laws requiring data controllers to inform individuals and/or authorities when a security breach has occurred have been passed or proposed in many countries. These laws are usually justified on the grounds that data controllers have little incentive to disclose breaches voluntarily, given the possible harm this can cause to their reputation. Requiring notification may enable individuals to take measures to protect themselves against the consequences of identity theft or other harms. Notification requirements may also provide privacy enforcement authorities or other authorities with information to determine whether to

investigate the incident or take other action. Ideally, breach notification laws also help to create an incentive for data controllers to adopt appropriate security safeguards for the personal data they hold.

In addition to contributing to data security, data breach notification enhances other basic principles set forth in Part Two of the Guidelines, including accountability, individual participation and openness. Furthermore, mandatory security breach notification may improve the evidence base for privacy and information security policies by generating information about the number, severity and causes of security breaches.

Security breaches not only raise privacy concerns, but also intersect with other issues, including criminal law enforcement and cybersecurity. When an organisation suffers a security breach, particularly one resulting from an external attack, notification of the breach to authorities other than privacy enforcement authorities (e.g. computer incident response teams, criminal law enforcement entities, other entities responsible for cybersecurity oversight) may be appropriate or required.

Requiring notification for every data security breach, no matter how minor, may impose an undue burden on data controllers and enforcement authorities, for limited corresponding benefit. Additionally, excessive notification to data subjects may cause them to disregard notices. Accordingly, the new provision that has been added to the Guidelines [paragraph 15(c)] reflects a risk-based approach to notification. Notice to an authority is called for where there is a "significant security breach affecting personal data", a concept intended to capture a breach that puts privacy and individual liberties at risk. Where such a breach is also likely to adversely affect individuals, notification to individuals would be appropriate as well. To determine whether individuals are likely to be "adversely affected" by a breach, the term "adverse effect" should be interpreted broadly to include factors other than just financial loss. Notification requirements should be flexible to allow for prevention and mitigation of further damage. There may be circumstances where notification to data subjects would be inappropriate, for example when it would increase the risk to data subjects or impede a law enforcement investigation.

Existing breach notification laws differ in terms of the thresholds for notification, the parties to be notified, the timing of the notification, as well as the role of privacy enforcement and other authorities. Further experience may be needed to determine which modalities of breach notification are most effective in practice.

Security breaches may affect the personal data of individuals residing in different jurisdictions. When designing, implementing or revising breach notification requirements, special consideration may be given to the interests of affected individuals who may live outside their jurisdiction. In particular, the notification of privacy enforcement authorities in other jurisdictions where a significant number of individuals are known or likely to have been affected, can be beneficial. Cross-border enforcement cooperation mechanisms are one way to foster arrangements that might support or disseminate breach notifications of importance to multiple jurisdictions. Such arrangements may also help to address issues arising from conflicting legal requirements.

64. The data controller should **provide notice**, as appropriate**, to privacy enforcement authorities or other relevant authorities** where there has been a significant data security breach affecting personal data. Where the breach is likely to adversely affect data subjects, a data controller should **notify affected data subjects** (paragraph 15(c)).

65. Data security breach notification is part of plans for responding to incidents (see Section 2.3.5 above), and therefore part of a privacy management programme. Data security breach notification enhances the accountability principle as well as other basic principles set forth in the Privacy Guidelines, as the 2013 Supplementary Explanatory Memorandum explains. Data security breach notifications will enable stakeholders to be aware of the breach and take measures to mitigate possible adverse impacts caused by the breach. In particular, notifications to data subjects are meant to alert them of specific risks that they are exposed to, and should therefore contain clear instructions on what they can do to protect themselves.

66. In order to meet data security breach notification requirements, organisations should put in place internal monitoring and escalation processes for data assets that have been identified to be at higher risk.

67. The data controller should notify privacy enforcement authorities or other authorities (e.g., criminal law enforcement authorities), where there is a significant data security breach affecting personal data, and notify individuals where such a breach is also likely to adversely affect them. To determine whether individuals are likely to be "adversely affected" by a data security breach, the process of privacy risk assessment is relevant (see Section 2.3.3 above).

68. As the 2013 Supplementary Explanatory Memorandum notes, existing data security breach notification frameworks could differ across jurisdictions in terms of the thresholds for notification, the parties to be notified, the timing of the notification, as well as the role of privacy enforcement and other authorities. According to the 2021 OECD Report on the implementation of the Privacy Guidelines, there is a general trend toward mandatory data security breach notification, including specific requirements for data subject notification. Thresholds to notify the authority are generally risk-based but vary among jurisdictions and sectors. Where timeframes for notification are prescribed, it is common to specify a time window (e.g., no later than 72 hours) or to require notifying "quickly or as soon as possible without unreasonable delay".[19] The data controller should consider the frameworks of the jurisdiction(s) in which it operates and take appropriate measures, with special consideration to the interests of affected individuals who may be located in other jurisdictions. In particular, the notification to privacy enforcement authorities in other jurisdictions can be beneficial where a significant number of individuals are known or likely to have been affected there.

## 2.4. To whom should accountability be demonstrated?

### *2.4.1. Demonstrating the privacy management programme*

Privacy Guidelines

15. A data controller should:

> b) Be prepared to demonstrate its privacy management programme as appropriate, in particular at the request of a competent privacy enforcement authority or another entity responsible for promoting adherence to a code of conduct or similar arrangement giving binding effect to these Guidelines;

2013 Supplementary Explanatory Memorandum

Paragraph 15(b) provides that a data controller should be prepared to demonstrate its privacy management programme as appropriate, in particular at the request of a competent privacy enforcement authority or another entity responsible for promoting adherence to a code of conduct or similar arrangement giving binding effect to these Guidelines. Establishing the capacity and effectiveness of a privacy management programme, even in the absence of a personal data security breach or allegation of non-compliance, enhances the accountability of data controllers. The assessment of the programme may be carried out directly by the privacy enforcement authority or by an agent on its behalf.

[19] OECD (2021), "Promoting comparability in personal data breach notification reporting", *OECD Digital Economy Papers*, No. 322, OECD Publishing, Paris, https://doi.org/10.1787/88f79eb0-en.

Paragraph 15(b) includes the terms "appropriate" and "competent" to highlight that data controllers should be prepared to demonstrate their privacy management programmes at the request of a privacy enforcement authority provided that this authority has jurisdiction over the data controller. The Guidelines do not address legal issues related to jurisdiction, competence and conflicts of law.

A privacy management programme may also be demonstrated to an entity which is responsible for promoting adherence to a code of conduct or similar arrangement giving binding effect to Guidelines. Such arrangements may involve seal programmes or certification schemes, and may also concern transborder flows of personal data. In this regard it can be noted that paragraph 21 encourages the development of international arrangements that give practical effect to the Guidelines. The European Union's Binding Corporate Rules (BCRs) and the APEC Cross-border Privacy Rules System provide two models for developing such an arrangement.

69. The data controller should be prepared to **demonstrate its privacy management programme** as appropriate, in particular at the request of a competent privacy enforcement authority (see Section 2.5 below) or another entity responsible for promoting adherence to a code of conduct or similar arrangement (such as certification schemes) giving binding effect to the Privacy Guidelines (see Section 2.4.2 below) (paragraph 15(b)).

70. Accountability can be demonstrated through robust privacy management programmes. As the 2013 Supplementary Explanatory Memorandum provides, establishing the capacity and effectiveness of a privacy management programme, even in the absence of a data security breach or allegation of non-compliance, enhances the accountability of data controllers.

71. Accountability is not only crucial from a compliance perspective but has also positive implications from a business and societal perspective so as to increase transparency and trust. Thus, the data controller should be prepared to demonstrate its privacy management programme not only to privacy enforcement authorities, but to a broad range of stakeholders including bodies responsible for promoting adherence to a code of conduct or certification schemes, shareholders, investors, and participants in a supply chain.

72. All stakeholders, such as privacy enforcement authorities, civil society, and individuals, have an interest in how organisations implement accountability, as the accountability principle gives effect to the other privacy principles and ultimately benefits privacy and individual liberties.

### *2.4.2. Role of organisational codes of conduct and certification schemes*

73. Mechanisms involving the private sector and that are legally binding and often voluntary, such as codes of conduct, certification schemes and binding corporate rules, also play a key role in demonstrating compliance with data protection obligations and thus the organisation's accountability to privacy enforcement authorities and stakeholders including shareholders, investors, and participants in a supply chain.[20]

74. **Codes of conduct** ("codes") are instruments adopted by organisations to help them fulfil data protection obligations. Codes can be drawn up by the organisation itself, representative bodies such as industry associations, business federations, governments or privacy enforcement authorities, typically in consultation or collaboration with interested

[20] This could include mechanisms for specific business areas. For example, in Japan, private organisations accredited by the Personal Information Protection Commission pursuant to the Act on the Protection of Personal Information set self-regulations and handle complaints in particular business areas. See https://www.ppc.go.jp/en/aboutus/roles/accredited_org/.

stakeholders. Codes sometimes require approval by an authority. The entity in charge reviews any applicant seeking membership and ensures compliance with the codes by the adhering organisations. These codes can be cross-sectoral, tailored to specific sectors, or tailored to the specific needs of the organisation itself.

75. **Certification** schemes and **seal/trustmark** programmes offer similar mechanisms that data controllers and processors can adhere to in order to demonstrate their compliance with data protection obligations. They often involve private certification bodies accredited by authorities.[21] A certification body issues a certification to an organisation (or its services/products), if it considers the organisation meets certain criteria set out by the certification body or authority, and can act in case of non-compliance. This may include international certifications. Certifications, seals and trustmarks may give data subjects and business partners trust in the level of data protection of the products and services they use. They may also include consultations between certification bodies/authorities and data controllers during and after the process of certification, which can improve privacy practices. Furthermore, they may help demonstrate compliance to the privacy enforcement authority.

76. With regard to data protection policies for cross-border transfers of personal data within a group of undertakings or enterprises, organisations can adhere to **binding corporate rules** ("BCRs"), sometimes referred to as intra-group rules. They can be particularly beneficial for companies that need to transfer data globally within their own group, including multinational corporate groups, groups of undertakings or a group of enterprises engaged in a joint economic activity such as franchises, joint ventures or professional partnerships. BCRs are often standardised, establishing uniform binding rules applicable to all relevant entities across the group, so that adequate protection can be ensured for data transferred across borders and for compliance with local law. BCRs sometimes require approval by a privacy enforcement authority.

77. As foreseen in the 2013 Supplementary Explanatory Memorandum, international arrangements that give practical effect to the Privacy Guidelines can be an important tool to strengthen accountability for transborder flows of personal data.

## 2.5. Role of privacy enforcement authorities

78. Regulation and effective enforcement enhance organisational accountability, and privacy enforcement authorities are crucial in this regard. As the 2013 Supplementary Explanatory Memorandum notes, with strong and predictable regulation and enforcement in place, a pivotal role may be played by mandatory data security breach notifications to privacy enforcement authorities, and by corrective actions, sanctions and fines imposed by them in case of violations of privacy rules, including those directed at the individuals concerned. Such actions by privacy enforcement authorities can highlight the financial, legal and reputational risks for organisations, and help ensure that privacy risk is given the same weight and importance as other categories of risk.

[21] Those schemes and programmes have been sometimes developed and operated by the private sector (as non-binding instruments) to enhance trust from the side of consumers and business partners. For example, Japan's PrivacyMark, administered by JIPDEC (a private promotion body) since 1998, assesses whether private organisations take appropriate data protection measures in accordance with JIS Q 15001 (a Japanese industrial standard concerning personal information protection management systems), which is aligned with international standards such as the OECD Privacy Guidelines. Certified organisations are granted the right to display "PrivacyMark" in their business activities. See https://privacymark.org/.

79. Privacy enforcement authorities may directly assess the effectiveness of the privacy management programme of organisations, as the 2013 Supplementary Explanatory Memorandum provides. Privacy enforcement authorities may assess the relevant aspects of the privacy management programme, for example:

    a. Scope and scale (e.g., whether it covers all personal data; whether it is tailored to the nature of the operations);

    b. Effectiveness of privacy risk assessment or risk management (e.g., whether it recognises and treats the privacy risks appropriately);

    c. Appropriateness of the protection (e.g., whether the policies in place are appropriate for the identified privacy risks);

    d. Governance (e.g., whether it is appropriately integrated into the governance structure; whether the governance is functioning to correct the potential misalignment of interests);

    e. Response to problems such as data security breaches and complaints (e.g., timeliness, existence and effectiveness of remedies).

80. In addition, privacy enforcement authorities can provide useful guidance for organisations on the implementation of the accountability principle and privacy management programmes, and set expectations for enforcement. They may regularly engage with organisations, accompany data controllers and deliver opinions or provide guidance on their compliance. This may secure top management's commitment, enhance compliance by organisations and lead to a reduction in full investigations. Privacy enforcement authorities may also consider incentives, as relevant and if available, for effective implementation of accountability by an organisation, and take accountable practices into account as mitigating factors or as grounds to offer voluntary undertakings. The latter may consist of accountability measures imposed on organisations, e.g., third-party assessments or specific governance structures around privacy accountability. Furthermore, privacy enforcement authorities can engage with organisations through regulatory sandboxes or private-public partnerships to encourage good practices for data protection. Policymakers should also consider appropriate legislation to support privacy management programmes[22] and strengthen the privacy enforcement authorities' role in their promotion.

81. To further promote accountability, in particular with respect to data security breaches or any privacy contraventions that occur across borders, privacy enforcement authorities can cooperate on such cases, and on wider technical issues related to regulation and enforcement. A framework for cooperation between privacy enforcement authorities can be established through agreements, such as Memorandums of Understanding (MoUs).

## 2.6. Accountability for micro, small, and medium-sized enterprises and local public authorities

82. Supporting micro, small, and medium-sized enterprises (MSMEs) in the use of personal data for their business is critical, as these enterprises are a vital component of the economic

[22] For example, the policy guidance "Fundamental principles on public policies related to appropriate handling of personal information", issued by the Personal Information Protection Commission Japan (https://www.ppc.go.jp/files/pdf/220525_shiryou-1.pdf, only available in Japanese), sets out principles applicable to public policies that involve handling of personal information by administrative authorities and the private sector concerned, to ensure accountability when implementing such public policies.

structure of many countries. Likewise, assisting all, but especially local public authorities in this regard is crucial, as they often have the most day-to-day interactions with data subjects. This section is applicable to them, as relevant.

83. MSMEs may face challenges, including a lack of awareness and capacity to develop and implement a privacy management programme. MSMEs may not be equipped with the necessary resources and understanding in this respect. This necessitates further guidelines from privacy enforcement authorities, for example to appropriately define risks and adverse outcomes to individuals. In this respect, efforts have been made by countries to provide guidance for MSMEs.[23]

84. Privacy management programmes, as described in the Privacy Guidelines, are scalable and designed to help any type of organisations, whether large or small. A privacy management programme should be tailored to the nature of the organisation's operations (see Section 2.3.2 above). The risk-based feature of privacy management programmes will enable MSMEs to implement appropriate safeguards, proportionate to the nature of their business. Model privacy management programmes for MSMEs may also be developed by privacy enforcement authorities, other government agencies or trade associations to make them specific to an industry.

85. A possible path for MSMEs to apply privacy management programmes is sketched below. It elaborates on elements of privacy risk assessments (or risk management) possibly relevant to MSMEs. Nonetheless, it is important to acknowledge that there is no one-size-fits-all approach.

    a. MSMEs (particularly top management) could first focus on understanding the objectives and the context of the use of personal data. This involves considering the basic principles of the Privacy Guidelines. If an MSME already holds data, it should start by mapping its different personal data processing activities and maintaining appropriate records. In this process, a MSME may need to consider:

        i. For what purpose does your organisation want to use personal data? Why does your organisation need them and what exactly does it need? (i.e. purpose specification principle)

        ii. Does your organisation consider the impacts on society of its processing of personal data? Does it consider the risks from the non-use of such data? Should your organisation be collecting and using personal data for this purpose?

        iii. Does your organisation only collect the personal data it needs? Has it identified the types of personal data to be processed and the methods to be used for the processing of personal data (i.e. collection limitation principle)?

        iv. Is your organisation handling personal data that are relevant to the purposes for which the data are to be used? Does it keep personal data that are accurate and up to date for the purpose (i.e. data quality principle)?

        v. Does your organisation not disclose, make available or otherwise use personal data for purposes other than those originally specified (i.e. use limitation principle) unless it is authorized to do so?

        vi. Does your organisation keep personal data secure (i.e. security safeguards principle)?

[23] See, for example, "Data Protection Essentials", and "Upscaling Digital Capabilities for Better Business Practices", published by the Infocomm Media Development Authority of Singapore.

vii. Does your organisation understand the characteristics of data subjects (especially their vulnerabilities), and offer them a way to exercise their rights regarding the personal data it holds about them (i.e. individual participation principle)?

b. Next, MSMEs could assess privacy risks and possible consequences associated with them. Various risks could be considered, depending on the nature of the MSME's operations. As explained in Section 2.3.3 above, these may include any adverse outcomes to an individual's privacy, such as financial loss and psychological harm, as well as to society as a whole.

c. Then, MSMEs could adjust operations according to identified privacy risks. If the operations of the MSME are overall considered to be low risk, the privacy risk management and privacy by design approaches may be adjusted to such risk. On the other hand, if high privacy risks are anticipated, the MSME may need to put additional safeguards in place by, for example, consulting with experts or reconsidering its operations.

86. Generally, privacy risks may be high for specific categories of business and operations even if MSMEs deal with a small volume of data, when business and operations involve, for example:

a. Use of sensitive data (e.g., a healthcare start-up that processes health data; local public authorities that process sensitive data for administrative services);

b. Automated methods of handling and processing data, including profiling (e.g., a large-scale AI processing) with significant potential impacts on individuals or society;

c. Complex operations (e.g., a small data analytics company that delegates data processing to several third-party organisations).

87. This kind of risk categorisation may differ depending on the type of sector to which MSMEs belong. In this regard, codes of conduct, certification schemes as well as seal/trustmark programmes (see Section 2.4.2 above) that are tailored for MSMEs may be particularly useful. Industry associations or certification bodies operating these schemes may define risk profiles that are often observed in specific industries or business models. MSMEs can rely on the guidance provided by those entities and assess the potential exposure to privacy-related risk. Codes of conduct can represent an especially feasible option for MSMEs in terms of cost efficiency.

88. Privacy enforcement authorities can play a key role. They may offer guidance and advisory services tailored to MSMEs. They may consider developing programmes to address data protection risks common among MSMEs (e.g., unintentional employee misuses of personal data), and to help MSMEs perform common business functions, possibly with the core elements of privacy management programmes that MSMEs should follow.

89. Policies and regulations by governments also play an important role. Policy makers may apply targeted and incentive-driven policy measures for MSME compliance. They could promote the aforementioned certification schemes to align economic incentives with raising privacy awareness by embedding the demonstration of accountability into transactions, procurements and the licensing processes in regulated sectors. Additionally, the option of using digital risk insurance may be more attractive for MSMEs. The financial impacts of a data security breach involving personal data can be significant. A small business without the resources to pay for legal assistance, forensic investigations, the required notifications, remediation measures, and the fines, penalties, or judgments that could arise in the event of a data security breach, might find itself out of business. Public policies can leverage insurance in raising awareness and incentivising the adoption of good

digital risk management practice. Furthermore, digital risk insurance companies may take into account data protection certifications as factors reducing the risk of data security breaches.

## 2.7. Accountability 2.0 and data ethics

90. As discussed thus far, the privacy management programmes that the Privacy Guidelines envisage are not only about legal compliance. As the 2013 Supplementary Explanatory Memorandum provides, privacy management programmes aim at establishing the capacity and effectiveness of organisations to enhance their accountability even in the absence of a data security breach or allegation of non-compliance. The risk-based nature of privacy management programmes will enable organisations to be proactive, responsive (see Section 2.3.3 above) and provide individuals and society as a whole with greater transparency and protections beyond just legal compliance (see Section 2.4 above).

91. These features are often stressed in the notion of "Accountability 2.0". Such a concept relies on a set of values and guiding principles that an organisation must elaborate to ensure legal, fair and just processing through its policies and processes.

92. Ethical considerations regarding data (sometime called "data ethics") are a related, emerging topic, which could be considered as an additional layer of accountability. Data ethics takes into account privacy and data protection, but also the wider societal dimension of personal data processing and the interconnected nature of privacy and other human rights.

93. Data ethics is not embedded in legislation but can be supported by it. Data ethics frameworks are emerging in several countries. Although there is still no shared definition or understanding, data ethics frameworks are directed at practitioners of both personal and non-personal data, setting out a series of principles as regards the processing of data, which encourages those using the framework to tailor their approach to the given situation or project. Legislation could support organisations to make meaningful disclosures of their data ethics practices, ensure regulators understand the practices of organisations, and increase individuals' awareness about these issues.

94. Whilst this Chapter does not attempt to articulate a set of ethical values for the use of personal data, organisations should promote the ethical use of data, especially when they process personal data at scale.

    a. First, organisations should articulate ethical values on their use and management of personal data in a transparent manner, as part of their general vision or in specific data ethics frameworks or guidelines. To do so, organisations should consider the interests at stake both within the organisation and of the external parties impacted by the processing, as well as the interplay with other human rights.

    b. Second, organisations should consider establishing structures such as data ethics boards to review whether their practice complies with their articulated data ethical values, while ensuring full compliance with the legal framework.

    c. Third, they should have processes in place to ensure that data ethical values are considered during the development of a new product or service, and in their relationship with customers or the public.

    d. Fourth, organisations should integrate data ethical values into their training programmes and ensure recognition of such values in staff appraisal programmes.

95. For organisations to implement privacy management programmes, ethical considerations regarding data complement privacy principles including the principle of accountability, and enable organisations to act more responsibly. In turn, data ethics cannot be achieved without a robust implementation of accountability and an established set of rules and principles.