HUNTON& WILLIAMS

global legal group

The International Comparative Legal Guide to:

Data Protection 2016

Preparing for Change: Europe's Data Protection Reforms Now a Reality

Hunton & Williams

Bridget Treacy

Introduction

Europe's data protection laws are about to change. The General Data Protection Regulation ("Regulation") [1] will significantly increase the compliance obligations of organisations that process personal data, strengthen the rights of individuals in relation to their data, and extend the enforcement powers of regulators, including the ability to impose fines of up to €20 million or 4% of global revenue. The Regulation is expected to take effect in early 2018, but organisations should be assessing their compliance posture now, and taking steps to prepare for implementation. A number of changes will require a lengthy lead time to implement. This chapter offers a practical perspective for organisations preparing for change.

European Data Protection Reform

The current reform of Europe's data protection laws was prompted by a widely held view that the Data Protection Directive (EC/95/46) is out of date and no longer fit for purpose. Data processing activities are becoming ever more complex, sophisticated and ubiquitous, and the legislative framework has not kept pace with the data revolution. However, the process of reforming Europe's data protection laws has not been easy. The European Commission released its data protection law reform package on 25 January 2012. Two new pieces of EU law, the Regulation and a directive on the processing of personal data by competent authorities for criminal justice purposes (the "Directive"), were proposed, repealing and replacing the current EU Data Protection Directive and Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters [2]. Political agreement on the legislative text was reached nearly four years later, on 15 December 2015. The Regulation is expected to be formally adopted during the first half of 2016, and will be followed by a two-year implementation period, coming into force in 2018.

Overview of Key Provisions

The Regulation should be regarded as an enhanced, more rigorous version of the existing Data Protection Directive and, given the hefty sanctions for failure to comply, it needs to be taken seriously. Some provisions are new, but many existing concepts have been tweaked or strengthened. Even where apparently small tweaks have been made, organisations should be cautious: in many cases, small tweaks (such as the strengthened requirements for consent) will have a big impact on internal processes, and may take some time to embed. A number of key provisions are explained below.

Harmonisation

The existing European Data Protection Directive has required local implementation by each Member State, and individual Member States have taken differing approaches to this. As a consequence, there is a patchwork of 28 separate data protection laws within the EU, so that organisations that operate in multiple Member States must comply with differing laws across multiple jurisdictions, at considerable cost. In contrast, the Regulation will take direct effect in every Member State without any need for local implementing law. This will streamline and harmonise EU data protection law to a significant extent. Local variances will still remain in a number of areas, such as processing personal data for health, employment and statistical purposes. Additionally, Member States may decide to impose further obligations under national law.

One Stop Shop and Consistency Mechanism

The term "One Stop Shop" was originally used by the European Commission to describe a proposed solution to one of the more frustrating aspects of the current data protection regime. At present, organisations may be subject to the supervisory powers of the data protection authorities of several Member States, each of which may have a different approach to an issue and differing powers of enforcement. For organisations with business operations in several Member States, it is time-consuming to deal with multiple regulators, and difficult (and expensive) to accommodate the differing approaches that regulators may take in relation to the same issue. Despite the European Commission's original intentions, the original "One Stop Shop" proposal has been significantly modified and diluted during negotiations to take into account technical legal concerns on jurisdiction. The supervisory authority of a business' main establishment (i.e., the place where the main processing activities take place), or its only establishment in Europe, will be the 'lead' authority for cross-border data processing [3]. In other words, if a business has multiple subsidiaries across the EU, the "One Stop Shop" is unlikely to apply, but if a single company has operations distributed across Europe, then the One Stop Shop may assist. It should also be noted that the appointment of a lead supervisory authority does not prevent other supervisory authorities from asserting jurisdiction over matters that concern them, such

as complaints made within their jurisdiction [4]. The details of how these provisions will work in practice remain unclear, but are expected to be the subject of early guidance by regulators.

In order to ensure that the Regulation is enforced uniformly across the EU, the Regulation will require the lead authority to consult with other concerned data protection authorities in cases in which enforcement action by a lead authority affects processing activities in more than one Member State (the "Consistency Mechanism") [5]. A wide range of issues, such as multijurisdictional enforcement and binding corporate rules, will fall under the Consistency Mechanism.

Extra-Territorial Effect

There is a significant change to the territorial scope of Europe's data protection law. Currently, the EU Data Protection Directive applies to data controllers that are established within the EU, or make use of data processing equipment situated within the EU. In contrast, the Regulation will apply to the activities of a data controller or data processor established in the EU, whether the processing takes place in the EU or elsewhere [6]. It will also apply to processing by a data controller or data processor established outside the EU where the processing relates to the offering of goods or services to data subjects in the EU or monitoring their behaviour in the EU [7]. This will mean that many non-EU businesses, particularly those active online, will find themselves subject to European law. It should also be noted that the Regulation places obligations on data processors, as well as data controllers. For the first time, data processors will be subject to the same range of sanctions as a data controller in the event of a violation of the Regulation.

Breach Notification Requirements

Currently, Europe does not have mandatory breach notification requirements across all industry sectors. There are some industry-specific notification requirements, and a handful of Member States have enacted their own data breach laws, but the position is not uniform. This position will change under the Regulation. In the event of a data breach, an organisation will be required to notify the competent data protection authority without undue delay and, where feasible, no later than 72 hours after becoming aware of the breach. There is an exemption from notification where the breach is unlikely to result in risk to individuals' rights and freedoms, for example, where the data are encrypted [8]. Where the breach involves high risks to individuals' rights and freedoms, an organisation must also communicate the breach to the individual without undue delay [9]. Mandatory breach notification, together with the ability for individuals to bring group actions against controllers or processors [10], is likely to transform the data breach landscape, bringing the EU closer to the U.S. breach regime, and making data breach a significant area of risk that organisations will need to prioritise.

Increased Obligations and Accountability

The Regulation introduces a number of requirements designed to make organisations more accountable in their data processing activities. The Regulation specifies detailed compliance requirements for both data controllers and data processors, and requires organisations to implement measures to ensure and to demonstrate, including through the adoption and implementation of appropriate data protection policies, that their processing activities comply with the requirements of the Regulation [11]. Some of these changes are set out below.

- Current Registration Requirements Abolished – Requirements to register or notify data processing activities with national data protection authorities will be abolished, but will be replaced by an obligation to maintain internal records [12] of all data processing activities.
- Maintain Inventory of Data Processing – Article 28 sets out a detailed list of information that must be included in an organisation's internal data processing inventory. In many cases, these requirements are significantly more detailed than the equivalent national registration requirements under the Data Protection Directive. Organisations will need to give careful thought as to how these records will be created and maintained. They must be available for inspection on request.
- Lawful Basis for Data Processing – As is the case under the Data Protection Directive, organisations may only process personal data where they have a lawful basis for doing so. The lawful bases are similar to those permitted under the Directive, but the legitimate interests ground, on which companies in the UK routinely rely, is tightened. The relevant legitimate interests must be set out in the data protection notice provided to individuals [13], and the individual can object to processing based on legitimate interests, including profiling [14].
- Tighter Requirements for Consent – Consent will become more difficult to use as a basis for data processing under the Regulation. Organisations that rely on consent will need to review their existing practices carefully and ensure that any consent which they obtain is freely given, specific, informed and unambiguous [15]. Data controllers will have the evidential burden of proving that they have obtained consent [16], which will require most organisations to scrutinise their existing consent mechanisms. "Opt-out" consent, and implied consent mechanisms will need to be updated. Consent will not be considered valid if there is a 'significant imbalance' between the parties, for example, in an employer/employee relationship, requiring detailed review of the circumstances in which consent is utilised in an employment context. The Regulation will also introduce a requirement to obtain parental consent to the processing of personal data relating to a child under 16 years of age [17]. Organisations will need to consider carefully how best to achieve this, particularly in an online context where age verification can be difficult.
- Data Protection by Design and by Default – The Regulation will require organisations to implement data protection by design and by default [18]. These principles require organisations to take privacy and data protection issues into account from the start of any product design process and during the entire life-cycle of the relevant processing activities, and to properly assess the data protection risks before launching any new products. Data controllers will be required to establish and maintain appropriate technical and organisational measures to implement data protection principles in an effective way and to integrate safeguards for data processing so that, by default, only data necessary for each specific processing purpose is collected. This emphasis on data minimisation should be noted, particularly in organisations embarked on big data projects.
- Data Protection Impact Assessments – Data controllers will be required to perform Data Protection Impact Assessments ("DPIA") [19], where the processing of personal data is likely to result in high risk for the rights and freedoms of individuals. In particular, a DPIA will be required for automated data processing activities, including (i) profiling leading to decisions that produce legal effects for an individual, (ii) where the processing includes large-scale processing of certain types of data, or (iii) systematic monitoring of a publicly accessible area on a large scale.

Contracting with Processors

Unlike the Data Protection Directive (which generally relies on data controllers to contractually flow down compliance obligations to data processors), the Regulation will impose direct compliance obligations on data processors [20]. As with the Data Protection Directive, the Regulation will require that the outsourcing of data processing activities by a data controller to a data processor is governed by a written data processing agreement. Whereas the Data Protection Directive does not specify the content of this data processing agreement, the Regulation mandates in detail the terms that must be included in such a contract. Data processors will be directly liable for the security of personal data during processing activities. As noted earlier, data processors will be subject to enforcement by supervisory authorities in the same way as data controllers for violation of the Regulation.

Data Protection Officers

The designation of a Data Protection Officer ("DPO") [21] will be compulsory under the Regulation where (i) the processing is carried out by a public authority or body, (ii) the core activities of the data controller or data processor require regular and systematic monitoring of individuals on a large scale, or (iii) the core activities of the data controller or data processor include processing sensitive personal data on a large scale, including data relating to criminal convictions and offences. In other situations, a DPO may be appointed by the data controller or data processor on a voluntary basis, and must be appointed where required by EU Member State law.

Enforcement

Enforcement powers under the Data Protection Directive vary considerably in practice. In a significant change, all sectors will be subject to the new enforcement powers, sanctions and penalties that the Regulation imposes. Currently, fines under national law are uneven, and are comparatively low (e.g., the maximum UK fine is £500,000). The Regulation will significantly increase the maximum fine to €20 million, or 4% of annual worldwide turnover, whichever is greater [22]. This higher band of fines is applicable to violation of core provisions of the Regulation, including the need for an applicable legal basis for processing. Additional powers include the power to audit data processing activities, which will be new in some jurisdictions, such as the UK. The Regulation will harmonise the approach to enforcement across the EU although, of necessity, there will continue to be variations in practice under local law. Further, the Regulation will make it easier for individuals to enforce their rights [23]. Individuals will have the right to lodge a complaint with a supervisory authority [24], obtain a judicial remedy against a supervisory authority [25], or obtain a judicial remedy against a controller or processor [26]. As noted earlier, where there has been a breach of the rights of data subjects, any association or body acting in the public interest will be able to bring a claim on behalf of affected data subjects under the Regulation, somewhat similar to U.S. class actions.

Strengthening of Data Subject Rights

The Regulation strengthens the rights of data subjects and shifts the burden of establishing such rights away from individuals and towards the organisations that process their personal data. The existing right of erasure is bolstered by an explicit "right to be forgotten", obliging organisations not only to delete data that it is no longer necessary to process, where consent has been withdrawn or where the individual objects, but also to inform recipients of the data that the individual requires those data to be deleted. Individuals will also have a new express right of data portability. This will require controllers to provide personal data in a structured, commonly-used and machine-readable format to individuals. Individuals will also be able to request, where technically feasible, that the data controller send his or her personal data to another data controller, making it easier for consumers to switch between service providers. In addition, individuals will have greater informational rights (including the right to be informed on collection of retention periods, potential third party recipients and the right to complain to supervisory authorities) and a general right to not be subject to automatic automated processing, such as profiling, that produces legal effects for individuals or otherwise significantly affects them.

What Should Organisations Do Now to Prepare?

Start Now!

Many organisations are unaware of the significance of Europe's new data protection laws, or of the extent to which their businesses may be affected. While there have been numerous media headlines about the levels of fines that supervisory authorities will be able to impose, and about the more controversial aspects of the right to be forgotten, many of the changes that form part of the Regulation are much more mundane, and do not merit media headlines. However, organisations need to get into the detail of these seemingly straightforward tweaks and amendments and consider the impact of these changes on their individual organisations. It is quite likely that some of these seemingly small amendments to the legislative text will have a big impact on internal processes, and take time to implement.

Many organisations have been working for some time to analyse what the Regulation will mean for them, and have been planning change projects to implement the required changes to their processes. It is by no means too late to start, but organisations should be aware that the longer they wait, the more they will have to compete for external legal and consultancy support. All organisations will have work to do in order to prepare for the Regulation, and there is already a sense that knowledgeable external legal advisers and consultants are busy.

Where to Start?

It is tempting to start by analysing the Regulation, but the better starting point is to verify existing personal data assets and how they are used within an organisation, for what purpose, with whom they are shared, and what the current data protection programme consists of. Without taking stock of these basic facts, a great deal of time can easily be wasted. The composition of the existing data assets will help to identify key risks and to prioritise remedial tasks.

The data diligence phase can be conducted by devising a basic questionnaire that addresses the following broad topics: data collection (including notice); data processing (legal basis); purpose limitation; data minimisation; data quality; data retention; individual rights; data security; service providers; international data transfers; and works councils. Once this core information is collated from across the business, it must be assessed in order to evaluate the current state of compliance. This should provide a good foundation for the work that will need to be undertaken to ensure compliance

with the Regulation, particularly in those areas where the new requirements represent only a small change to the position under the Directive.

Analysing the Regulation

The second phase of activity is to identify which of the changes in the Regulation will impact the organisation, and what changes will need to be made to the company's existing data protection compliance programme. Based on an assessment of this sort, the organisation will be able to create a list of remedial activities, and begin to prioritise them for action.

Analysing the Regulation may seem daunting, but a number of organisations have approached this task by breaking down the requirements into manageable topics, which are then discussed in detail with relevant business colleagues. It is crucial that those responsible for the operation of business processes are engaged in these discussions. Key topics to consider include the following: definitions; territorial scope; key principles for processing; legal basis for processing; sensitive personal data; privacy notices; individual rights (access, rectification, erasure, restriction of processing, portability, objection, automated decision-making (including profiling)); controller/processor responsibilities; data protection by design and by default; data protection impact assessments; security; breach notification; and cross-border data transfers. Under each of these topic headings, organisations need to understand what the new requirements are, and how they differ from the position under the Directive.

Gap Analysis

The next step is to assess existing compliance against the requirements of the Regulation, and devise specific steps to address any gaps. This gap analysis is a critical step, and a thorough approach is required so that the organisation can then prioritise key remedial tasks. It is only by descending into the detail of the legislation that an organisation will have a true sense of the magnitude of the remedial actions that lie ahead.

Creating Implementation Plan

Once the remedial activities have been identified, the organisation will need to prioritise tasks for implementation. Those that require a lengthy implementation period will need to be planned accordingly. Otherwise, some organisations may prefer to action a number of easy, "quick wins" at the outset. Remaining tasks will need to be scheduled for attention having regard to the importance of the issue, the amount of time likely to be required to address the issue, and available resources.

The data protection team will need to engage the support of others in the organisation to plan and implement required changes. The volume of work, the technical complexity of some of the tasks, and the need for the organisation to play an active role in ensuring that any changes work from an operational perspective, all point to the need to engage additional resources, both internal and external. The data protection team will play a key role in managing the project, and evaluating the implementation, but some organisations are also requiring operational teams to take responsibility and report progress with implementation to regular meetings of the compliance committee. Such a reporting structure may help to ensure that preparation for the Regulation has sufficient internal visibility.

Key Tools for Managing Privacy Risk

In addition to planning for implementation of the Regulation, organisations must consider how they will maintain their data protection compliance programme on an ongoing basis. Key tools to assist with this include the appointment of a DPO, an ongoing focus on the structure and content of the data protection compliance programme, and considering how to adopt a risk-based approach to data protection that, beyond legal compliance, reflects an individual organisation's risk appetite and culture.

Appointing a Data Protection Officer

Many organisations are seeking to appoint DPOs, even where they are not mandated by the Regulation. DPOs can play a key role in managing data privacy risk. As companies search for new ways to understand their customers, manage their businesses and monetise their data assets, a DPO can help to realise these opportunities, ensuring that existing data assets are safeguarded and helping to enhance and protect a corporate reputation.

The detailed responsibilities of a DPO will vary from one organisation to another, but the key focus of the role is to oversee data privacy compliance and to manage data protection risk for the organisation. This is not just about legal compliance with data privacy laws and breach prevention. A DPO can actually help organisations assess new business opportunities that utilise data assets.

Where mandated, the Regulation specifies the tasks that a DPO is required to undertake. First and foremost, a DPO is expected to advise the controller or processor about their compliance obligations under the Regulation, and to monitor compliance with the Regulation, other applicable data protection requirements, and internal data protection policies. The DPO will provide advice on data protection impact assessments, cooperate with the supervisory authority, and act as a contact point for the regulator. Finally, the Regulation specifically requires the DPO to have regard to the risks associated with particular data processing activities; such as the nature, scope, context and purposes of the processing.

Data Protection Compliance Programme

As organisations prepare for implementation of the Regulation, they should also look to their broader privacy compliance framework to ensure that work to implement the Regulation is embedded in that framework.

Typically, a privacy compliance programme will focus on four key areas:

- legal compliance risk – ensuring that the company complies with data privacy laws wherever it does business;
- reputation risk – managing the risk of harm to a company's reputation that can arise from data protection mistakes;
- investment risk – ensuring that data privacy and security requirements are addressed early in the development of new technologies, services and processes. This can prevent disruption and additional costs to business, and limit privacy risk for both the organisation and individuals; and
- reticence risk – companies need to use data protection as a 'business enabler'. Unless companies understand and proactively address data privacy, they may overlook business opportunities, or fall behind their competitors.

Key components of the programme include: policies and processes; people; and technology to help manage data protection compliance.

- *Policies and processes* constitute the rulebook which describes the organisation's approach to data protection, and set out the guidelines and rules that staff are expected to follow. Processes include specific tools that help the organisation, and the DPO, to identify and calibrate privacy risk.
- *People* are key to implementing the organisation's data privacy rulebook. Training and awareness-raising are essential to embedding a privacy programme and building a corporate privacy culture. Staff need to know what the baseline legal requirements are, what the organisation's approach is, and why the organisation thinks data protection is important. The DPO can play a key role in raising awareness and rolling out training.
- *Technology* refers to systems and automated controls. The DPO needs to work with the organisation's IT and Information Security functions to ensure that systems operate in a privacy-compliant way, and that data security is ensured.

Risk-Based Approach

It should also be noted that the Regulation proposes a risk-based approach to compliance, under which organisations will bear responsibility for assessing the degree of risk that their processing activities pose to individuals. Adopting a risk-based approach to compliance does not alter rights or obligations, but is a valuable tool that organisations can utilise to demonstrate accountability, prioritise actions, raise and inform awareness about risk, and identify appropriate mitigation measures. The goal of a risk-based approach to compliance is to reduce the risk as far as is practical but to be explicit about the remaining risk, and how it will be managed. By adopting a risk-based approach to the entire life-cycle management of personal data, from collection to processing to deletion, an organisation can achieve a scalable and proportionate approach to compliance. Boards of directors, CEOs and general counsel have started to realise that irresponsible uses of data, and data breaches, can jeopardise customer trust, destroy reputations, affect their share price, and lead to fines. These incidents can even result in senior executives losing their jobs.

Conclusion

As European data protection law is reformed, existing legal requirements will be tightened, and sanctions strengthened. Fines of up to €20 million, or 4% of annual worldwide turnover, will be available under the new regime. Now, more than ever, organisations need to manage data privacy risk proactively. There is no time to lose. Organisations must begin to consider what the Regulation will mean for them, and start to assess their compliance posture, so that remedial tasks can be identified and targeted in good time. In a world in which personal data processing underpins so much business, social, charitable and public sector activity, and where individuals are increasingly aware of their data protection rights, these tasks cannot be left to chance. An organisation's reputation is increasingly tied to how well they respect and take care of the personal data that they process. The time has come to begin preparations for implementing the Regulation.

Endnotes

1. A copy of the consolidated text is available at: http://static.ow.ly/docs/Regulation_consolidated_text_EN_47uW.pdf.
2. The discussion in this chapter focuses only on the Regulation.
3. Article 51a(1) of the Regulation.
4. Article 51a(2a) of the Regulation.
5. Articles 57–62 of the Regulation.
6. Article 3(1) of the Regulation.
7. Article 3(2) of the Regulation.
8. Article 31 of the Regulation.
9. Article 32 of the Regulation.
10. Article 76 of the Regulation.
11. Articles 5 and 22 of the Regulation.
12. Article 28 of the Regulation.
13. Article 14(1)(c) of the Regulation.
14. Article 19(1) of the Regulation.
15. Article 4 of the Regulation.
16. Article 7 of the Regulation.
17. Article 8 of the Regulation.
18. Article 23 of the Regulation.
19. Article 33 of the Regulation.
20. Articles 28–31, 33–35 and 40 of the Regulation.
21. Articles 35–37 of the Regulation.
22. Article 79 of the Regulation.
23. Articles 53, 74, 75 and 77 of the Regulation.
24. Article 73 of the Regulation.
25. Article 74 of the Regulation.
26. Article 75 of the Regulation.

Bridget Treacy
Hunton & Williams
30 St Mary Axe
London, EC3A 8EP
United Kingdom

Tel: +44 207 220 5600
Fax: +44 207 220 5772
Email: btreacy@hunton.com
URL: www.hunton.com

Bridget Treacy leads Hunton & Williams' UK Privacy and Cybersecurity team and is also the Managing Partner of the firm's London office. Her practice focuses on all aspects of privacy, data protection, information governance and e-commerce issues for multinational companies across a broad range of industry sectors. Bridget's background in complex technology transactions enables her to advise on the specific data protection and information governance issues that occur in a commercial context. Bridget is the editor of the specialist privacy journal, *Privacy and Data Protection*, and has contributed to a number of published texts. According to *Chambers UK*, "she is stellar, one of the leading thinkers on data protection, providing practical solutions to thorny legal issues".

HUNTON& WILLIAMS

Hunton & Williams' Global Privacy and Cybersecurity practice is a leader in its field. It has been ranked by *Computerworld* for four consecutive years as the top law firm globally for privacy and data security. *Chambers & Partners* ranks Hunton & Williams as the top privacy and data security practice in its *Chambers & Partners UK*, *Chambers Global* and *Chambers USA* guides.

The team of more than 25 privacy professionals, spanning three continents and five offices, is led by Lisa Sotto, who was named among the *National Law Journal*'s "100 Most Influential Lawyers". With lawyers qualified in six jurisdictions, the team includes internationally-recognised partners Bridget Treacy and Wim Nauwelaerts, former FBI cybersecurity counsel Paul Tiao, and former UK Information Commissioner Richard Thomas.

In addition, the firm's Centre for Information Policy Leadership, led by Bojana Bellamy, collaborates with industry leaders, consumer organisations and government agencies to develop innovative and pragmatic approaches to privacy and information security.

Belgium

Wim Nauwelaerts

Hunton & Williams

David Dumont

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The Act on the Protection of Privacy in Relation to the Processing of Personal Data of December 8, 1992 (*Wet tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens/Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel*) (the "Data Protection Act") (as amended) and the Royal Decree of February 13, 2001 implementing the Data Protection Act (the "Royal Decree").

1.2 Is there any other general legislation that impacts data protection?

The Electronic Communications Act of June 13, 2005 (*Wet betreffende de elektronische communicatie/Loi relative aux communications électroniques*) (the "Electronic Communications Act") (as amended) contains provisions regarding the confidentiality of electronic communications and the use of cookies and similar technologies.

In addition, the processing of personal data for electronic marketing purposes is regulated in the Belgian Code on Economic Law of February 28, 2013.

1.3 Is there any sector specific legislation that impacts data protection?

The Electronic Communications Act imposes requirements on providers of telecommunication and internet services regarding data retention, the use of location data and the notification of data security breaches. There is also specific legislation on the processing of personal data in the financial sector.

1.4 What is the relevant data protection regulatory authority(ies)?

The Belgian Privacy Commission (*Commissie voor de bescherming van de persoonlijke levenssfeer/Commission de la protection de la vie privée*) oversees compliance with Belgian privacy and data protection law.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **"Personal Data"**

  Personal data is "any information relating to an identified or identifiable natural person".
- **"Sensitive Personal Data"**

  The Data Protection Act identifies three types of sensitive personal data:
  - personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership as well as the processing of data concerning sex life;
  - health-related personal data; and
  - personal data relating to litigation that has been submitted to Courts and Tribunals as well as to administrative judicial bodies, relating to suspicions, prosecutions or convictions in matters of crime, administrative sanctions or security measures.
- **"Processing"**

  Processing is "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by means of transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction of personal data".
- **"Data Controller"**

  The data controller is "any natural or legal person, un-associated organisation or public authority which alone or jointly with others determines the purposes and means of the processing of personal data".
- **"Data Processor"**

  The data processor is "any natural person, legal person, un-associated organisation or public authority which processes personal data on behalf of the controller, except for the persons who, under the direct authority of the controller, are authorised to process the data".
- **"Data Subject"**

  The data subject is "an identified or identifiable natural person". An identifiable person is "one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".

- *Other key definitions – please specify (e.g., "Pseudonymous Data", "Direct Personal Data", "Indirect Personal Data")*
  - **"Pseudonymous Data"**

    Belgian data protection law does not contain a definition of "pseudonymous data". However, the Royal Decree defines encoded data as "personal data which can only be linked to an identified or identifiable individual by way of a code".
  - **"Direct Personal Data"**

    "Direct personal data" is not defined or used in Belgian data protection law.
  - **"Indirect Personal Data"**

    "Indirect personal data" is not defined or used in Belgian data protection law.

3 Key Principles

3.1 What are the key principles that apply to the processing of personal data?

- **Transparency**

  Data controllers are required to inform data subjects of the processing of their personal data. The Data Protection Act lists the information that must be provided to data subjects (e.g., processing purposes, data subjects' rights, etc.).
- **Lawful basis for processing**

  Data controllers must have a legal basis for each data processing activity. The Data Protection Act includes an exhaustive list of the legal grounds for processing of (sensitive) personal data (e.g., data subjects' consent).
- **Purpose limitation**

  Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a way incompatible with those purposes.
- **Data minimisation**

  Personal data must be accurate, relevant and not excessive in relation to the purposes for which they were collected and processed. Data controllers are required to limit the data processing to what is strictly necessary for the processing purpose.
- **Proportionality**

  As part of the data minimisation principle, personal data collected and processed must be proportionate to the processing purposes.
- **Retention**

  Personal data must be kept in a form that allows for the identification of data subjects for no longer than necessary in light of the purposes for which the data are collected or further processed.
- *Other key principles – please specify*

  There are no other key principles in particular.

4 Individual Rights

4.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Access to data**

  Data subjects are entitled to request that the data controller provides information regarding the processing of their personal data and communicates the data in an intelligible form. This does not necessarily entail that data subjects should have direct access to data files or have the right to obtain a copy of their personal data.
- **Correction and deletion**

  Data subjects are entitled to obtain, free of charge, the rectification of incorrect personal data relating to them. Data subjects are also entitled to obtain, free of charge, the erasure of or the prohibition to use all personal data relating to them that is incomplete or irrelevant with a view to the purpose of the processing, or where the recording, disclosure or storage of the data is prohibited, or where it has been stored for longer than the authorised period of time.
- **Objection to processing**

  Under certain conditions, data subjects are entitled to object to the processing of personal data relating to them.
- **Objection to marketing**

  If personal data are obtained for direct marketing purposes, data subjects may object to the intended processing of their personal data, free of charge and without reason.

  Data subjects must be informed of this right to object when their personal data are collected for direct marketing purposes.
- **Complaint to relevant data protection authority(ies)**

  Data subjects are entitled to request the Privacy Commission, free of charge, to exercise their rights on their behalf.
- *Other key rights – please specify*
  - **Automated decision-making**

    Data subjects have the right not to be subject to decisions having legal effects or significantly affecting them, which are taken purely on the basis of automatic data processing aimed at assessing certain aspects of their personality, unless the decisions are taken in the context of an agreement or if they are based on a legal provision.
  - **Right to compensation**

    Data subjects have the right to receive compensation from data controllers for damage incurred as a result of a violation of the Data Protection Act, unless the data controllers can prove that the facts which caused the damage cannot be ascribed to them.

5 Registration Formalities and Prior Approval

5.1 In what circumstances is registration or notification required to the relevant data protection regulatory authority(ies)? (E.g., general notification requirement, notification required for specific processing activities.)

In Belgium, there is a general obligation for data controllers to notify their data processing activities to the Privacy Commission. Exemptions from this notification obligation exist for standard data processing activities (e.g., standard payroll administration), provided certain conditions are met (e.g., conditions concerning types of data and data subjects, data retention, disclosure to third parties, etc.).

5.2 On what basis are registrations/notifications made? (E.g., per legal entity, per processing purpose, per data category, per system or database.)

Notifications are made per processing purpose or set of related purposes.

5.3 Who must register with/notify the relevant data protection authority(ies)? (E.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation.)

Data controllers must notify their data processing activities (falling within the scope of the Data Protection Act) to the Privacy Commission unless an exemption applies. This includes data processing activities performed in the context of the effective and actual activities of a data controller permanently established on Belgian territory or in a place where Belgian law applies by virtue of international public law, as well as data processing activities of data controllers established outside the EU, using means for processing personal data located on Belgian territory (unless the means are only used for the purposes of transit of personal data through Belgian territory). In the latter case, the data controller established outside the EU is required to appoint a representative in Belgium.

Furthermore, joint data controllers may file a common notification.

5.4 What information must be included in the registration/notification? (E.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes.)

The notification should describe the data processing operation(s). In particular, the notification should include the name, address and contact details of the data controller (and, if applicable, his representative), the name of the processing activity, the purpose or set of related purposes of the data processing, the categories of personal data being processed (including a detailed description of sensitive data, if any), the categories of data recipients (including the safeguards linked to the disclosure of data to these third parties), the manner in which data subjects are informed of the data processing and how they can exercise their rights, the applicable data retention periods, the security measures implemented to protect the personal data and the countries to which personal data may be transferred (including the legal basis for transfers to non-EEA countries).

5.5 What are the sanctions for failure to register/notify where required?

Failure to notify can be sanctioned with fines of up to EUR 600,000.

5.6 What is the fee per registration (if applicable)?

The fee for notification is:

- EUR 25 for notifications submitted online;
- EUR 125 for notifications submitted via paper forms; and
- EUR 20 for amending existing notifications.

5.7 How frequently must registrations/notifications be renewed (if applicable)?

Notifications should be updated when the information provided therein is no longer accurate.

5.8 For what types of processing activities is prior approval required from the data protection regulator?

In general, prior approval from the Privacy Commission is not required to carry out data processing activities. However, specific authorisation requirements may apply in certain exceptional cases (e.g., for the processing of data from the national register or for data processing for historical, statistical or scientific purposes).

International data transfers on the basis of *ad hoc* international data transfer agreements or Binding Corporate Rules ("BCR") also require prior approval (see section 8 below).

5.9 Describe the procedure for obtaining prior approval, and the applicable timeframe.

Several sector committees are established within the Privacy Commission which are responsible for granting prior approval for certain specific types of data processing. The procedure differs depending on the sector committee.

The procedure for prior approval of *ad hoc* international data transfer agreements or BCRs is described in section 8 below.

6 Appointment of a Data Protection Officer

6.1 Is the appointment of a Data Protection Officer mandatory or optional?

The appointment of a Data Protection Officer is optional (except for certain public bodies). The Privacy Commission has indicated that it supports the appointment of Data Protection Officers and that these appointments should be seen as an accountability measure which the data controller should be able to take freely, considering the processing operations carried out, the actual risks, the existence of other protection mechanisms and the actual benefits the appointment of a Data Protection Officer would offer in terms of increased data protection.

6.2 What are the sanctions for failing to appoint a mandatory Data Protection Office where required?

This is not applicable.

6.3 What are the advantages of voluntarily appointing a Data Protection Officer (if applicable)?

There are no specific legal advantages (such as exemption from notification obligation). Nevertheless, the appointment of a Data Protection Officer is one of the information security measures recommended by the Privacy Commission.

6.4 Please describe any specific qualifications for the Data Protection Officer required by law.

This is not applicable.

6.5 What are the responsibilities of the Data Protection Officer, as required by law or typical in practice?

Typically, a Data Protection Officer is responsible for the execution of the data controller's information security policy.

6.6 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

No, this is not the case in Belgium (unless in limited cases where prior approval of one of the sector committees of the Privacy Commission is required).

7 Marketing and Cookies

7.1 Please describe any legislative restrictions on the sending of marketing communications by post, telephone, email, or SMS text message. (E.g., requirement to obtain prior opt-in consent or to provide a simple and free means of opt-out.)

The automated sending of marketing communications by telephone without human intervention or by fax requires prior opt-in consent. The sending of marketing communications by SMS or by email also requires prior consent, unless the recipients are existing customers or legal entities and specific conditions are met. Direct marketing via other techniques to individuals who opted out of receiving such marketing communications is prohibited.

In addition, the Data Protection Act contains a general obligation for data controllers to provide data subjects with a right to opt-out of the processing of their personal data for direct marketing purposes.

7.2 Is the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

The Privacy Commission has indicated that it considers direct marketing to be an important issue. However, it is unclear whether the Privacy Commission is actively enforcing marketing rules since the Privacy Commission rarely publishes information on its enforcement actions.

7.3 Are companies required to screen against any "do not contact" list or registry?

Before contacting individuals by phone for marketing purposes, companies are required to verify whether or not the concerned individuals have registered their name on the "do not call me anymore" list ("*bel-me-niet-meer-lijst*"), which is kept by non-profit organisation DNCM. Telecom operators are required to inform their users about this list and individuals can register online (www.bel-me-niet-meer.be). Contacting individuals registered on the list is prohibited, unless the company has obtained the specific consent of the individuals.

The Belgian Direct Marketing Association maintains a similar list for marketing by post, called the "Robinson" list. However, this list only imposes obligations on members of the Belgian Direct Marketing Association.

7.4 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

The use of automated calling systems without human intervention (automatic calling machines) or fax machines for sending marketing without prior opt-in consent may lead to fines of up to EUR 60,000. Sending marketing by SMS or email without prior opt-in consent may result in fines of up to EUR 150,000.

7.5 What types of cookies require explicit opt-in consent, as mandated by law or binding guidance issued by the relevant data protection authority(ies)?

The use of cookies requires opt-in consent, unless the cookie is used for the sole purpose of carrying out the transmission of a communication over an electronic communications network or if the cookie is strictly necessary to provide a service requested by the subscriber or user.

7.6 For what types of cookies is implied consent acceptable, under relevant national legislation or binding guidance issued by the relevant data protection authority(ies)?

The cookie rules imposed by EU Directive 2009/136/EC have been transposed in Article 129 of the Electronic Communications Act. Article 129 contains the same language as the cookie clause in EU Directive 2009/136/EC and it does not provide guidance as to how to obtain consent to the use of cookies. According to the Privacy Commission's Recommendation (nr. 01/2015) on the Use of Cookies, consent requires a clear action from the user (e.g., ticking a box or browsing to another webpage provided that the cookie notice is displayed until the user makes an explicit choice). Implied consent for the use of cookies is generally not considered acceptable.

7.7 To date, has the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

In June 2015, the Privacy Commission initiated legal proceedings against Facebook for tracking individuals' browsing behaviour through cookies and social plug-ins without obtaining their consent. The Brussels Court of First Instance ordered Facebook to stop this practice. If Facebook does not comply with the Court's decision, it will have to pay a fine of EUR 250,000 per day of non-compliance.

7.8 What are the maximum penalties for breaches of applicable cookie restrictions?

Certain sanctions provided in the Belgian Criminal Code and the Data Protection Act could be imposed in the case of violation of the Belgian cookie rules. Possible sanctions include fines of up to EUR 600,000.

8 Restrictions on International Data Transfers

8.1 Please describe any restrictions on the transfer of personal data abroad?

In principle, the transfer of personal data to a country outside the EEA that does not provide an "adequate level of protection" is prohibited. The Privacy Commission follows the European Commission's decisions as regards those countries that are considered to provide such adequate level of protection.

The Data Protection Act provides a limited list of exceptions to this general prohibition. For instance, data transfers are permitted if the data subject has unambiguously given his/her consent to the proposed data transfer. The Data Protection Act also provides a derogation from the general prohibition if the data controller "ensures adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals, and regarding the exercise of the corresponding rights; such safeguards can result from appropriate contractual clauses in particular".

8.2 Please describe the mechanisms companies typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions.

Companies typically put in place data transfer agreements based on the European Commission's Standard Contractual Clauses. More and more companies are also starting to use BCRs.

8.3 Do transfers of personal data abroad require registration/notification or prior approval from the relevant data protection authority(ies)? Describe which mechanisms require approval or notification, what those steps involve, and how long they take.

Each notification with the Privacy Commission contains a section on international data transfers that must be completed in cases where personal data are transferred abroad.

International data transfers to non-EEA countries that provide an adequate level of data protection, or that are based on one of the statutory exemptions listed in the Data Protection Act, do not require authorisation. However, in the case of data transfers based on a data transfer agreement, the agreement must be submitted to the Privacy Commission for approval, even if the agreement is based on one of the European Commission's Standard Contractual Clauses. In accordance with the Protocol of June 25, 2013 between the Privacy Commission and the Belgian Ministry of Justice, if the Privacy Commission concludes that the data transfer agreement incorporates the European Commission's Standard Contractual Clauses, the Privacy Commission will simply inform the data controller that the proposed international data transfers are permitted. In the case of a non-standardised data transfer agreement, the Privacy Commission will examine whether the data transfer agreement provides adequate safeguards for the international data transfer. If the Privacy Commission determines that the safeguards are adequate, the Ministry of Justice will verify that the entity complied with the applicable procedural rules and, if so, approve the agreement by Royal Decree.

In cases of data transfers based on a BCR, the BCR also needs to be sent to the Privacy Commission for approval. The Privacy Commission will review the BCR and send its opinion to the Ministry of Justice. In accordance with the Protocol of July 13, 2011 between the Privacy Commission and the Ministry of Justice, if the Privacy Commission's opinion is favourable, the Ministry of Justice will verify that the process specified in the Protocol has been followed and, if so, automatically approve the BCR by Royal Decree.

9 Whistle-blower Hotlines

9.1 What is the permitted scope of corporate whistle-blower hotlines under applicable law or binding guidance issued by the relevant data protection authority(ies)? (E.g., restrictions on the scope of issues that may be reported, the persons who may submit a report, the persons whom a report may concern.)

In accordance with the Privacy Commission's Recommendation on the implementation of whistle-blowing schemes (Recommendation 01/2006 of November 29, 2006), the scope of corporate whistle-blower hotlines under Belgian data protection law does not need to be limited to certain issues. However, the Privacy Commission recommends that whistle-blower hotlines should only be used for reporting very serious issues that should be reported in the general interest or for the proper governance of the company (e.g., violations of financial, accounting or criminal law) and which, in the opinion of the whistle-blower, cannot be reported through the company's normal reporting channels (for example, the whistle-blower's first-line manager).

9.2 Is anonymous reporting strictly prohibited, or strongly discouraged, under applicable law or binding guidance issued by the relevant data protection authority(ies)? If so, how do companies typically address this issue?

Anonymous reporting is not prohibited, but it should not be encouraged. The Privacy Commission follows the Article 29 Working Party Opinion 1/2006 (WP 117) on this point, which provides that anonymous reporting should only be allowed as an exception to the rule and under the following conditions:

- anonymous reporting is not encouraged; and
- whistle-blowers are informed, when submitting a report, that their identity will be kept confidential at all the stages of the process and in particular will not be disclosed to third parties, either to the incriminated person or to the whistle-blower's line management.

If, despite this information, the person reporting to the scheme still wants to remain anonymous, the report will be accepted into the scheme.

9.3 Do corporate whistle-blower hotlines require separate registration/notification or prior approval from the relevant data protection authority(ies)? Please explain the process, how long it typically takes, and any available exemptions.

Prior to implementation, the whistle-blower hotline must be notified to the Privacy Commission. The notification will typically be processed and published within 21 days after completion of the notification procedure. Prior approval is not required.

9.4 Do corporate whistle-blower hotlines require a separate privacy notice?

There is no explicit requirement to have a separate notice for a whistle-blower hotline. However, as the information that needs to be provided to individuals about the whistle-blower hotline is rather specific (e.g., description of the procedure for submitting and handling reports, possible consequences of unfounded reports, etc.), in practice companies tend to implement a separate privacy notice for their whistle-blower hotline.

9.5 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

Works councils/trade unions/employee representatives must be informed prior to implementing a whistle-blower hotline in the company.

10 CCTV and Employee Monitoring

10.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies)?

In accordance with the Camera Surveillance Act of March 21, 2007, the use of CCTV requires a separate notification with the Privacy Commission. In the case of CCTV surveillance at the workplace, an additional notification with the Privacy Commission is required in accordance with Collective Labour Agreement no. 68 concerning camera surveillance at the workplace.

10.2 What types of employee monitoring are permitted (if any), and in what circumstances?

Employers may monitor employees' use of the company's email and internet system, in accordance with the procedures set out in Collective Labour Agreement no. 81 concerning the monitoring of electronic online communications of employees. Collective Labour Agreement no. 81 limits the monitoring to the following purposes:

1. the prevention of any unwanted, improper or defamatory activities or facts, or activities or facts that are against the public decency or may harm the dignity of other persons;
2. the protection of confidential economic, commercial and financial interests of the company, and to act against any practices inconsistent with the preservation of these interests;
3. the preservation of the security and/or the good technical functioning of the company's IT network systems, including monitoring the costs associated with it and the physical protection on the company's facilities; and
4. compliance in good faith with the company's policies and any other applicable principles and rules on the use of online technologies.

On May 2, 2012, the Privacy Commission issued a Recommendation on workplace cyber-surveillance (Recommendation 08/2012). In this Recommendation, the Privacy Commission explains via practical examples how employers can comply with Belgian privacy and data protection law when monitoring employees' use of the company's IT system. For instance, the Privacy Commission strongly recommends employers to encourage employees to label their private emails as "personal" and/or to store them in a folder marked as private. The Privacy Commission also recommends companies to appoint a neutral, trusted individual who will be authorised to review an absent/dismissed employee's emails and determine which emails are of a professional nature and need to be read by the employer (e.g., to pass on an urgent matter to a colleague while an employee is absent).

10.3 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Employees should be informed of any monitoring. This is typically done via a HR privacy policy, an IT acceptable use policy or a specific monitoring policy. It is not required, nor is it advisable, to obtain their consent. The Privacy Commission takes the view that an employee's consent is, in principle, not considered to be freely given, because of his/her subordinate position.

10.4 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

Employee representative bodies such as works councils must be informed of the introduction of employee monitoring systems and should evaluate the systems on a regular basis.

10.5 Does employee monitoring require separate registration/notification or prior approval from the relevant data protection authority(ies)?

Employee monitoring can be notified to the Privacy Commission as part of a general HR management registration.

11 Processing Data in the Cloud

11.1 Is it permitted to process personal data in the cloud? If so, what specific due diligence must be performed, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

To date, the Privacy Commission has not issued specific guidance on processing of personal data in the cloud. However, it has announced that it is currently preparing such guidance. In the meantime, the Privacy Commission is likely to expect that data controllers and processors follow the guidelines issued by the Article 29 Working Party on this topic (in particular, Opinion 05/2012). In addition, the Data Protection Act imposes a general obligation on data controllers to: a) select processors providing sufficient safeguards in respect of the technical and organisational measures for the intended processing; and b) ensure compliance with these measures, in particular by contractual stipulations. This general obligation also applies in a cloud computing context.

11.2 What specific contractual obligations must be imposed on a processor providing cloud-based services, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

In the absence of specific guidance on processing of personal data in the cloud, the contract with a processor providing cloud-based services must contain at least the following elements:

- an obligation for the data processor to implement technical and organisational security measures for the intended processing;

- the data processor's liability towards the data controller; and
- the requirement that the data processor shall only act on behalf of the data controller and that it is bound by the same data security duties as the data controller.

12 Big Data and Analytics

12.1 Is the utilisation of big data and analytics permitted? If so, what due diligence is required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

To date, the Privacy Commission has not issued specific guidance on the utilisation of big data and analytics. However, Royal Decree of February 13, 2001 contains specific rules on further processing of personal data for historical, statistical or scientific purposes, which may be relevant to certain big data applications or analytics. Pursuant to the Royal Decree, further processing of personal data for historical, statistical or scientific purposes must in principle take place using anonymous data. If it is impossible to achieve the historical, statistical or scientific purposes using anonymous data for the further processing, the data controller of the further processing for historical, statistical or scientific purposes may process encoded data and, in exceptional circumstances, non-encoded personal data.

13 Data Security and Data Breach

13.1 What data security standards (e.g., encryption) are required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

Data controllers and processors are required to implement appropriate technical and organisational measures to protect personal data from accidental or unauthorised destruction, accidental loss, as well as from alteration, access and any other unauthorised processing. These measures must ensure an appropriate level of security taking into account the state of technological development in this field and the cost of implementing the measures on the one hand, and the nature of the personal data to be protected and the potential risks related to the processing on the other hand.

The Privacy Commission has issued non-binding guidance as to the type of security measures (e.g., encryption) that should be implemented (*Referentiemaatregelen voor de beveiliging van elke verwerking van persoonsgegevens/Mesures de référence en matière de sécurité applicables à tout traitement de données à caractère personnel* and *Aanbeveling uit eigen beweging betreffende de na te leven veiligheidsmaatregelen ter voorkoming van gegevenslekken/ Recommandation d'initiative relative aux mesures de sécurité à respecter afin de prévenir les fuites de données*).

13.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.

The Electronic Communications Act imposes a duty on providers of publicly available electronic communications services to notify data breaches, under certain conditions, to the Privacy Commission. The notification should contain the following information: (i) the nature of the data breach; (ii) consequences of the data breach; (iii) details of person which can be contacted for more information concerning the breach; (iv) measures suggested or implemented to address the data breach; and (v) measures recommended to mitigate the negative effects of the data breach. Where feasible, the notification should be completed within 24 hours after detection of the breach. In cases where the company does not have all required information within this timeframe, it can complete the notification within 72 hours after the initial notification. The Privacy Commission has published a template form on its website to accommodate companies in complying with their data breach notification obligations.

Except for the notification duty in the Electronic Communications Act, there is currently no general data breach notification obligation. However, the Privacy Commission strongly recommends all types of data controllers to notify data breaches. It has published a separate template form on its website to be used by data controllers that are not electronic communication providers for the purposes of notifying data breaches.

13.3 Is there a legal requirement to report data breaches to individuals? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.

Unless a specific exemption applies, providers of publicly available electronic communications services should report data breaches to the affected individuals immediately after detection of the breach in cases where the breach is likely to negatively impact their privacy. This notification should contain the following information: (i) name of the company; (ii) contact person; (iii) description of the data breach; (iv) date of the data breach; (v) the data affected by the breach; (vi) possible consequences for the privacy of the concerned individual; (vii) circumstances of the data breach; (viii) measures implemented by the company to remedy the data breach; and (ix) recommended measures for the affected individuals to mitigate the negative effects of the breach. The Privacy Commission also recommends data controllers that do not qualify as electronic communication providers to notify the affected individuals in the event of a data breach.

13.4 What are the maximum penalties for security breaches?

Belgian data protection law does not provide specific penalties for security breaches.

14 Enforcement and Sanctions

14.1 Describe the enforcement powers of the data protection authority(ies):

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
The Privacy Commission has the power to investigate possible violations of Belgian privacy and data protection law, at its own initiative or following complaints from individuals.	The Privacy Commission cannot impose sanctions. If it determines that Belgian privacy and data protection law may have been violated, it can bring the case before the Court of First Instance or refer it to the Public Prosecutor. In addition, a violation of Belgian privacy and data protection law may lead to civil action for damages.	Unlawfully processing personal data is punishable with fines of up to EUR 600,000, confiscation of the media containing the personal data to which the offence relates, the erasure of the data or the prohibition to manage any processing of personal data, directly or through an agent, for a period of up to two years. A Court may also order the publication of the judgment in one or more newspapers. Any repeated violation of the Data Protection Act is punishable by a term of imprisonment of up to two years, and/or fines of up to EUR 600,000.

14.2 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

The Privacy Commission does not publish statistics on its enforcement actions, but criminal proceedings will typically only be initiated in cases of severe violations.

15 E-discovery / Disclosure to Foreign Law Enforcement Agencies

15.1 How do companies within your jurisdiction respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

As a matter of best practice, companies within Belgium should attempt to comply with the recommendations in Working Document 1/2009 of the Article 29 Working Party when responding to foreign e-discovery requests or requests for disclosure from foreign law enforcement agencies.

15.2 What guidance has the data protection authority(ies) issued?

To date, the Privacy Commission has not issued specific guidance on the processing of personal data in the context of e-discovery requests. However, the Privacy Commission is likely to expect that data controllers and processors follow the guidelines issued by the Article 29 Working Party on this topic (in particular, Working Document 1/2009), as representatives of the Privacy Commission participated in the sub-group of the Article 29 Working Party that drafted the Working Document.

16 Trends and Developments

16.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

In 2015, the Privacy Commission has taken a number of enforcement initiatives related to the protection of individuals' privacy online.

The Privacy Commission has, for example, participated in the Internet Sweep Day organised by the Global Privacy Enforcement Network ("GPEN"), during which a number of data protection authorities performed a coordinated audit of approximately 1,500 websites and apps intended for, or popular with, children. The Privacy Commission has announced that it will reach out to a number of website and app developers with the findings of the audit. In cases where the audit revealed serious violations of the Data Protection Act, the Privacy Commission may issue a formal warning and, where necessary, forward the case to the competent authorities for further investigation and/or prosecution (e.g., to the Public Prosecutor).

The Privacy Commission's focus on online privacy was further demonstrated by its enforcement actions against Facebook for tracking online behaviour of non-members through cookies and social plug-ins. After issuing a formal Recommendation to Facebook, the Privacy Commission initiated legal proceedings before the Brussels Court of First Instance in June 2015. In November 2015, the Brussels Court ordered Facebook to stop tracking non-users. If Facebook does not comply with the Court's decision, it faces a fine of EUR 250,000 per day.

16.2 What "hot topics" are currently a focus for the data protection regulator?

Similar to other data protection authorities throughout the EU, the Privacy Commission will most likely focus on preparing for its new role and tasks under the upcoming General Data Protection Regulation.

International data transfers and the mechanisms available to companies to legitimise such transfers will probably also remain a "hot topic" for the Privacy Commission following the invalidation of Safe Harbour and the introduction of the alternative EU-US Privacy Shield for transatlantic data flows.

Wim Nauwelaerts
Hunton & Williams
Park Atrium
Rue des Colonies 11
1000 Brussels
Belgium

Tel: +32 2 643 58 14
Fax: +32 2 643 58 22
Email: wnauwelaerts@hunton.com
URL: www.hunton.com

Wim Nauwelaerts is the managing partner of the firm's Brussels office and leads the Privacy and Cybersecurity team there. Wim advises companies on all aspects of EU and international data protection and privacy compliance, including data protection notifications, implementation of data security measures, compliance training, data transfer strategies, privacy implications of cross-border M&A transactions and representations before data protection authorities. Wim has been recognised as a leading privacy practitioner by *Chambers Global*, *Chambers Europe*, *The Legal 500* (Belgium), the *International Who's Who of Technology Lawyers*, and by *Global Law Experts*. He has written and spoken widely on privacy-related topics, such as cloud computing, interest-based advertising, cross-border discovery and privacy compliance in pharmaceutical research.

David Dumont
Hunton & Williams
Park Atrium
Rue des Colonies 11
1000 Brussels
Belgium

Tel: +32 2 643 58 18
Fax: +32 2 643 58 22
Email: ddumont@hunton.com
URL: www.hunton.com

David Dumont assists a broad range of clients with all aspects of Belgian and EU data protection law, including HR and customer data privacy issues, implementation of cross-border data transfer strategies and completing registrations with national data protection authorities.

HUNTON& WILLIAMS

Hunton & Williams' Global Privacy and Cybersecurity practice is a leader in its field. It has been ranked by *Computerworld* for four consecutive years as the top law firm globally for privacy and data security. *Chambers & Partners* ranks Hunton & Williams as the top privacy and data security practice in its *Chambers & Partners UK*, *Chambers Global* and *Chambers USA* guides.

The team of more than 25 privacy professionals, spanning three continents and five offices, is led by Lisa Sotto, who was named among the *National Law Journal*'s "100 Most Influential Lawyers". With lawyers qualified in six jurisdictions, the team includes internationally-recognised partners Bridget Treacy and Wim Nauwelaerts, former FBI cybersecurity counsel Paul Tiao, and former UK Information Commissioner Richard Thomas.

In addition, the firm's Centre for Information Policy Leadership, led by Bojana Bellamy, collaborates with industry leaders, consumer organisations and government agencies to develop innovative and pragmatic approaches to privacy and information security.

China

Manuel E. Maisog

Judy Li

Hunton & Williams

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

There is no comprehensive, consolidated data protection law in China.

1.2 Is there any other general legislation that impacts data protection?

The *P.R.C. Constitution* establishes an individual's right to dignity, which under relevant rules is further interpreted to include a right of privacy. The *P.R.C. Constitution* also establishes an individual's right of freedom and secrecy of correspondence. The *Tort Liability Law* explicitly protects the right of privacy, and allows private rights of action for invasions of privacy. The *Ninth Amendment to the P.R.C. Criminal Law* establishes criminal liabilities for the sale or provision of personal information to a third party in violation of law. The *Decision on Enhancing Internet Information Protection* protects personal electronic data which is collected and transferred through the Internet. In addition, a consumer's personal information is protected under the *Consumer Rights Protection Law*. Finally, a draft *Cybersecurity Law* may have impact on the manner in which the development and promotion of cybersecurity will be governed in China.

1.3 Is there any sector specific legislation that impacts data protection?

In China, personal data protection rules are scattered among various sector specific Chinese laws and regulations. For example, personal financial information has extensive protection under banking sector regulations, and the telecommunications sector has its own rules protecting the personal information of telecommunications service users.

1.4 What is the relevant data protection regulatory authority(ies)?

There is no particular data protection regulatory authority. Government agencies may act as regulatory authorities in particular industry sectors under their respective oversight.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **"Personal Data"**

  There is no clear, single and fundamental definition of "personal data". However, generally speaking "personal data" refers to information which relates to an individual and which either (1) can independently identify the individual, or (2) may be used to identify the individual when combined with other information.

  To take one example, a regulation of the State Administration for Industry and Commerce defines "consumer personal information" as "information collected by an enterprise operator during the sale of products or provision of services, that can, singly or in combination with other information, identify a consumer". The regulation then provides a list of specific examples: a consumer's "name, gender, occupation, birth date, identification card number, residential address, contact information, income and financial status, health status, and consumer status". This is only one regulatory definition among several. Definitions provided for other sector specific regulations can be even more broadly stated than this one.

- **"Sensitive Personal Data"**

  There is no definition of "sensitive personal data". However, some sector specific regulations provide special protections of certain personal data, effectively treating them much like "sensitive personal data". These include personal financial information, disease and medical history, status as a hepatitis B carrier, and others.

- **"Processing"**

  There is no definition of "processing", but in practice it may usually include collection, transmission, use, disclosure, storage, disposal, etc.

- **"Data Controller"**

  There is no definition of "data controller", but the existing data protection rules mainly regulate entities which collect and use personal information.

- **"Data Processor"**

  There is no definition of "data processor".

- **"Data Subject"**

  There is no definition of "data subject", but in practice it usually refers to an individual whose personal data is collected, used or processed.

- *Other key definitions – please specify (e.g., "Pseudonymous Data", "Direct Personal Data", "Indirect Personal Data")*
  - **"Pseudonymous Data"**

    There is no definition of "pseudonymous data".
  - **"Direct Personal Data"**

    There is no definition of "direct personal data".
  - **"Indirect Personal Data"**

    There is no definition of "indirect personal data".

3 Key Principles

3.1 What are the key principles that apply to the processing of personal data?

- **Transparency**

  Although no precise principle is established for the processing of personal data, existing sector specific data protection rules often require that the data subject be expressly informed of the purpose, method and scope for collecting and using the personal data. Typically, the consent of the data subject is also required.
- **Lawful basis for processing**

  There is no general requirement to have a lawful basis for processing of personal data. Some existing sector specific data protection rules, however, require that personal information not be illegally or improperly collected, used or transferred.
- **Purpose limitation**

  Existing sector specific data protection rules, when requiring that the data subject must be expressly informed of the purpose, method and scope for collecting and using the personal data, also imply that the collection and use must not exceed the prescribed purpose and scope.
- **Data minimisation**

  Some existing sector specific data protection rules require that unnecessary personal data must not be collected.
- **Proportionality**

  There is no data protection rule concerning this principle.
- **Retention**

  Some existing sector specific data protection rules require: that personal data be kept strictly confidential, and not be disclosed, sold or illegally provided to others; that technical measures be taken to ensure data security and to prevent any data leakage or loss; and that in the event of any occurrence or risk of data leakage or loss, immediate remedial measures be taken.
- *Other key principles – please specify*

  There are no other key principles in particular.

4 Individual Rights

4.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Access to data**

  Some existing sector specific data protection rules explicitly provide that a data subject may access his/her own personal data.
- **Correction and deletion**

  Some existing sector specific data protection rules explicitly provide that a data subject may correct mistake(s) concerning his/her personal data. However, there is no rule which provides a data subject with the right of deletion.
- **Objection to processing**

  There is no precise rule which provides a data subject with the right of objection to processing.
- **Objection to marketing**

  There is no precise rule which provides a data subject with the right to object to his/her personal data being processed for marketing purposes. However, it is clearly provided in the *Consumer Rights Protection Law* that without a consumer's consent or request, or where a consumer explicitly rejects, a company shall not distribute commercial information to the consumer. There is also a regulation imposing rules and restrictions on the use of "spam" emails, as well as short commercial messages.
- **Complaint to relevant data protection authority(ies)**

  There are regulatory authorities which respectively supervise the enforcement of existing sector specific data protection rules. Certain sector specific data protection regulations, such as the *Administrative Provisions on Short Message Services*, establish precise rules on how a data subject may make a complaint to the competent authorities.
- *Other key rights – please specify*

  There are no other key rights in particular.

5 Registration Formalities and Prior Approval

5.1 In what circumstances is registration or notification required to the relevant data protection regulatory authority(ies)? (E.g., general notification requirement, notification required for specific processing activities.)

There are no such circumstances.

5.2 On what basis are registrations/notifications made? (E.g., per legal entity, per processing purpose, per data category, per system or database.)

This is not applicable.

5.3 Who must register with/notify the relevant data protection authority(ies)? (E.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation.)

This is not applicable.

5.4 What information must be included in the registration/notification? (E.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes.)

This is not applicable.

5.5 What are the sanctions for failure to register/notify where required?

This is not applicable.

5.6 What is the fee per registration (if applicable)?

This is not applicable.

5.7 How frequently must registrations/notifications be renewed (if applicable)?

This is not applicable.

5.8 For what types of processing activities is prior approval required from the data protection regulator?

This is not applicable.

5.9 Describe the procedure for obtaining prior approval, and the applicable timeframe.

This is not applicable.

6 Appointment of a Data Protection Officer

6.1 Is the appointment of a Data Protection Officer mandatory or optional?

There is no requirement to appoint a company "Data Protection Officer" as a general matter. In the banking sector, commercial banks are required to appoint a "Chief Information Officer". This position may involve functions that are similar to those of a Data Protection Officer, but it is not chiefly responsible for data protection matters. Companies in the postal and courier services sector are required to appoint a "Security Information Officer". Finally, medical institutions are required to establish a separate department and personnel who would normally also have the responsibilities of a Data Protection Officer.

6.2 What are the sanctions for failing to appoint a mandatory Data Protection Office where required?

This is not applicable.

6.3 What are the advantages of voluntarily appointing a Data Protection Officer (if applicable)?

This is not applicable.

6.4 Please describe any specific qualifications for the Data Protection Officer required by law.

This is not applicable.

6.5 What are the responsibilities of the Data Protection Officer, as required by law or typical in practice?

The responsibilities of a "Chief Information Officer" in a bank are to administer the bank's information technology department and to be responsible for information technology, and also to establish a department to be responsible for IT risk management. A postal or courier services company's "Security Information Officer" is responsible for collecting, reporting and handling security information. A medical institution's department and personnel acting in the role of a "Data Protection Officer" would generally have responsibility for the collection, use and processing of personal medical information.

6.6 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

This is not applicable.

7 Marketing and Cookies

7.1 Please describe any legislative restrictions on the sending of marketing communications by post, telephone, email, or SMS text message. (E.g., requirement to obtain prior opt-in consent or to provide a simple and free means of opt-out.)

Under the *Consumer Rights Protection Law*, without a consumer's consent or request, or where a consumer explicitly rejects, a company may not distribute commercial information to the consumer.

In particular, the *Measures for the Administration of Internet Email Services* require that: (1) emails containing commercial advertisement content may not be sent to recipients without their explicit consent; (2) such commercial advertisement emails must be identified by the words "advertisement" or "AD" in the email's subject field; (3) the identity or origin of the email sender may not be intentionally concealed or forged; (4) the email must provide valid contact methods (including the sender's email address) through which recipients may indicate their refusal of further emails and which should be valid for 30 days; and (5) the sender is required to stop sending such emails when the recipient indicates his/her refusal, unless otherwise agreed by the parties involved.

In addition, the *Administrative Provisions on Short Message Services* requires that if short message service providers and short message content providers request their users to agree to receive short commercial messages, they must explain the types, sending frequencies and sending periods of the short commercial messages which they propose to send. If the users explicitly refuse or fail to give a reply, no further short messages having the same or similar contents may be sent to them. Also, they are required to offer convenient and effective ways to refuse to receive the short messages, and to inform the users of these in the same short messages, and are required not to hinder their users' refusal to receive short messages by any means.

7.2 Is the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

It does not appear to be the case. Not much news on the enforcement of such breaches is reported.

7.3 Are companies required to screen against any "do not contact" list or registry?

There are no such requirements in particular.

7.4 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

Under the *Measures for the Administration of Internet Email Services*, the maximum penalty for sending emails having commercial advertisement content is RMB 30,000.

According to the *Consumer Rights Protection Law*, if a business operator infringes a consumer's rights in connection with his/her personal information, it may be required to make corrections, receive a warning, forfeit related illegal income and be charged a fine of up to 10 times the illegal income (if there is no illegal income, the fine will be up to RMB 500,000). Under the *Administrative Provisions on Short Message Services*, violations of relevant provisions regarding short commercial messages may be penalised with a fine of up to RMB 30,000.

7.5 What types of cookies require explicit opt-in consent, as mandated by law or binding guidance issued by the relevant data protection authority(ies)?

There is no rule which addresses cookies in particular. However, in the context of telecommunications and Internet services, the "user's personal information" includes any information regarding the time and place at which a user uses the telecommunications or Internet service. This may imply protection of a user's location or behavioural tracking information.

7.6 For what types of cookies is implied consent acceptable, under relevant national legislation or binding guidance issued by the relevant data protection authority(ies)?

There is no rule particularly addressing cookies.

7.7 To date, has the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

There is no rule particularly addressing cookies.

7.8 What are the maximum penalties for breaches of applicable cookie restrictions?

There is no rule particularly addressing cookies.

8 Restrictions on International Data Transfers

8.1 Please describe any restrictions on the transfer of personal data abroad?

There are no requirements applicable to cross-border transfers as a general matter. However, there are cross-border transfer restrictions that particularly apply to transfers of personal financial, credit reference and health information to places outside of China.

Under a draft *Cybersecurity Law*, operators of key information infrastructure must store important data, such as personal information, within the territory of China, and cross-border transfer of such important data is allowed when there is an operational requirement, as long as a security assessment has been conducted.

8.2 Please describe the mechanisms companies typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions.

No exemptions are provided to the foregoing restrictions.

8.3 Do transfers of personal data abroad require registration/notification or prior approval from the relevant data protection authority(ies)? Describe which mechanisms require approval or notification, what those steps involve, and how long they take.

No exemptions are provided to the foregoing restrictions. There is no registration/notification requirement applicable to cross-border transfers of personal data.

9 Whistle-blower Hotlines

9.1 What is the permitted scope of corporate whistle-blower hotlines under applicable law or binding guidance issued by the relevant data protection authority(ies)? (E.g., restrictions on the scope of issues that may be reported, the persons who may submit a report, the persons whom a report may concern.)

There is no rule on the use of whistle-blower hotlines.

9.2 Is anonymous reporting strictly prohibited, or strongly discouraged, under applicable law or binding guidance issued by the relevant data protection authority(ies)? If so, how do companies typically address this issue?

There is no rule on this matter.

9.3 Do corporate whistle-blower hotlines require separate registration/notification or prior approval from the relevant data protection authority(ies)? Please explain the process, how long it typically takes, and any available exemptions.

There is no rule on the use of whistle-blower hotlines.

9.4 Do corporate whistle-blower hotlines require a separate privacy notice?

There is no rule on the use of whistle-blower hotlines.

9.5 To what extent do works councils/trade unions/ employee representatives need to be notified or consulted?

There is no rule on the use of whistle-blower hotlines.

10 CCTV and Employee Monitoring

10.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies)?

There is no registration/notification or prior approval requirement on the use of closed circuit television.

10.2 What types of employee monitoring are permitted (if any), and in what circumstances?

In China, there is no specific rule explicitly addressing employee monitoring. However, employee monitoring may be subject to the following restrictions under Chinese law:

(1) In China, an individual is entitled to a constitutional right to dignity, of which a right of privacy is a part.

(2) The *P.R.C. Constitution* also grants an individual the freedom and secrecy of correspondence.

(3) The *Decision on Enhancing Internet Information Protection* provides broad protections for personal electronic data, by way of which employee personal information is protected.

(4) An employer must keep employees' personal data in confidence. The employer must obtain the relevant employee's prior written consent before disclosing the personal data to a third party.

10.3 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

There is no special rule or policy regulating the monitoring of employees. Even so, it would still be prudent to provide employees with notice and obtain the consent of the employees to the implementation of the monitoring programme. In practice, the consent may be obtained by way of an appropriate statement in an employment contract, or a provision in an employee handbook or workplace rules that each employee is required to acknowledge and accept by way of a signature.

10.4 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

There is no requirement to notify or consult with a works council or trade union.

10.5 Does employee monitoring require separate registration/notification or prior approval from the relevant data protection authority(ies)?

There is no registration/notification or prior approval requirement.

11 Processing Data in the Cloud

11.1 Is it permitted to process personal data in the cloud? If so, what specific due diligence must be performed, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

There is no data protection rule specifically concerning personal data in the cloud.

11.2 What specific contractual obligations must be imposed on a processor providing cloud-based services, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

There is no data protection rule specifically concerning data processing by cloud-based services.

12 Big Data and Analytics

12.1 Is the utilisation of big data and analytics permitted? If so, what due diligence is required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

There is no general data protection rule specifically concerning big data and analytics.

13 Data Security and Data Breach

13.1 What data security standards (e.g., encryption) are required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

Certain sector specific data protection rules require a company to take technical measures to ensure data security and prevent any data leakage or loss, and in the event of any occurrence or risk of data leakage or loss, to take immediate remedial measures. However, except in particular sectors, there is usually no detailed and specific rule on what technical measures must be implemented.

For example, the State Administration of Taxation requires a local tax bureau which receives the tax filing data from an individual whose annual income exceeds RMB 120,000 to make sure the data is encrypted during data transfer, and the China Securities Regulatory Commission requires encryption of storage and transfer of usernames and passwords kept in the application system of a securities and futures institution.

In addition to personal tax information, detailed or extensive data security standards have been established for the medical, financial, telecommunications and Internet, and courier services sectors. The *Ninth Amendment to the P.R.C. Criminal Law* also establishes criminal liability for network service providers which fail to perform their obligations to manage the security of information networks as provided by law and administrative regulation. However, more generally stated security standards have been established for numerous other industry sectors.

13.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.

There are no requirements applicable to information security breaches of personal data as a general matter. However, there are specific requirements in relation to the financial, credit reference, Internet service, telecommunications, postal and tax sectors.

Financial institutions are required to establish a system for reporting major safety incidents and risk events arising in the electronic

banking business, and to maintain regular communications with supervisory departments. In situations where the electronic banking system is maliciously damaged, or infected by a virus which results in a breach of confidential information, financial institutions must report to the China Banking Regulatory Commission within 48 hours.

If a serious information leakage accident occurs at a credit reference institution which operates a personal credit information business, at the Basic Database of Financial Credit Information, or at the institution which provides credit information or which makes inquiry with the Database, the administrative authority of the credit information collection sector may take necessary measures such as a temporary takeover in order to mitigate the damages.

In cases where there is any leakage or possible leakage of users' personal information, which has caused or which may cause serious consequences, then the relevant telecommunications business operator or Internet information service provider should report such events to the competent telecommunications regulatory agency.

Any company providing postal services or courier services must report to the relevant postal administration authority within three days, if an employee opens, hides or discards more than 10 pieces of another person's mail without authorisation.

In the event of any incident in which tax-related confidential information is leaked, the relevant tax agency must report such events in a timely manner according to the relevant laws and rules.

13.3 Is there a legal requirement to report data breaches to individuals? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.

There is no such requirement.

13.4 What are the maximum penalties for security breaches?

There is no general data protection rule specifically concerning penalties for security breaches. However, there are specific penalties in relation to certain industry sectors. For example, Internet information services providers which fail to take technical measures to ensure data security may be subject to administrative penalties possibly including a warning and a fine of more than RMB 10,000 and up to RMB 30,000. Network service providers which fail to perform their obligations to manage the security of information networks may be subject to criminal liability, which may include public surveillance, detention or fixed-term imprisonment of up to three years, and/or be fined, and an entity committing such crime may be subject to a fine.

14 Enforcement and Sanctions

14.1 Describe the enforcement powers of the data protection authority(ies):

China does not have a particular data protection authority with specific investigatory power(s).

14.2 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

This is not applicable.

15 E-discovery / Disclosure to Foreign Law Enforcement Agencies

15.1 How do companies within your jurisdiction respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

There is no particular rule on how companies within China may respond to foreign e-discovery requests for disclosure of personal data.

15.2 What guidance has the data protection authority(ies) issued?

There is none.

16 Trends and Developments

16.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

On May 6, 2015, an Intermediate People's Court in Nanjing, Jiangsu Province ruled that the use of cookies by Baidu (a popular Chinese search engine) to personalise advertisements that would be directed at a consumer on third-party websites did not infringe the consumer's right of privacy. However, the judgment was largely based on particularised findings of fact that would likely have been peculiar to this case; therefore, it is not clear whether this ruling will have influence on future cases.

16.2 What "hot topics" are currently a focus for the data protection regulator?

There are two at this time:

(1) Though it remains subject to change before it is finalised and promulgated, the draft *Cybersecurity Law* includes provisions that may push China towards a policy of data localisation.

(2) Certain provisions in the *Anti-Terrorism Law* require telecommunication system operators and Internet service providers to provide technical support and assistance, such as access to their technical interfaces and assistance with decryption, to public security and state security authorities.

Manuel E. Maisog
Hunton & Williams
517–520 South Office Tower
Beijing Kerry Centre, No. 1 Guanghua Road
Chaoyang District
Beijing 100020
China

Tel: *+86 10 5863 7500*
Email: *bmaisog@hunton.com*
URL: *www.hunton.com*

Bing Maisog is the Chief Representative of the firm's office in Beijing, and is a Principal of the Centre for Information Policy Leadership. His practice focuses on data protection and privacy, energy, finance, mergers and acquisitions, and foreign direct investment. Bing frequently advises clients on existing and emerging privacy and data security laws in the Asia-Pacific region, including with respect to the ongoing development of China's developing data protection framework. He graduated with an undergraduate degree in Public and International Affairs from Princeton University, and studied Law at Harvard Law School.

Judy Li
Hunton & Williams
517–520 South Office Tower
Beijing Kerry Centre, No. 1 Guanghua Road
Chaoyang District
Beijing 100020
China

Tel: *+86 10 5863 7500*
Email: *jli@hunton.com*
URL: *www.hunton.com*

Judy Li is an Associate in the firm's office in Beijing. Her experience includes representation of multinational companies, Chinese state-owned companies and investment banks. She advises multinational companies operating in China on all aspects of privacy and data protection compliance governing the collection, use and processing of personal data in China.

HUNTON& WILLIAMS

Hunton & Williams' Global Privacy and Cybersecurity practice is a leader in its field. It has been ranked by *Computerworld* for four consecutive years as the top law firm globally for privacy and data security. *Chambers & Partners* ranks Hunton & Williams as the top privacy and data security practice in its *Chambers & Partners UK*, *Chambers Global* and *Chambers USA* guides.

The team of more than 25 privacy professionals, spanning three continents and five offices, is led by Lisa Sotto, who was named among the *National Law Journal*'s "100 Most Influential Lawyers". With lawyers qualified in six jurisdictions, the team includes internationally-recognised partners Bridget Treacy and Wim Nauwelaerts, former FBI cybersecurity counsel Paul Tiao, and former UK Information Commissioner Richard Thomas.

In addition, the firm's Centre for Information Policy Leadership, led by Bojana Bellamy, collaborates with industry leaders, consumer organisations and government agencies to develop innovative and pragmatic approaches to privacy and information security.

France

Hunton & Williams

Claire François

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The principal data protection legislation is Act No. 78-17 of January 6, 1978 on Information Technology, Data Files and Civil Liberties as amended (*Loi Informatique et Libertés*) (the "**Data Protection Act**" or "**DPA**") and Decree No. 2005-1309 implementing the French DPA. The DPA transposes into French law the requirements of the EU Data Protection Directive (95/46/EC) (the "**Data Protection Directive**") as well as some of the requirements of Directive 2002/58/EC (as amended by Directive 2009/136/EC) (the "**ePrivacy Directive**"). The purpose of the DPA is to ensure that any use of information technology does not violate "human identity, human rights, privacy, or individual or public liberties". The DPA applies to both the public and private sectors.

1.2 Is there any other general legislation that impacts data protection?

The DPA and its implementing Decree are the only legislation explicitly governing data protection. However, some provisions of French Codes may regulate specific issues, e.g., Article L.34-5 of the French Postal and Electronic Communications Code which regulates direct marketing by electronic means.

1.3 Is there any sector specific legislation that impacts data protection?

Other provisions of the French Postal and Electronic Communications Code implement the requirements of the ePrivacy Directive. These requirements impose additional data protection obligations on telecommunications service providers, in addition to the French DPA.

1.4 What is the relevant data protection regulatory authority(ies)?

The *Commission Nationale de l'Informatique et des Libertés* (the "**CNIL**") supervises compliance with the DPA in France. The CNIL's current Chairwoman, elected in September 2011 and re-elected in February 2014, is Isabelle Falque-Pierrotin. The CNIL elects its Chairman or Chairwoman from among its members. The CNIL is an independent administrative body. It does not receive any instructions from any single authority.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **"Personal Data"**

  "Personal Data" means any information relating to an individual who is or can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to him/her. The concept of Personal Data is interpreted broadly and assessed on a case-by-case basis by the CNIL.

- **"Sensitive Personal Data"**

  "Sensitive Personal Data" means Personal Data that reveals, directly or indirectly, the racial and ethnic origins, the political, philosophical, religious opinions or trade union affiliation of individuals, or which concern their health or sexual life.

- **"Processing"**

  "Processing" of Personal Data (or "Data Processing") means any operation or set of operations in relation to such data, whether or not by automated means, especially the collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, deletion or destruction.

- **"Data Controller"**

  The DPA defines the "Data Controller" as a person, public authority, department or any other organisation who determines the purposes and means of the Data Processing.

- **"Data Processor"**

  The DPA defines the "Data Processor" as a person who processes Personal Data on behalf of the Data Controller.

- **"Data Subject"**

  A "Data Subject" is the individual to whom the Personal Data covered by the Processing relate.

- *Other key definitions – please specify (e.g., "Pseudonymous Data", "Direct Personal Data", "Indirect Personal Data")*

  There are no other key definitions in particular.

3 Key Principles

3.1 What are the key principles that apply to the processing of personal data?

- **Transparency**

  Under Article 6(1) of the DPA, Personal Data must be processed fairly and lawfully. Specifically, Data Subjects must be informed by the Data Controller of how their Personal Data will be used.

  When the Data Controller directly collects the Personal Data from Data Subjects, it must provide notice, as a minimum, at the time of collection, of: (i) its identity; (ii) the purpose of the Processing; (iii) whether replies to the questions are compulsory or optional; (iv) the possible consequences for Data Subjects in the absence of a reply; (v) the categories of persons to whom the data are disclosed; (vi) the rights granted to Data Subjects; and (vii) if applicable, information on the transfers of the Personal Data outside of the EU.

- **Lawful basis for processing**

  For Personal Data to be processed lawfully, the Data Controller must have a legal basis for each Processing activity. The DPA sets out legal bases for the Processing of Personal Data in Article 7, and for Sensitive Personal Data in Article 8.

  The legal bases commonly relied upon by French Data Controllers to process Personal Data are: (i) compliance with a legal obligation of the Data Controller; (ii) the performance of a contract to which the Data Subject is a party or steps taken at the request of the Data Subject prior to entering into a contract; and (iii) the pursuit of the legitimate interest of the Data Controller, provided that this is not incompatible with the fundamental rights and freedoms of the Data Subject. In principle, the Processing of Sensitive Personal Data is only permitted with the Data Subject's consent.

- **Purpose limitation**

  Under Article 6(2) of the DPA, Personal Data may only be obtained for specific, explicit and legitimate purposes, and cannot be further processed in any manner incompatible with those purposes.

- **Data minimisation**

  Under Article 6(3) of the DPA, Personal Data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and further processed. Data Controllers are therefore under a duty to process only the Personal Data necessary to achieve the purpose of the Processing, and to not collect or retain unnecessary or irrelevant Personal Data.

- **Proportionality**

  See "Data minimisation".

- **Retention**

  Under Article 6(5) of the DPA, Personal Data must not be retained for longer than is necessary for the purposes for which they are collected and further processed. The CNIL has recommended specific retention periods in its various decisions (such as its Simplified Norms).

- *Other key principles – please specify*

  - **Security**

    Under Article 34 of the DPA, Data Controllers must implement appropriate organisational and technical measures to ensure the security and confidentiality of the Personal Data. As part of this obligation, Article 35 of the DPA requires the Data Controller to conclude a written contract with the Data Processor, specifying the obligations incumbent upon the Data Processor as regards the protection of the security and confidentiality of the data and providing that the Data Processor may act only upon the instruction of the Data Controller.

4 Individual Rights

4.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Access to data**

  Data Subjects have the right to require the Data Controller to: (i) confirm whether it is processing their Personal Data; (ii) provide a description of the Processing (i.e., information on the purposes of the Processing, the categories of Personal Data processed, the persons or categories of persons to whom the data may be disclosed and, if applicable, information on the transfers of Personal Data outside the EU); and (iii) provide a copy of their Personal Data as well as any available information on the origin of the data. Data Subjects may make their requests in writing or on site at the premises of the Data Controller. Data Subjects must provide proof of identity. Data Controllers must respond to the requests within two months (unless the request is manifestly abusive or the data are no longer retained) and may charge a fee for providing a copy of the Personal Data.

- **Correction and deletion**

  Data Subjects have the right to require the Data Controller to, as the case may be, rectify, complete, update, block or delete their Personal Data that are inaccurate, incomplete, equivocal, expired, or whose collection, usage, disclosure or storage is prohibited. The Data Controller also has two months to respond to such requests. At the request of the Data Subjects, the Data Controller must provide confirmation that the corrections or deletions have been made and the Data Controller cannot charge any fee for doing so. If data have been shared with a third party, the Data Controller must ensure that this third party makes the requested corrections/deletions.

- **Objection to processing**

  Data Subjects have the right to object, on legitimate grounds, to the Processing of their Personal Data. Data Subjects must justify their requests and it is up to the Data Controller to assess if the reason invoked by the Data Subject is legitimate.

- **Objection to marketing**

  Data Subjects have the right to object, free of charge, to the Processing of their Personal Data for direct marketing.

- **Complaint to relevant data protection authority(ies)**

  Data Subjects may raise complaints with the CNIL. In 2014, the CNIL received 5,825 complaints. Data Subjects may submit their complaint online on the CNIL's website.

- *Other key rights – please specify*

  - **Consent**

    Data Subjects have further rights in relation to direct marketing and cookies (see section 7 below).

  - **De-listing of search engines' results**

    Data Subjects have the right to request search engines, under certain conditions, to de-list certain links to information affecting their privacy from the results for searches made against their name.

5 Registration Formalities and Prior Approval

5.1 In what circumstances is registration or notification required to the relevant data protection regulatory authority(ies)? (E.g., general notification requirement, notification required for specific processing activities.)

Under the DPA, Data Controllers must register any automated Processing of Personal Data with the CNIL prior to its implementation. Several exemptions exist, e.g., for the Processing carried out by a non-profit organisation or institution with religious, philosophical, political or trade union purposes or for the Processing implemented in accordance with one of the CNIL's exemption decisions (such as for payroll administration or vendor management). Certain types of Data Processing may not benefit from any exemption and require the CNIL's prior approval (see question 5.8 below).

5.2 On what basis are registrations/notifications made? (E.g., per legal entity, per processing purpose, per data category, per system or database.)

Registrations must be submitted for each legal entity acting as a Data Controller and per Processing purpose.

5.3 Who must register with/notify the relevant data protection authority(ies)? (E.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation.)

Organisations subject to the DPA and not benefiting from one of the registration exemptions must register their Data Processing activities with the CNIL. This includes both French legal entities and non-EU legal entities using means or equipment located in France to process Personal Data (except where the Personal Data are in mere transit through the French territory).

5.4 What information must be included in the registration/notification? (E.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes.)

The following information must be included in the CNIL's standard registration (*Déclaration normale*): (i) identity and contact details of the Data Controller or its representative; (ii) department or organisation in charge of implementing the Processing; (iii) purpose of the Processing; (iv) categories of Data Subjects to whom the Processing relates; (v) categories of Personal Data processed, their origin, the data retention period and the categories of recipients (persons/departments/entities) to whom the data may be disclosed; (vi) steps taken to ensure the security of the Personal Data processed; (vii) if applicable, any data transfers to a country outside the EU and details about the transfers; (viii) if applicable, the combination of the Personal Data with other data contained in a different database; (ix) information on how Data Subjects are informed of their data protection rights and on the entity/department where Data Subjects may exercise their rights; (x) contact details of a person whom the CNIL may contact in case of questions; and (xi) identity, email address and function of the signatory of the registration.

5.5 What are the sanctions for failure to register/notify where required?

Failure to register with the CNIL where required is a criminal offence and may lead to up to five years' imprisonment and a fine of up to €300,000 (for individuals) or a fine of up to €1.5 million (if the company is held liable). In addition, the CNIL may impose an administrative sanction (see question 14.1 below).

5.6 What is the fee per registration (if applicable)?

This is not applicable.

5.7 How frequently must registrations/notifications be renewed (if applicable)?

This is not applicable.

5.8 For what types of processing activities is prior approval required from the data protection regulator?

The Processing activities requiring the CNIL's prior approval include:

- the Processing of Sensitive Personal Data if it is in the public interest or if the data are subject, within a short period of time, to an anonymisation procedure approved by the CNIL;
- the Processing of biometric data;
- the Processing of genetic data (except if the Processing is carried out by doctors or biologists for preventive medicine, medical diagnosis or the administration of care or treatment);
- the Processing relating to data containing the social security number (except for organisations which have been authorised to process this number, such as public authorities and employers for HR purposes);
- the Processing of Personal Data including assessments of the social difficulties of individuals;
- the Processing of Personal Data relating to offences, convictions or security measures (except for representatives of the law);
- the Processing of Personal Data which may preclude persons from the benefit of a right, a service or a contract in the absence of any legislative or regulatory provision;
- the combination of databases, each of which was created for a different purpose;
- the Processing of Personal Data for the purpose of medical research;
- the Processing of Personal Data for the purpose of evaluation or analysis of care and prevention practices or activities; and
- transfers of Personal Data to a country outside the EU which does not provide a sufficient level of data protection, where the transfers are based on the European Commission's Standard Contractual Clauses or Binding Corporate Rules ("**BCRs**").

5.9 Describe the procedure for obtaining prior approval, and the applicable timeframe.

A request for approval must be completed and submitted with the CNIL (preferably online on the CNIL's website). The CNIL must issue a decision within two months of receipt of the request. This period may be renewed once. The absence of a decision within this timeframe is considered to be a refusal.

6 Appointment of a Data Protection Officer

6.1 Is the appointment of a Data Protection Officer mandatory or optional?

The appointment of a Data Protection Officer (*Correspondant Informatique et Libertés* or "**CIL**") is optional.

6.2 What are the sanctions for failing to appoint a mandatory Data Protection Officer where required?

This is not applicable.

6.3 What are the advantages of voluntarily appointing a Data Protection Officer (if applicable)?

Organisations that appoint a Data Protection Officer are not required to register their standard Data Processing activities with the CNIL. However, Data Processing activities requiring prior approval must still be registered.

6.4 Please describe any specific qualifications for the Data Protection Officer required by law.

There are no specific qualifications prescribed by law. There is only a general requirement that a Data Protection Officer shall have the qualifications required to perform his/her duties. The Data Protection Officer may be an employee or an external person in organisations with fewer than 50 persons involved in the Processing or having access to the data. The Data Protection Officer should, in principle, be an employee in larger organisations.

6.5 What are the responsibilities of the Data Protection Officer, as required by law or typical in practice?

The responsibilities of the Data Protection Officer prescribed by law include: (i) establishing and keeping a list of the organisation's Data Processing activities for which he/she was appointed; (ii) ensuring compliance with the DPA; (iii) advising the organisation, in particular on any new Data Processing activities to be included on that list, prior to their implementation; (iv) receiving Data Subjects' requests and complaints relating to these Data Processing activities; and (v) submitting an annual report of his/her activities to the organisation and making it available to the CNIL. In practice, typical duties also include: developing internal policies and procedures; conducting compliance checks; preparing (and delivering) staff training; reviewing contractual clauses relating to data protection; advising on appropriate notices to Data Subjects; registering with the CNIL the Data Processing activities subject to prior approval; and generally raising awareness of data protection issues throughout the organisation.

6.6 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

Yes, organisations that appoint a Data Protection Officer must notify the CNIL of the appointment.

7 Marketing and Cookies

7.1 Please describe any legislative restrictions on the sending of marketing communications by post, telephone, email, or SMS text message. (E.g., requirement to obtain prior opt-in consent or to provide a simple and free means of opt-out.)

The sending of marketing communications by post and by live telephone calls requires (i) notice, and (ii) a simple and free means of opting out of receiving marketing communications, at the time of collection of the postal address or telephone number.

The sending of marketing communications by automated recorded calls requires prior opt-in consent. In addition, each telephone recorded message must specify the identity of the advertiser and provide a simple means to opt-out of receiving new marketing communications. This must not result in any additional cost for the individual (e.g., no premium-rate number must be used).

The sending of marketing communications to consumers by email or SMS/MMS requires prior opt-in consent, unless the individual is already an existing customer and the marketing communication relates to similar products or services to those already provided by the advertiser. In addition, each marketing email, SMS or MMS must specify the identity of the advertiser and provide a simple way to opt-out of receiving new marketing communications.

7.2 Is the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

Yes. Recent enforcement actions include a fine of €15,000 imposed in June 2015 on PRISMA MEDIA, the leading press group in France, for various violations of the DPA, including for not obtaining web users' specific and informed consent to receive newsletters and for continuing to send newsletters to users who opted out of receiving them.

7.3 Are companies required to screen against any "do not contact" list or registry?

Yes, companies are required to screen against some "do not contact" lists, e.g., the Robinson list held by the French Direct Marketing Association ("**UFMD**") if they are a member of that association. The Robinson list identifies individuals who do not wish to receive marketing communications by post. The UFMD shares the Robinson list with its members who have committed to respect consumers' objection to receive such marketing communications. Also, as from June 2016, companies that wish to send marketing communications by telephone or SMS will have to screen against a new "do not contact" list managed by the French company, Opposetel. This new list will replace the Pacitel list identifying individuals who do not wish to receive marketing communications by telephone or SMS.

7.4 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

The maximum criminal penalties are five years' imprisonment and a fine of €300,000 (for individuals) or €1.5 million (if the company is held liable). In addition, a fine of €750 may be imposed per marketing communication under the French Postal and Electronic Communications Code, and the CNIL may impose a maximum administrative fine of €300,000.

7.5 What types of cookies require explicit opt-in consent, as mandated by law or binding guidance issued by the relevant data protection authority(ies)?

Cookies and similar technologies require notice and prior opt-in consent, except where the cookie or similar technology is exclusively intended to enable or facilitate electronic communications or is strictly necessary for the provision of an online communication service as expressly requested by the user. Web analytics cookies may also qualify for an exemption from the consent requirement but under strict conditions. The law does not stipulate different types of consent for different types of cookies. Where consent is required, consent must be freely given, specific and informed. The CNIL considers that consent must result from a positive action of the user and may be implied (see question 7.6 below).

7.6 For what types of cookies is implied consent acceptable, under relevant national legislation or binding guidance issued by the relevant data protection authority(ies)?

In December 2013, the CNIL issued a new Recommendation and a set of FAQs providing guidance on how to obtain consent for the use of cookies and similar technologies. The CNIL recommends obtaining consent using a two-stage approach, which suggests that consent may be implied under the DPA for all types of cookies subject to the consent requirement.

7.7 To date, has the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

Yes. In January 2014, the CNIL imposed a fine of €150,000 on Google Inc. for not complying with French data protection requirements, including the obligation to obtain the user's consent before placing cookies on their terminal device. In January 2016, the CNIL issued formal notice to Facebook to comply with that obligation within three months.

7.8 What are the maximum penalties for breaches of applicable cookie restrictions?

The maximum penalty is €300,000.

8 Restrictions on International Data Transfers

8.1 Please describe any restrictions on the transfer of personal data abroad?

Transfers of Personal Data from France to a country outside the EU are prohibited, unless that country ensures a sufficient level of data protection. A "transfer" includes the ability to access data from outside the EU, e.g., viewing it on a computer screen from another country.

8.2 Please describe the mechanisms companies typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions.

Typically, Personal Data may be transferred to a country outside the EU if: (i) the law of that country has been recognised by the European Commission as providing a sufficient level of data protection; (ii) the data exporter adduces sufficient safeguards by signing the European Commission' Standard Contractual Clauses or adopting BCRs; or (iii) a relevant derogation applies, including the express consent of the Data Subject. The CNIL considers that derogations can only be used on an exceptional and specific basis and not for frequent or large transfers of Personal Data.

8.3 Do transfers of personal data abroad require registration/notification or prior approval from the relevant data protection authority(ies)? Describe which mechanisms require approval or notification, what those steps involve, and how long they take.

Transfers of Personal Data outside the EU must be registered with the CNIL but do not require a separate registration: Data Controllers only need to complete the section on data transfers of the registration form. In addition to registration, transfers of Personal Data based on the European Commission's Standard Contractual Clauses or BCRs require the CNIL's prior approval. In such cases, the CNIL must issue its decision (authorising or not authorising the transfers) within two months. In 2015, the CNIL implemented a new procedure to facilitate registration requirements for data transfers based on BCRs. According to this new procedure, the CNIL will issue a single authorisation decision to each group that has implemented BCRs and wishes to participate in that procedure. The group's French affiliates bound by BCRs will then need to submit a simplified registration covering all their data transfers based on BCRs. They will no longer have to obtain the CNIL's prior approval for each of these data transfers.

9 Whistle-blower Hotlines

9.1 What is the permitted scope of corporate whistle-blower hotlines under applicable law or binding guidance issued by the relevant data protection authority(ies)? (E.g., restrictions on the scope of issues that may be reported, the persons who may submit a report, the persons whom a report may concern.)

The CNIL considers that corporate whistle-blower hotlines are internal reporting mechanisms, which must be limited in scope. The CNIL has issued a decision called Single Authorisation AU-004 laying down specific requirements for corporate whistle-blower hotlines that only allow reports in the following areas: (i) finance, accounting, banking and anti-corruption; (ii) anti-competitive practices; (iii) fight against discrimination and harassment in the workplace; (iv) health, hygiene and safety in the workplace; and (v) protection of the environment.

9.2 Is anonymous reporting strictly prohibited, or strongly discouraged, under applicable law or binding guidance issued by the relevant data protection authority(ies)? If so, how do companies typically address this issue?

Anonymous reporting is discouraged. The CNIL's Single Authorisation AU-004 emphasises that whistle-blowers must identify themselves and that anonymous reports may only be processed exceptionally and subject to conditions. Companies typically inform their employees located in France that they should give their names when submitting a report through the hotline.

9.3 Do corporate whistle-blower hotlines require separate registration/notification or prior approval from the relevant data protection authority(ies)? Please explain the process, how long it typically takes, and any available exemptions.

As a rule, corporate whistle-blower hotlines require the CNIL's prior approval. The CNIL must issue its decision within two months. However, if the corporate whistle-blower hotline complies with all the requirements of the CNIL's Single Authorisation AU-004, only a prior simplified registration needs to be filed with the CNIL. In this case, the corporate whistle-blower hotline can be implemented as soon as the company has received a receipt from the CNIL.

9.4 Do corporate whistle-blower hotlines require a separate privacy notice?

Companies operating a whistle-blower hotline are required to provide Data Subjects with clear and complete information about the Processing of their Personal Data through the hotline. The DPA or the CNIL's Single Authorisation AU-004 does not specify how this information must be provided. However, in practice, companies typically provide a separate privacy notice to comply with the notice requirement.

9.5 To what extent do works councils/trade unions/ employee representatives need to be notified or consulted?

The French Labour Code requires to inform and consult works councils before implementing a whistle-blower hotline. Committees on hygiene, safety and working conditions ("**CHSCT**") should also be consulted, according to some Court decisions.

10 CCTV and Employee Monitoring

10.1 Does the use of CCTV require separate registration/ notification or prior approval from the relevant data protection authority(ies)?

The use of CCTV requires separate registration with the CNIL if CCTV records a place not open to the public (such as storage areas, areas dedicated to staff members, etc.). If CCTV records a place open to the public (entrance and exit areas for the public, sales counters, etc.), the use of CCTV must be approved by the prefect of the French department concerned.

10.2 What types of employee monitoring are permitted (if any), and in what circumstances?

Employers may control and limit the use of Internet and company emails for the purpose of ensuring network security and limiting risks of abuse of a too personal use of Internet and company emails. Employers may have access to professional emails of an employee and review the websites visited by him or her, even if the employee is not present. However, employers may not freely consult emails that employees have clearly identified as "private" or "personal", even if the private use of professional IT tools has been strictly forbidden.

An employer may also listen to or record employee telephone calls, e.g., for training, performance or quality purposes. However, such listening/recording should not be permanent and employees should be able to disconnect the recording function to receive or make private calls.

Further, employers may install GPS in company vehicles for limited purposes, and incidentally, for monitoring working time, when this cannot be achieved by other means. However, GPS may not be used to monitor compliance with speed restrictions and to permanently monitor an employee.

10.3 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Consent is generally not considered valid in an employment context. However, notice is required. Each individual employee must be provided notice by any appropriate written means, such as IT guidelines, individual mail, a clause in the employment contract, etc.

10.4 To what extent do works councils/trade unions/ employee representatives need to be notified or consulted?

Employee representatives must be consulted before implementing monitoring technologies.

10.5 Does employee monitoring require separate registration/notification or prior approval from the relevant data protection authority(ies)?

In most cases, employee monitoring requires separate registration.

11 Processing Data in the Cloud

11.1 Is it permitted to process personal data in the cloud? If so, what specific due diligence must be performed, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

Processing Personal Data in the cloud is permitted. In June 2012, the CNIL published practical recommendations for companies that consider using cloud computing services, such as the need to conduct proper risk assessments in order to define the security measures to be required from the cloud provider or to be implemented within the company, the need to identify which type of cloud computing services is relevant for the Processing envisaged, the need to review internal security policies and procedures, etc. The CNIL has also suggested some model contractual clauses, which can be included in cloud computing agreements.

11.2 What specific contractual obligations must be imposed on a processor providing cloud-based services, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

There are no specific contractual obligations under the DPA that must be imposed on Data Processors providing cloud-based services, in addition to the general contractual obligations (see question 3.1 above). The CNIL has suggested some specific model contractual clauses but their use is not mandatory.

12 Big Data and Analytics

12.1 Is the utilisation of big data and analytics permitted? If so, what due diligence is required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

The utilisation of big data and analytics is a reality, and the CNIL is considering the privacy challenges associated with big data and how the principles of the DPA (see question 3.1 above) may apply in this context.

13 Data Security and Data Breach

13.1 What data security standards (e.g., encryption) are required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

The DPA requires Data Controllers to "take all useful precautions, with regard to the nature of the data and the risks of the Processing, to preserve the security of the data". Specific standards are not stipulated by law or binding guidance. However, the CNIL has published a set of non-binding guides to help Data Controllers to choose the appropriate organisational and technical measures to protect Personal Data.

13.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.

There is no general legal requirement to report data breaches to the CNIL under the DPA. The DPA only requires providers of publicly available electronic communications services to report data breaches to the CNIL. The service providers must notify the CNIL of any data breaches within 24 hours following their detection by completing a specific notification form available on the CNIL's website. If the service providers do not have all the information required to complete the form, they may make an initial notification to the CNIL within 24 hours following the detection of the breach and then a supplementary notification within three days following the initial notification.

13.3 Is there a legal requirement to report data breaches to individuals? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.

Only providers of publicly available electronic communications services are required under the DPA to notify individuals of a data breach. This requirement applies when the breach is likely to adversely affect individuals' Personal Data or privacy. In this case, the service providers should notify the affected individuals without delay. However, telecommunications service providers do not have to notify the affected individuals when the CNIL has found that the service providers implemented appropriate technical security measures prior to the data breach. The CNIL has two months to make this assessment. In the absence of any feedback from the CNIL after that period, the service providers must immediately inform the affected individuals if they have not already done so. The CNIL expects other Data Controllers to notify individuals of data breaches that may adversely affect them.

13.4 What are the maximum penalties for security breaches?

The maximum criminal penalties are five years' imprisonment and a fine of €300,000 (for individuals) or €1.5 million (if the company is held liable). In addition, the CNIL may impose a maximum administrative fine of €300,000.

14 Enforcement and Sanctions

14.1 Describe the enforcement powers of the data protection authority(ies):

Investigatory Power	Civil/ Administrative Sanction	Criminal Sanction
In May 2015, the CNIL announced that it planned to conduct approximately 550 inspections in 2015 (compared to 421 inspections conducted in 2014). The CNIL can conduct four types of investigations: ■ **On-site inspections** On this occasion, the CNIL may have access to any materials (servers, computers, applications, etc.) in which Personal Data is stored. This type of inspection currently represents the vast majority of inspections conducted by the CNIL. ■ **Documentary inspections** These inspections allow the CNIL to obtain disclosure of documents or files upon written request. ■ **Hearing inspections** These inspections consist of summoning representatives of organisations to appear at the CNIL in order to obtain any necessary information. ■ **Online inspections** Since March 2014, the CNIL may also remotely establish violations of the DPA. Two hundred online inspections were planned for 2015.	In the case of violations of the DPA, the CNIL may impose an administrative sanction, including: (i) a warning; (ii) a fine of up to €150,000 (or up to €300,000 in the case of a repeated breach within five years) if the CNIL served formal notice on the Data Controller to cease its non-compliance within a given deadline and the Data Controller did not comply with the notice served; (iii) an injunction to cease the Processing; or (iv) a withdrawal of the authorisation granted. The CNIL may make its sanction public by publishing it on its website and ordering its publication in French journals, newspapers or other media.	In addition, the CNIL may refer the case to the French public prosecutor, or a Data Subject may raise a criminal complaint and a French judge may impose a criminal sanction, which may lead to up to five years' imprisonment and a fine of up to €300,000 (for individuals) or a fine of up to €1.5 million (if the company is held liable).

14.2 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

The CNIL is regarded as being an active regulator. Nevertheless, the CNIL usually issues a warning or serves formal notice on the Data Controller to cease its non-compliance within a given deadline. The CNIL imposes a fine only if the Data Controller does not comply with the notice served within this deadline.

Examples of recent enforcement action brought by the CNIL:

- In January 2014, Google Inc. was fined €150,000 for various violations of the DPA (such as the failure to provide complete notice to Data Subjects). This is the highest fine imposed by the CNIL to date.
- In August 2014, the CNIL issued a public warning against the French telecommunications service provider, Orange, for having failed to ensure the security and confidentiality of its customers' Personal Data. In April 2014, Orange notified the CNIL of a data security breach due to a technical failure of one of its Data Processors. Orange was sanctioned in particular for not having carried out a security audit of the application specifically developed by the Data Processor, prior to using that application.
- In November 2015, the CNIL imposed a fine of €50,000 on Optical Center, a distributor of optical products, for violations related to the security and confidentiality of its customers' Personal Data.

15 E-discovery / Disclosure to Foreign Law Enforcement Agencies

15.1 How do companies within your jurisdiction respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

The collection and transfer of Personal Data are both Processing activities subject to the key data protection principles set out in the DPA (see question 3.1 above). Companies typically must:

- ensure that they have a legal basis to process the Personal Data (typically, companies rely on their legitimate interest to process the data; however, in the context of discovery, this requires the data to be processed in accordance with the Hague Convention and the French Blocking Statute);
- ensure that only the necessary Personal Data are processed, e.g., by using a filtering mechanism in France;
- provide notice to Data Subjects at the time of recording their data;
- ensure that the Personal Data are processed in compliance with general obligations of secrecy and confidentiality and only retained for the duration of the investigation/proceeding; and
- ensure that their existing registrations with the CNIL reflect the transfer of Personal Data and that they have an appropriate data transfer mechanism in place (see question 8.2 above).

15.2 What guidance has the data protection authority(ies) issued?

In July 2009, the CNIL issued guidance on the transfer of Personal Data in the context of discovery proceedings. The guidance reflects the key data protection principles set out in the DPA (see question 3.1 above) which a Data Controller must adhere to when processing Personal Data in the context of discovery.

16 Trends and Developments

16.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

In March 2014, the CNIL's investigative powers were strengthened to allow the CNIL to identify remotely, from a computer connected to the Internet, violations of the DPA. As a result, the number of inspections carried out by the CNIL has recently increased. In most cases, however, no sanction is imposed as organisations remedy the situation by complying with the DPA. Over the past 12 months, the French Supreme Court has also issued important rulings. In particular, the French Supreme Court confirmed that an employer can read SMS messages sent or received by employees on company-issued devices, without the employees being present, unless such SMS messages have been identified as private.

16.2 What "hot topics" are currently a focus for the data protection regulator?

Ensuring compliance of transatlantic data flows with the DPA is definitively an area of focus for the CNIL. In November 2015, the CNIL sent an email to organisations that have registered data transfers to the U.S. based on the Safe Harbour Principles, inviting them to implement the European Commission's Standard Contractual Clauses and update their registrations by the end of January 2016. The CNIL is currently analysing, within the Article 29 Working Party, the level of protection afforded by the new EU-U.S. arrangement known as the "Privacy Shield". Preparing organisations for their new obligations under the future EU General Data Protection Regulation constitutes another area of focus for the CNIL. In this respect, the CNIL already published in July 2015 new guides for carrying out Privacy Impact Assessments ("**PIAs**") to help Data Controllers to implement the principle of "Privacy by design".

Claire François
Hunton & Williams
Park Atrium
Rue des Colonies 11
1000 Brussels
Belgium

Tel: +32 2 643 58 00
Email: cfrancois@hunton.com
URL: www.hunton.com

Claire is a French qualified lawyer and advises a broad spectrum of clients on EU and French data protection and cybersecurity matters, including implementation of global data management strategies, international data transfers, and local data compliance. Claire also regularly represents clients before the French Data Protection Authority.

HUNTON& WILLIAMS

Hunton & Williams' Global Privacy and Cybersecurity practice is a leader in its field. It has been ranked by *Computerworld* for four consecutive years as the top law firm globally for privacy and data security. *Chambers & Partners* ranks Hunton & Williams as the top privacy and data security practice in its *Chambers & Partners UK*, *Chambers Global* and *Chambers USA* guides.

The team of more than 25 privacy professionals, spanning three continents and five offices, is led by Lisa Sotto, who was named among the *National Law Journal*'s "100 Most Influential Lawyers". With lawyers qualified in six jurisdictions, the team includes internationally-recognised partners Bridget Treacy and Wim Nauwelaerts, former FBI cybersecurity counsel Paul Tiao, and former UK Information Commissioner Richard Thomas.

In addition, the firm's Centre for Information Policy Leadership, led by Bojana Bellamy, collaborates with industry leaders, consumer organisations and government agencies to develop innovative and pragmatic approaches to privacy and information security.

Germany

Hunton & Williams

Anna Pateraki

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The principal data protection legislation is the Federal Data Protection Act (*Bundesdatenschutzgesetz*) (the "**FDPA**"), which was last amended in 2009 and implements into German law the requirements of the EU Data Protection Directive (95/46/EC) (the "**Data Protection Directive**"). Where no other law is referred to, references in the following responses to "sections" are references to sections of the FDPA.

1.2 Is there any other general legislation that impacts data protection?

The 16 German federal states have state-level data protection laws. These laws only apply to the public sector in the relevant state.

1.3 Is there any sector specific legislation that impacts data protection?

The Telecommunications Act (*Telekommunikationsgesetz*) contains sector specific data protection provisions that apply to telecommunications services providers such as internet access providers. The Telemedia Act (*Telemediengesetz*) also contains sector specific data protection provisions that apply to telemedia service providers such as website providers.

Specific rules for online marketing (email, SMS, MMS) are set out in the Unfair Competition Act (*Gesetz gegen den unlauteren Wettbewerb*).

1.4 What is the relevant data protection regulatory authority(ies)?

There are 17 state data protection authorities which oversee and enforce private and public sector data protection compliance of entities established in their state. The federal data protection commissioner (*Bundesdatenschutzbeauftragter*) oversees and enforces data protection compliance within the federal public sector (e.g., federal ministries) as well as certain parts of the postal services and telecommunications services providers' activities.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **"Personal Data"**

  "Personal data" means any information concerning the personal or material circumstances of an identified or identifiable natural person.

- **"Sensitive Personal Data"**

  More commonly known as "special categories of personal data", which refers to information on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life.

- **"Processing"**

  "Processing" means the recording, alteration, transfer, blocking and erasure of personal data. Specifically, irrespective of the procedures applied:

  1. "recording" means the entry, recording or preservation of personal data on a storage medium in order that they can be further processed or used;
  2. "alteration" means the modification of the substance of recorded personal data;
  3. "transfer" means the disclosure of personal data recorded or obtained by data processing to a third party either a) through transfer of the data to a third party, or b) by the third party inspecting or retrieving data available for inspection or retrieval;
  4. "blocking" means the identification of recorded personal data in order to restrict their further processing or use; and
  5. "erasure" means the deletion of recorded personal data.

- **"Data Controller"**

  "Data controller" means any person or body which collects, processes or uses personal data on his, her or its own behalf, or which commissions others to do the same.

- **"Data Processor"**

  The FDPA uses the term "data processor" without explicitly defining it. The closest to a formal definition is section 11 (1), sentence 1 which reads: "If other bodies collect, process or use personal data on behalf of the controller, the controller shall be responsible for compliance with the provisions of this Act and other data protection provisions."

- **"Data Subject"**

  "Data subject" means an identified or identifiable natural person.

- *Other key definitions – please specify (e.g., "Pseudonymous Data", "Direct Personal Data", "Indirect Personal Data")*
  - **"Pseudonymous Data"**

    "Pseudonymous data" is not defined. However, "pseudonymising" means replacing the data subject's name and other identifying features with another identifier in order to make it impossible or extremely difficult to identify the data subject.
  - **"Direct Personal Data"**

    "Direct personal data" is not defined.
  - **"Indirect Personal Data"**

    "Indirect personal data" is not defined.
  - **"Anonymising"**

    "Anonymising" means the alteration of personal data so that information concerning personal or material circumstances cannot be attributed to an identified or identifiable natural person, or so that such an attempt at attribution would require a disproportionate amount of time, expense and effort.

3 Key Principles

3.1 What are the key principles that apply to the processing of personal data?

- **Transparency**

  There are two transparency requirements enshrined in the FDPA. The first is set out in section 4 (2). This section states that personal data must be collected directly from the data subject and they may only be collected without the data subject's involvement if it is legally required or if, broadly, the processing purpose necessitates an indirect collection and this indirect collection passes the balancing of interests test.

  The second transparency requirement is that the data subject be informed about the collection and processing of personal data relating to him or her.

  Where personal data are collected from the data subject, section 4 (3) requires that, if the data subject is not already aware of it, the data controller inform him/her/it as to: (i) the identity of the controller; (ii) the purposes of collection, processing or use; and (iii) the categories of recipients, if the data subject has no expectation that his/her/its data will be transferred to such recipients in the particular case.

  Where personal data are stored without the data subject's knowledge, section 33 (1) requires that the data subject be informed of the type of data, the purpose of the collection, processing or use, the identity of the data controller and the categories of recipients, if the data subject has no expectation that his/her/its data will be transferred to such recipients in the particular case.
- **Lawful basis for processing**

  Section 4 (1) states that the collection, processing and use of personal data is only lawful if the FDPA or another law permits or requires it, or if the data subject has consented.

  The main legal bases set out in the FDPA are: section 28 (data collection and storage for own commercial purposes); section 32 (data collection, processing and use for employment purposes); section 4 (1) and 4a (consent); and section 29 (commercial data collection and storage for transfer purposes).
- **Purpose limitation**

  Where personal data is processed on the basis of section 28 (data collection and storage for own commercial purposes), the purpose of the data processing and use must be determined at the time of collection. Section 28 (2) permits a change of purpose if it passes the balancing of interests test, the personal data are publicly available, it is required to safeguard a third party's lawful interests, it is required to guard against dangers to the state or public, or it is for research purposes which clearly outweigh the data subject's legitimate interests.

  Personal data can be processed on the basis of section 32 (employment purposes) only if this is necessary for hiring decisions or, after hiring, for carrying out or terminating the employment contract. Employees' personal data may be processed to detect crimes only if there is a documented reason to believe the data subject has committed a crime while employed and the processing is necessary to investigate the crime following a balancing of interests test.
- **Data minimisation**

  Section 3a sets out the principles of data minimisation and data economy. The section states that as little personal data as possible should be collected, processed and used, and data processing systems should be chosen and organised accordingly. Further, personal data should be anonymised or pseudonymised if and when the purpose for which they are processed allows it and provided that the effort involved here is not disproportionate.
- **Proportionality**

  The proportionality principle is reflected throughout the FDPA. It is used both where particular operations *vis-à-vis* personal data are concerned (e.g., when personal data should be anonymised (section 3a)) as well as in the form of the balancing of interests test to determine whether a particular legal basis applies (e.g., section 28).
- **Retention**

  Section 35 (2) No. 3 states that personal data that are processed for the data controller's own purposes must be deleted when they are no longer required for the purpose for which they are stored. If personal data are stored for commercial transfer purposes, their continued storage must be evaluated every three or four years to determine whether they are still needed.
- *Other key principles – please specify*

  There are no other key principles in particular.

4 Individual Rights

4.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Access to data**

  The data subject's right of access is mainly set out in section 34 and concerns access to information about: (1) recorded data relating to them, including information relating to the source of the data; (2) the recipients or categories of recipients to which the data are transferred; and (3) the purpose of recording the data.

  Data subjects have to be specific about the type of personal data about which information is to be given. Where the personal data are stored for commercial transfer purposes, the data subject must be provided with information about the personal data's source and recipients, even where such details are not recorded. The latter information can be withheld, though, if the interest in safeguarding trade secrets outweighs the data subject's interest in being provided with the information.

  More detailed provisions apply where scoring (e.g., credit scores calculated by credit reference agencies) and commercial data transfers are concerned.

  Information should be provided in writing and free of charge, unless any of the exemptions set out in section 34 apply.

- **Correction and deletion**

  The data subject's rights of correction, deletion and blocking are codified in section 35. Personal data must be corrected if they are inaccurate. They can be deleted at any time unless certain exemptions apply and they must be deleted if: (a) their storage would be unlawful; (b) they concern racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life, or criminal or administrative offences the accuracy of which the data controller cannot prove; (c) they are processed for own purposes and they are no longer required for the purpose for which they are stored; or (d) they are processed for commercial transfer purposes and their retention is no longer required.

  In certain circumstances, personal data must be blocked instead of deleted.

- **Objection to processing**

  The data subject's general right to object to the processing of his/her/its personal data is set out in section 35 (5). This section states that personal data must not be collected, processed or used if the data subject has objected and if an evaluation of the data subject's specific personal circumstances shows that his/her/its legitimate interests outweigh the data controller's legitimate interests in collecting, processing or using his/her/its personal data.

  In addition to this general right to object, the FDPA contains more specific rights to object to certain types of processing.

- **Objection to marketing**

  Section 28 (4) of the FDPA states that if the data subject has objected to the processing of his/her/its personal data for marketing purposes or for the purposes of market or opinion research, then the personal data must not be processed or used for these purposes.

  Section 7 (1) of the Unfair Competition Act states that sending advertisements to a recipient who clearly does not wish to receive advertisements is unlawful.

  In an online context, section 15 (3) of the Telemedia Act states that telemedia service providers may only use pseudonymised usage profiles for marketing purposes if the user has not objected. The user must be specifically informed about his/her right to object.

- **Complaint to relevant data protection authority(ies)**

  The FDPA does not formalise a complaints procedure. However, it is common for data subjects to contact the relevant data protection authority and for the data protection authority to then investigate the complaint.

- *Other key rights – please specify*

  There are no other key rights in particular.

5 Registration Formalities and Prior Approval

5.1 In what circumstances is registration or notification required to the relevant data protection regulatory authority(ies)? (E.g., general notification requirement, notification required for specific processing activities.)

Although there is a general requirement in section 4 to notify the relevant data protection authority of the automated processing of personal data, in practice such notification is the exception rather than the rule. The reason is that the general notification requirement does not apply if the data controller has appointed a Data Protection Officer who has the obligation to maintain data protection inventories. It also does not apply if only up to nine staff process personal data for the data controller's own purposes on the basis of consent or for the purpose of the creation, performance of termination of a contractual or quasi-contractual relationship with the data subject.

Nonetheless, a notification is always required if personal data are processed: (a) for commercial transfer purposes (e.g., for address-selling businesses); (b) for anonymised commercial transfer purposes; or (c) for market and opinion research purposes.

5.2 On what basis are registrations/notifications made? (E.g., per legal entity, per processing purpose, per data category, per system or database.)

Each automated processing operation is covered by the notification obligation where this applies.

5.3 Who must register with/notify the relevant data protection authority(ies)? (E.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation.)

All entities to whom German data protection law applies and who cannot avail themselves of either of the exceptions to the general duty to notify must file notifications with the relevant data protection authority. This may include foreign legal entities as well as their German representative or branch offices.

Whether German data protection law applies is determined under section 1.

5.4 What information must be included in the registration/notification? (E.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes.)

Where a notification must be filed, the content of the notification is prescribed in section 4e as:

- name or company name of the data controller;
- owners, management boards, managing directors or other company leaders appointed by law or by the company's regulations, and the persons in charge of data processing;
- the data controller's address;
- the purposes of the data collection, processing or use;
- a description of categories of data subjects and the data or categories of data relating to them;
- the recipients or categories of recipients to whom the data can be disclosed;
- standard retention periods for the data;
- intended transfers of the data to third countries; and
- a general description allowing a preliminary assessment of whether the security measures implemented in accordance with section 9 are appropriate.

5.5 What are the sanctions for failure to register/notify where required?

The sanction for failure to register/notify where required is €50,000 (sections 43(3) and (1) No. 1).

5.6 What is the fee per registration (if applicable)?

Generally, there is no notification fee.

5.7 How frequently must registrations/notifications be renewed (if applicable)?

The notifications must be updated before the data processing is changed as well as before its termination (section 4e).

5.8 For what types of processing activities is prior approval required from the data protection regulator?

Section 4d (5) requires that if automated processing operations are particularly risky for the rights and freedoms of the data subjects, then they must be analysed before any processing starts. This analysis or "prior checking" will be required especially where sensitive personal data are processed or where the processing is intended to evaluate the data subject's personality, performance or behaviour. It is, however, not required where the processing is required by law, required for the creation, performance of termination of a contractual or quasi-contractual relationship with the data subject or where the data subject has consented.

5.9 Describe the procedure for obtaining prior approval, and the applicable timeframe.

The data controller's Data Protection Officer is responsible for carrying out the prior checking. He/she must carry out the prior checking after having received an overview of the relevant processing operation from the data controller and can involve the relevant data protection authority as required (section 4d (6)).

6 Appointment of a Data Protection Officer

6.1 Is the appointment of a Data Protection Officer mandatory or optional?

There is a general requirement in section 4f (1) to appoint a Data Protection Officer ("**DPO**"). However, this general notification requirement does not apply if only nine members of staff or fewer process personal data regularly.

Nonetheless, a DPO will always have to be appointed if the entity in question uses automated means to processes personal data that are subject to prior checking or for the purposes of commercial data transfer, anonymised commercial transfer or market or opinion research.

6.2 What are the sanctions for failing to appoint a mandatory Data Protection Officer where required?

The relevant entity may be fined up to €50,000 and the relevant data protection authority may order it to appoint a Data Protection Officer.

6.3 What are the advantages of voluntarily appointing a Data Protection Officer (if applicable)?

The majority of businesses in Germany will already have to appoint a DPO by law; therefore, voluntary appointments of DPOs are rare.

6.4 Please describe any specific qualifications for the Data Protection Officer required by law.

The DPO must possess the necessary expertise and reliability in order to fulfil his/her responsibilities (section 4f (2)). The German data protection authorities issued more detailed guidance (dated November 4–5, 2010) on what level of qualification and expertise is typically expected. According to this guidance, all DPOs should have:

- basic knowledge of the personality rights granted by the German Constitution to the customers and employees of the data controller; and
- comprehensive knowledge of the FDPA, including technical (e.g., data security measures) and organisational (e.g., concepts of availability, authenticity and integrity of data) rules.

Additional areas of expertise will be required depending on the data controller's size, industry sector, IT infrastructure and sensitivity of the personal data processed.

Furthermore, the Data Protection Officer must be independent within the company and report directly to German management.

6.5 What are the responsibilities of the Data Protection Officer, as required by law or typical in practice?

The DPO must work towards compliance with the FDPA and other data protection provisions (e.g., data protection provisions in the Telemedia Act). In particular, the FDPA requires the DPO to undertake the following tasks:

- Monitor how data processing software is used to process personal data and verify that the processing is compliant with relevant data protection provisions.
- Take appropriate measures to educate and train individuals processing personal data about the provisions of the FDPA and other relevant data protection provisions.
- If the company is not required to notify its processing to the DPA, the DPO must provide the public data processing inventory to those who request it. The company must provide the DPO with the data inventory.
- Where a prior checking is required, the DPO is responsible for carrying it out.

6.6 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

No, this is not the case.

7 Marketing and Cookies

7.1 Please describe any legislative restrictions on the sending of marketing communications by post, telephone, email, or SMS text message. (E.g., requirement to obtain prior opt-in consent or to provide a simple and free means of opt-out.)

The Unfair Competition Act generally requires the recipient's consent if marketing messages are sent to him/her by phone, SMS, fax or email. However, there are exceptions. As regards email, for example, section 7(3) of the Unfair Competition Act allows marketing emails to be sent without the recipient's consent (therefore opt-out is sufficient) where the following conditions are met cumulatively:

- the company obtained the recipient's email address from the recipient in connection with the sale of a good or a service;
- the company uses the email address to advertise directly for similar and own goods or services;
- the recipient has not objected to such use; and
- at the time the email address is collected as well as each time it is used, the recipient is informed clearly and unambiguously that he/she can object to such use at any time without incurring transmission costs which exceed the basic transmission tariffs.

For certain types of marketing activities (e.g., marketing list data), more detailed regulations apply (e.g., section 28 (3)).

7.2 Is the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

Yes. Enforcement action, as well as litigation concerning breaches of marketing restrictions, is frequent in Germany.

7.3 Are companies required to screen against any "do not contact" list or registry?

There is no obligation to screen against "do not contact" lists as explicit consent is required in most cases.

7.4 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

Breaches of the Unfair Competition Act's marketing restrictions can result in fines of up to €300,000 (section 20 (2) of the Unfair Competition Act).

7.5 What types of cookies require explicit opt-in consent, as mandated by law or binding guidance issued by the relevant data protection authority(ies)?

There are currently conflicting interpretations of the applicable law. The German government's position is that only those cookies that are strictly necessary for the user to receive telemedia services (e.g., to view a website) can be used without the user's prior opt-in consent. The German government's position is outlined in a communication to the European Commission (COCOM11-20) dated October 4, 2011 and relies on section 15 (1) of the Telemedia Act.

The German data protection authorities, however, issued a resolution dated February 5, 2015 in which they request the German government to implement the requirement of the e-Privacy Directive (Article 5 (3)) for opt-in consent for cookies.

7.6 For what types of cookies is implied consent acceptable, under relevant national legislation or binding guidance issued by the relevant data protection authority(ies)?

Please refer to the answer above. The position is currently not settled in Germany.

7.7 To date, has the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

The Bavarian Data Protection Authority ("**DPA**") has analysed various web analytics tools in detail and made recommendations on how such tools can be used in a compliant manner. Cookies and opt-out methods played a central role in these analyses.

7.8 What are the maximum penalties for breaches of applicable cookie restrictions?

Breaches of the relevant provisions of the FDPA could result in fines of up to €300,000. Breaches of the relevant provisions of the Telemedia Act could result in fines of up to €50,000.

8 Restrictions on International Data Transfers

8.1 Please describe any restrictions on the transfer of personal data abroad?

International transfers of personal data subject to German law must pass a two-stage test. The first stage is whether there is a legal basis for transferring the personal data to a third party since there is no privilege for sharing data within a group of companies. The second stage is whether the personal data will be afforded an adequate level of protection in the country to which they are transferred (section 4b) or whether an exception applies (section 4c).

8.2 Please describe the mechanisms companies typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions.

Following the invalidation of Safe Harbour by the European Court of Justice (October 6, 2015), companies still use EU Standard Contractual Clauses to transfer personal data to countries outside the EEA. For international transfers within a corporate group, Binding Corporate Rules are becoming increasingly common.

8.3 Do transfers of personal data abroad require registration/notification or prior approval from the relevant data protection authority(ies)? Describe which mechanisms require approval or notification, what those steps involve, and how long they take.

No. However, the German data protection authorities have the power to authorise individual transfers on an *ad hoc* basis, where other legal grounds for international data transfer do not apply (section 4c (2)). However, at the time of writing, the German data protection authorities have suspended granting new authorisations for data transfers to the U.S. (see the German data protection authorities' position paper dated October 26, 2016).

9 Whistle-blower Hotlines

9.1 What is the permitted scope of corporate whistle-blower hotlines under applicable law or binding guidance issued by the relevant data protection authority(ies)? (E.g., restrictions on the scope of issues that may be reported, the persons who may submit a report, the persons whom a report may concern.)

The German data protection authorities have issued formal guidance on the scope of whistle-blowing hotlines (see the data protection authorities' April 2007 working paper). According to the guidance, the following matters are within the permitted scope:

- any conduct which constitutes a crime and affects the interests of the business. This includes, for example, fraud and fraudulent accounting, corruption, financial crimes, and illegal insider dealing;
- any conduct in breach of human rights. This includes, for example, the use of child labour; and
- any conduct in breach of environmental protection rules.

It may also include substantial, serious breaches of lawful and clear company policies but this has to be evaluated on a case-by-case basis.

The data protection authorities also recommend that companies review whether it is possible to restrict the scope of persons who may submit reports. They recognise, however, that this requires a case-by-case evaluation.

9.2 Is anonymous reporting strictly prohibited, or strongly discouraged, under applicable law or binding guidance issued by the relevant data protection authority(ies)? If so, how do companies typically address this issue?

According to the German data protection authorities' guidance, anonymous reporting is strongly discouraged. It is recommended that whistle-blowers are informed that their identity will be treated confidentially and that whistle-blowers are not disadvantaged as a result of filing a report.

9.3 Do corporate whistle-blower hotlines require separate registration/notification or prior approval from the relevant data protection authority(ies)? Please explain the process, how long it typically takes, and any available exemptions.

Where a company has appointed a Data Protection Officer, there is no requirement to make a notification to the relevant data protection authority. However, it is likely that the Data Protection Officer has to conduct a formal prior check before the whistle-blowing system is deployed. The length of this prior checking depends on the complexity of the whistle-blowing system and can range from days to months. The Data Protection Officer will also have to update the processing inventories.

9.4 Do corporate whistle-blower hotlines require a separate privacy notice?

There is no general requirement to have a separate notice for a whistle-blower hotline. Where works council agreements have been made within the employer's organisation regarding whistle-blowing which also cover data protection issues, the regulators require the employer to make the content of those agreements easily available to all employees, including new hires. As the information that needs to be provided to individuals about the whistle-blower hotline is rather specific (e g., description of the procedure for submitting and handling reports, possible consequences of unfounded reports), in practice companies tend to implement a separate privacy notice for their whistle-blower hotline.

9.5 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

Where a works council exists within an organisation, it has to be informed and consulted for any issue related to the implementation of technical means intended to monitor the activities of employees. Regulators advise that companies which plan to implement whistle-blowing hotlines better ensure the agreement of their works council in a timely fashion. In practice, companies tend to engage into negotiations with their works councils before implementing whistle-blowing hotlines.

10 CCTV and Employee Monitoring

10.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies)?

Where a company has appointed a DPO, there is no requirement to make a notification to the relevant data protection authority. However, it is likely that the Data Protection Officer has to conduct a formal prior check before the CCTV system is deployed. The DPO will also have to update the processing inventories.

Section 6b regulates in detail how publicly accessible premises may be monitored via CCTV, and the data protection authorities have issued guidelines on CCTV implementation.

10.2 What types of employee monitoring are permitted (if any), and in what circumstances?

Employee monitoring is only permitted in very limited circumstances since the relevant legal basis (section 32) is a specific provision for employee data processing. For example, data controllers may process personal data of employees if it is necessary to discover crimes but only if: (a) there are documented factual indications which support the suspicion that the employee has committed a crime in the course of the employment relationship; (b) the processing of personal data is necessary to discover the crime; and (c) the protected privacy interests of the employee do not take precedence.

Permanent monitoring of employees via CCTV is usually not permitted and companies have been fined for doing so. Sporadic monitoring for quality and training purposes (e.g., listening in on customer calls) may be lawful provided it is not excessive and the relevant legal requirements (e.g., notice) are met.

10.3 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

In an employment context, data protection authorities consider that consent is not a valid legal basis for the processing of personal data since employees are rarely free to give or withhold consent

demanded by the employer. Therefore, the employer needs to ensure that any monitoring of employees that involves the processing of personal data is covered by section 32.

In addition to the legal basis, the employer must provide advance and sufficiently detailed notice of any employee monitoring. Where the employer has a works council, a works council agreement will usually be required to legitimise the employee monitoring. Employees must then be made aware of these works council agreements, which is usually done via email or another type of prominent notice.

10.4 To what extent do works councils/trade unions/ employee representatives need to be notified or consulted?

Section 87 Nos. 1 and 6 of the Works Constitution Act (*Betriebsverfassungsgesetz*) requires that the works council must be informed about, and agree to, all measures that concern how the employees' behaviour is regulated and whenever technical means to monitor the employees' behaviour and performance are to be introduced. This process usually takes several months.

10.5 Does employee monitoring require separate registration/notification or prior approval from the relevant data protection authority(ies)?

Where a company has appointed a DPO, there is no requirement to make a notification to the relevant data protection authority. However, it is likely that the DPO has to conduct a formal prior checking before the employee monitoring measures are deployed. The DPO will also have to update the processing inventories.

11 Processing Data in the Cloud

11.1 Is it permitted to process personal data in the cloud? If so, what specific due diligence must be performed, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

Yes, personal data may be processed in the cloud provided all legal requirements are met. In their detailed guidance (dated September 26, 2011), the German data protection authorities identified five areas where specific due diligence by the data controller is required:

- the risk of re-identification of anonymised data;
- the data protection obligations of all parties involved in providing the cloud service (including sub-processors);
- the data controller's continued ability to comply if a data subject exercises his/her/its rights of access, correction, deletion and blocking;
- the lawfulness of any international transfers of personal data in the context of the cloud services; and
- the presence and verification of appropriate technical and organisational security measures, particularly concerning deletion, data separation, transparency, data integrity, back-ups and audit functions.

11.2 What specific contractual obligations must be imposed on a processor providing cloud-based services, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

The FDPA's requirements for data processing agreements must be met. These are mainly set out in section 11 and include contractual provisions concerning:

- the subject and duration of the data processing;
- the extent, type and purpose of the intended collection, processing or use of data, the type of data and category of data subjects;
- the technical and organisational security measures to be implemented pursuant to section 9;
- the rectification, erasure and blocking of data;
- the processor's obligations under section 11 (4), in particular as regards monitoring the data processing;
- any right to appoint sub-processors;
- the data controller's rights to monitor and the data processor's corresponding obligations to accept such monitoring and cooperate with the data controller;
- notification obligations where the data processor or its employees breach applicable data protection law or the contract;
- the extent of the data controller's authority to issue instructions to the data processor; and
- the return of data storage media and the erasure of data recorded by the data processor at the end of the data processing.

12 Big Data and Analytics

12.1 Is the utilisation of big data and analytics permitted? If so, what due diligence is required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

Yes, provided the processing involved in the analysis of the personal data is covered by a legal basis and the remaining provisions of the FDPA (e.g., regarding notice) are complied with.

In practice, the Baden-Wurttemberg Data Protection Authority states in its 2013 report that the principles of data minimisation and data economy should be reflected in the design of big data platforms. Where anonymisation and pseudonymisation are used, it should be ensured that the risk of re-identification is properly taken into account.

13 Data Security and Data Breach

13.1 What data security standards (e.g., encryption) are required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

Section 9 and its annex set out the legally required data security measures that must be applied when personal data are processed, namely:

1. measures to control who has physical access to the personal data;

2. measures to control who has virtual access to the personal data;
3. measures to enforce limits on user access rights;
4. measures to control to whom personal data are disclosed;
5. measures to monitor and log any input, modification or deletion of personal data;
6. measures to control subcontractors;
7. measures to ensure availability of the personal data; and
8. measures to ensure that personal data collected for different purposes are used separately and not mixed.

The FDPA recognises that state-of-the-art encryption is particularly suitable as a type of security measure listed under Nos. 2 to 4 above.

13.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.

Yes, section 42a requires that in the circumstances described below, the competent data protection authority as well as the affected individuals must be informed without undue delay.

The circumstances in which section 42a applies are that there is an unlawful transfer or other disclosure to third parties of the following types of personal data and there is a danger of serious adverse effects against the rights or protected interests of the affected individuals.

The types of personal data which are within the scope of this section are:

- sensitive data as defined in the FDPA;
- personal data that are subject to professional or official confidentiality obligations;
- data concerning criminal acts or administrative offences;
- bank or credit card account details;
- customer usage data (e.g., user identification data and traffic data), where the Telecommunications Act applies; and
- customer contract data (e.g., subscriber registration data), where the Telecommunications Act applies.

The data protection authorities have issued detailed guidance on section 42a.

13.3 Is there a legal requirement to report data breaches to individuals? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.

Yes, where section 42a applies, the data controller must notify the affected individuals as soon as appropriate measures to secure the relevant data have been implemented and any criminal prosecution is no longer endangered.

Each affected individual must be provided with information about the kind of data breach and about ways of mitigating any adverse effects on their interests.

13.4 What are the maximum penalties for security breaches?

Administrative fines for not reporting security breaches appropriately may amount up to €300,000.

14 Enforcement and Sanctions

14.1 Describe the enforcement powers of the data protection authority(ies):

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
Conduct inquiries (section 38 (3)).		
Conduct on-site audits (section 38 (4)).		
Impose compliance orders, including prohibiting individual processing operations (section 38 (5)).	Impose fines until order is complied with.	
Require the appointment of a different DPO (section 38 (5)).		
Inform data subjects about breaches of data protection law (section 38 (1)).		
Inform responsible criminal prosecutor about breaches of data protection law (section 38 (1)).		
Inform other competent supervisory authorities about breaches of data protection law (section 38 (1)).		
	Impose administrative fines of up to €50,000 under section 43 (1) (if the state data protection law has transferred this power to the state data protection authority).	
	Impose administrative fines of up to €300,000 under section 43 (2) (if the state data protection law has transferred this power to the state data protection authority).	
		Apply to the competent criminal prosecutor under section 44 (2) which can trigger sanctions of up to two years' imprisonment as well as a fine.

14.2 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

German data protection authorities exercise their enforcement powers reasonably frequently. Most common are audits (whether

by way of questionnaire or on-site inspection) as well as specific compliance orders. Where serious breaches occurred or orders are not complied with, German data protection authorities impose fines.

Notable cases include a €1.1 million fine imposed on Deutsche Bahn for multiple breaches of the FDPA, as well as a €1.5 million fine imposed on the Lidl group for using private detectives and secret cameras in their German shops.

Recent cases concerned Hamburg DPA's €54,000 fine of Europcar for using GPS trackers in certain rental cars.

15 E-discovery / Disclosure to Foreign Law Enforcement Agencies

15.1 How do companies within your jurisdiction respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

In our experience, German companies tend to refer foreign public authorities to the relevant mutual legal assistance treaties so that disclosures of personal data are done in a manner compliant with German data protection law. Where e-discovery requests are concerned, German companies tend to pseudonymise or anonymise the relevant materials first, before they are transferred.

15.2 What guidance has the data protection authority(ies) issued?

Where direct disclosure requests/orders by foreign public authorities are concerned, the German data protection authorities have stated that the relevant German authorities should be involved immediately so that the disclosure can be done in accordance with relevant mutual legal assistance treaties (see the Berlin Data Protection Authority's statement dated November 14, 2008, as well as the German Federal Ministry of Justice's letter to the Berlin Data Protection Authority dated January 31, 2007).

As regards foreign e-discovery requests/orders, the German data protection authorities' position is that in light of the Article 29 Working Party's paper on this topic (WP 158) as well as the Hague Convention, there must not be a transfer of personal data abroad before proceedings have been issued (i.e., pre-trial). Once the proceedings are underway, though, personal data can be transferred in pseudonymised form and data such as individual names may be de-pseudonymised as required on a case-by-case basis (see section 11.3 of the Berlin Data Protection Authority's 2009 report).

16 Trends and Developments

16.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

German courts and DPAs have been increasingly active during the last 12 months. There have been a number of important cases in various areas which demonstrate that data protection compliance is taken very seriously by the German DPAs and the German courts. Below are a number of examples of recent case law and DPA proceedings. Further, there has been significant legislative activity.

a) Case Law

- **Applicable Law**

  On January 24, 2014, the Chamber Court of Berlin rejected Facebook's appeal of an earlier judgment by the Regional Court of Berlin in cases brought by a German consumer rights organisation. In particular, the court: (i) enjoined Facebook from, broadly, operating its "Find a Friend" functionality in a way that violates the German Unfair Competition Act; (ii) enjoined Facebook from using certain provisions in (1) its terms and conditions, and (2) privacy notices concerning advertisements, licensing, personal data relating to third parties and personal data collected through other websites; and (iii) mandated that Facebook provide users with more information about how their address data will be used by the "Find a Friend" functionality.

  Similar to an earlier case against Apple, the German consumer rights organisation successfully argued that German, not Irish, data protection law applied. Although other German courts have not always accepted this line of reasoning, the court followed it here and, notably, held that a breach of data protection law may also constitute a breach of the Unfair Competition Act. This approach represents a new development in the data protection context. One of the conditions for consumer rights organisations to be able to commence legal proceedings is that there is a violation of the Unfair Competition Act. Therefore, recognising data protection law violations as violations of the Unfair Competition Act arguably makes it easier for consumer rights organisations to bring privacy-oriented cases. It also can be seen as part of a wider trend to improve the ability of German consumer rights organisations to sue for breaches of data protection law.

- **Web Analytics**

  On February 18, 2014, the Frankfurt am Main Regional Court issued a ruling addressing the use of opt-out notices for web analytics tools. The case concerned Piwik web analytics software and its "AnonymizeIP" function. The court held that website users must be informed clearly about their right to object to the creation of pseudonymised usage profiles. This information must be provided when a user first visits the website (e.g., via a pop-up or highlighted/linked wording on the first page) and must be accessible at all times (e.g., via a privacy notice). Although the website provider in question had enabled an "anonymising" function in Piwik, the court found that pseudonymised usage profiles were being created. To make that determination, the court drew on the Schleswig-Holstein Data Protection Authority ("**DPA**")'s detailed analysis of Piwik, as well as the federal German DPA's formal resolution on web analytics. Notably, the case was brought by a competitor of the website provider who argued that the website provider breached Germany's Unfair Competition Act. This case, along with the Bavarian DPA's reports on Adobe Analytics and Google Analytics, illustrates that web analytics continue to be a "hot topic" in Germany. The case also represents a broader trend in Germany of treating violations of data protection law as breaches of unfair competition law.

- **€1.3 million Fine for Violation of Data Protection Law**

  On December 29, 2014, the Commissioner for Data Protection and Freedom of Information of the German state Rhineland-Palatinate issued a press release stating that it imposed a fine of €1,300,000 on the insurance group Debeka. According to the Commissioner, Debeka was fined due to its lack of internal controls and its violations of data protection law. Debeka sales representatives allegedly bribed public sector employees during the eighties and nineties to obtain address data of employees who were on path to become civil servants. Debeka purportedly wanted this address data to market insurance contracts to these employees. The Commissioner asserted that the action against Debeka is intended to emphasise

that companies must handle personal data in a compliant manner. The fine was accepted by Debeka to avoid lengthy court proceedings. In addition to the monetary fine, the Commissioner imposed obligations on Debeka with respect to its data protection processes and procedures, including a requirement that Debeka's employees obtain written consent from customers when they disclose their addresses. The insurance group also has appointed 26 Data Protection Officers. The public prosecutor has initiated criminal proceedings against representatives of Debeka in this matter and those proceedings are ongoing.

- **Fines for Inadequate Data Processing Agreement**

  On August 20, 2015, the Bavarian DPA issued a press release stating that it imposed a significant fine on a data controller for failing to adequately specify the security controls protecting personal data in a data processing agreement with a data processor. The DPA stated in the press release that the data processing agreement did not contain sufficient information regarding the technical and organisational measures to protect the personal data. The press release noted that the agreement was not specific enough and merely repeated provisions mandated by law. According to the German Federal Data Protection Act, data controllers must impose detailed data security measures on data processors in data processing agreements. The text of a data processing agreement must enable the data controller to assess whether or not the data processor is able to ensure the protection and security of the personal data. According to the DPA, the law provides some flexibility for companies to determine which contractual obligations are appropriate for a particular engagement. The DPA stated that this choice may depend on the data security plan of the data processor and related data processing systems used. In all data processing agreements, however, the following controls must be specified: (1) physical admission control; (2) virtual access control; (3) access control; (4) transmission control; (5) input control; (6) assignment control; (7) availability control; and (8) separation control.

- **Fines for Unlawful Transfer of Customer Data as Part of an Asset Deal**

  On July 30, 2015, the Bavarian DPA issued a press release stating that it imposed a significant fine on both the seller and purchaser in an asset deal for unlawfully transferring customer personal data as part of the deal.

  In the press release, the DPA stated that customer data often have significant economic value to businesses, particularly with respect to delivering personalised advertising. If a company terminates its business, it may sell its valuable economic assets, including customer data, to another company as part of an asset deal. In addition, insolvency administrators may try to sell the customer data maintained by the business during the insolvency process.

  According to the press release, the Bavarian DPA fined both the seller and the purchaser for unlawfully transferring email addresses of customers of an online shop. The exact fines were not announced, but the press release mentions that they were fined upwards of five figures. The DPA also stated that transferring customer email addresses, phone numbers, credit card information and purchase history requires prior customer consent or, alternatively, customers must be given prior notice about the intent to transfer such personal data so that they have an opportunity to object to the transfer. Since the seller and the purchaser failed to obtain customer consent or give the customers an opportunity to object, the DPA found both companies in violation of German data protection law. The DPA also pointed out that both seller and purchaser are "data controllers" and thus have broader responsibilities than data processors under German data protection law. In addition, the DPA stated that it will act similarly in future cases and will fine companies that sell customer data in a non-compliant manner during asset deals.

b) Legislative Activity

Further, there has been significant legislative activity in the area of enforcement of data protection law by Consumer Protection Organisations. On December 18, 2015, the German Federal Parliament approved a draft law to improve the enforcement of data protection provisions that are focused on consumer protection. The new law will bring about a fundamental change in how German data protection law is enforced. The draft law enables consumer protection organisations, trade associations and certain other associations to enforce cease-and-desist letters and file interim injunctions in cases where companies violate the newly defined protective data protection provisions for consumers. The draft law targets data processing practices for the following purposes: 1) advertising, marketing and opinion research; 2) operating credit agencies; 3) creating personality and usage profiles; 4) selling addresses; 5) other data trading activities; and 6) other similar commercial purposes. The draft law will also introduce a requirement that courts must grant the data protection authorities an opportunity to comment before issuing decisions.

16.2 What "hot topics" are currently a focus for the data protection regulator?

The German DPAs are very active in issuing guidance papers and addressing a variety of "hot topics" from their perspective.

Use of Personal Data for Advertising Purposes

For example, on December 10, 2013, a German data protection working group on advertising and address trading published new guidelines on the collection, processing and use of personal data for advertising purposes (the "**Guidelines**"). These new Guidelines cover, among other things, the following: the use of personal data for advertising purposes without the data subject's consent (so-called "**list-privilege**"); consent in the context of advertising, including form (written, electronic, double opt-in) and content requirements; and the data subject's rights with respect to advertising and the timeframes within which data controllers must respond to the exercise of such rights. Both sets of guidelines represent a significant clarification of the data protection regulations that apply to advertising in Germany. They are relevant to all businesses with German advertising operations, regardless of target audience (business-to-business and business-to-consumer) or advertising channel (email, telephone, mail).

Use of CCTV

On March 10, 2014, the German Federal Commissioner for Data Protection and Freedom of Information and all 16 German state data protection authorities responsible for the private sector issued guidelines on the use of closed-circuit television ("**CCTV**") by private companies. The guidelines provide information regarding the conditions under which CCTV may be used and outline the requirements for legal compliance.

Use of Apps

On June 18, 2014, the German state data protection authorities responsible for the private sector (the *Düsseldorfer Kreis*) issued guidelines concerning the data protection requirements for app

developers and app publishers. The Guidelines (33 pages) were prepared by the Bavarian DPA and cover requirements in Germany's Telemedia Act as well as the Federal Data Protection Act.

Data Transfers and Safe Harbour

On October 26, 2015, the German federal and state data protection authorities (the "**German DPAs**") published a joint position paper on Safe Harbour and potential alternatives for transfers of data to the U.S. (the "**Position Paper**").

The Position Paper follows the ruling of the Court of Justice of the European Union ("**CJEU**") on Safe Harbour and contains 14 statements regarding the ruling, including the following key highlights:

- In light of the Safe Harbour Decision of the CJEU, the German DPAs call into question the lawfulness of data transfers to the U.S. on the basis of other transfer mechanisms, such as standard contractual clauses or Binding Corporate Rules ("**BCRs**").
- To the extent that they become aware, the Position Paper indicates that the German DPAs will prohibit data transfers to the U.S. that are solely based on Safe Harbour.
- When using their powers under Article 4 of the respective Commission Decisions on the standard contractual clauses of December 2004 (2004/915/EC) and February 2010 (2010/87/EC) to assess data transfers, the Position Paper indicates that the German DPAs will rely on the principles formulated by the CJEU. In particular, the German DPAs will focus on Nos. 94 and 95 of the judgment, which address recipient countries that compromise the fundamental right of respect for private life and lack respect for the essence of the fundamental right to effective judicial protection.
- At this time, the Position Paper discloses that the German DPAs will not issue new approvals for data transfers to the U.S. on the basis of BCRs or data export agreements.
- The Position Paper requests companies to immediately design their data transfer procedures in a way that considers data protection. Companies that would like to export data to the U.S. or other third countries should also use as guidance the German DPAs' March 2014 resolutions on "Human Rights and Electronic Communication" and the October 2014 guidelines on "Cloud Computing".
- The German DPAs indicate that consent for the transfer of personal data may be a sound legal basis under narrow conditions. In principle, however, the data transfer must not be massive or occur routinely or repeatedly, according to the Position Paper.
- With respect to the export of employee data and certain third party data, the German DPAs indicate that consent may only be a lawful legal basis in exceptional cases for a data transfer to the U.S.
- The German DPAs request that the legislators grant them a right to file an action in accordance with the CJEU judgment.

In the Position Paper, the German DPAs also call upon the European Commission to push for the creation of sufficiently far-reaching guarantees for the protection of privacy during its negotiations with the U.S., including such protections as the right to judicial remedy, data protection rights and the principle of proportionality. Further, the German DPAs indicate that it is essential to promptly adjust the Commission Decisions on EU model clauses to the requirements of the CJEU decision. To this extent, the DPAs welcomed the deadline of January 31, 2016 set by the Article 29 Working Party.

Anna Pateraki
Hunton & Williams
Park Atrium
Rue des Colonies 11
1000 Brussels
Belgium

Tel: +32 2 643 58 28
Fax: +32 2 643 58 22
Email: apateraki@hunton.com
URL: www.hunton.com

Anna Pateraki has experience in advising multinational clients of all industry sectors on a broad range of EU data protection and cybersecurity matters, including German-related data protection issues. She has particular experience in developing strategies for international data transfers and regularly advises clients on issues such as data breach notification, cloud computing, smart grids, big data and e-discovery.

HUNTON& WILLIAMS

Hunton & Williams' Global Privacy and Cybersecurity practice is a leader in its field. It has been ranked by *Computerworld* for four consecutive years as the top law firm globally for privacy and data security. *Chambers & Partners* ranks Hunton & Williams as the top privacy and data security practice in its *Chambers & Partners UK*, *Chambers Global* and *Chambers USA* guides.

The team of more than 25 privacy professionals, spanning three continents and five offices, is led by Lisa Sotto, who was named among the *National Law Journal*'s "100 Most Influential Lawyers". With lawyers qualified in six jurisdictions, the team includes internationally-recognised partners Bridget Treacy and Wim Nauwelaerts, former FBI cybersecurity counsel Paul Tiao, and former UK Information Commissioner Richard Thomas.

In addition, the firm's Centre for Information Policy Leadership, led by Bojana Bellamy, collaborates with industry leaders, consumer organisations and government agencies to develop innovative and pragmatic approaches to privacy and information security.

United Kingdom

Bridget Treacy

Hunton & Williams

Stephanie Iyayi

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The principal data protection legislation is the Data Protection Act 1998 (the "**DPA**"), which took effect in 2000 and implements into UK law the requirements of the EU Data Protection Directive (95/46/EC) (the "**Data Protection Directive**"). The purpose of the DPA is to balance the rights of individuals and the commercial interests of organisations that use personal data about individuals.

1.2 Is there any other general legislation that impacts data protection?

The Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended by the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011) ("**PECR**") implement the requirements of Directive 2002/58/EC (as amended by Directive 2009/136/EC) (the "**ePrivacy Directive**"). PECR regulates direct marketing by electronic means and the use of cookies and similar technologies. It also imposes sector specific breach reporting requirements, applicable to providers of public electronic communications services.

1.3 Is there any sector specific legislation that impacts data protection?

Regulated organisations within the financial services sector have a separate obligation to conduct their business activities with "due skill, care and diligence" and to "take reasonable care to organise and control [their] affairs responsibly and effectively, with adequate risk management systems". These requirements impose additional data protection compliance obligations on data controllers within the financial services sector, in addition to the DPA.

1.4 What is the relevant data protection regulatory authority(ies)?

The Information Commissioner's Office (the "**ICO**") oversees and enforces the DPA and PECR in the UK. The current Information Commissioner, appointed in June 2009, is Christopher Graham. His term expires in June 2016, and the name of his successor will be announced imminently. The Information Commissioner is appointed by HM The Queen, has independent status, and reports directly to Parliament. Data controllers within the financial services sector are also regulated by the Prudential Regulation Authority (the "**PRA**") and the Financial Conduct Authority (the "**FCA**").

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **"Personal Data"**

  "Personal data" means any data which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller. Under the DPA, "personal data" does not include information relating to persons who are not individuals (e.g., companies or trusts).

- **"Sensitive Personal Data"**

  "Sensitive personal data" means personal data relating to ethnicity, race, political or religious beliefs, trade union membership, health, sexual life and orientation, or actual or alleged criminal proceedings and convictions. Sensitive personal data are subject to increased compliance obligations due to their sensitive nature and the increased risk of harm to the individual if the data are improperly handled.

- **"Processing"**

  The DPA governs the collection, use and storage of personal data and applies to both manual and computerised data and all forms of data "processing". "Processing" means obtaining, recording or holding data, including the organisation, adaptation or alteration, retrieval, consultation or use, disclosure and blocking, destroying or erasure of personal data.

- **"Data Controller"**

  The DPA defines a "data controller" as a natural or legal person who, alone or jointly, determines the purposes for which, and the manner in which, the personal data are processed. The DPA only applies to data controllers.

- **"Data Processor"**

  A "data processor" is defined as any natural or legal person (other than an employee of the controller) who processes personal data on behalf of the controller. A data processor does not have any direct statutory obligations under the DPA and is only subject to contractual obligations imposed by the data controller.

- **"Data Subject"**

  A "data subject" is the individual who is the subject of the personal data.

- *Other key definitions – please specify (e.g., "Pseudonymous Data", "Direct Personal Data", "Indirect Personal Data")*

  There are no other key definitions in particular.

3 Key Principles

3.1 What are the key principles that apply to the processing of personal data?

- **Transparency**

  Under Principle 1 of the DPA, personal data must be processed fairly and lawfully. Specifically, data subjects must be informed by the data controller of how their personal data will be used.

  As a minimum, at the time of collection of the personal data or before it is first processed by the data controller, the data controller must provide notice of: (i) its identity; (ii) the fact that personal data are collected and the types of personal data collected; (iii) the specific purposes for which the personal data will be processed; and (iv) any further information required to make the processing fair in the particular circumstances, e.g., disclosures of the personal data to third parties or transfers of the personal data outside of the jurisdiction.

  Notice should be clear, easily understandable and genuinely informative.

- **Lawful basis for processing**

  For personal data to be processed lawfully, the data controller must have a legal basis for each processing activity. The DPA sets out legal bases for the processing of personal data in Schedule 2, and for sensitive personal data in Schedule 3.

  The legal bases commonly relied upon by UK data controllers to process personal data are: (i) consent of the data subject; (ii) processing that is necessary to perform a contract, or to enter into a contract, with the data subject; (iii) processing that is necessary to comply with a legal obligation of the data controller (other than a contractual obligation); and (iv) processing that is necessary for the legitimate interests of the data controller or a third party to whom the data are disclosed, except where it would prejudice the fundamental rights and freedoms of the data subject (this is a balancing test).

  Where processing sensitive personal data, UK data controllers commonly rely on explicit consent or compliance with an employment law obligation.

- **Purpose limitation**

  Under Principle 2 of the DPA, personal data may only be obtained for one or more specified and lawful purposes, and cannot be further processed in any manner incompatible with that purpose. Determining whether a further purpose is "compatible" with the original purpose is a question of fact. Where a further purpose is deemed incompatible with the original purpose, the data controller must provide notice of the further purpose and be able to rely on a legal ground for the further purpose.

- **Data minimisation**

  Under Principle 3 of the DPA, personal data must be relevant and not excessive in relation to the purpose for which they are processed. Data controllers are therefore under a duty to process only the personal data necessary for the relevant processing purpose, and to refrain from collecting or retaining unnecessary or irrelevant personal data.

- **Proportionality**

  As part of the data minimisation principle, personal data collected and processed should be proportionate to the processing purposes. In practice, this means processing the least amount of personal data necessary for the purposes, and using anonymous or pseudonymous data where possible.

- **Retention**

  Under Principle 5 of the DPA, personal data must not be retained for longer than is necessary for the processing purpose. Data controllers must ensure that data are only collected, used and retained to satisfy the relevant processing purpose. The DPA does not, however, stipulate any specific retention periods.

- *Other key principles – please specify*

  The DPA also requires data controllers to ensure that the personal data they process are accurate and up to date (Principle 4 – see Section 4), processed in accordance with the rights of affected data subjects (Principle 6 – see Section 4), safeguarded by appropriate organisational and technical measures (Principle 7 – see Section 13), and not transferred outside of the European Economic Area ("**EEA**"), unless an adequate level of data protection exists (Principle 8 – see Section 8).

4 Individual Rights

4.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Access to data**

  A data subject has the right to submit a subject access request ("**SAR**") to a data controller, requiring the data controller to: (i) confirm whether it is processing the data subject's personal data; (ii) provide a description of their personal data held by the data controller, the purpose for which their data are held, the persons or category of persons to whom their data may be disclosed, and any information about the source of the data; and (iii) provide a copy of their personal data. SARs must be made in writing, and data controllers are permitted to charge a statutory fee (currently £10) towards the costs of responding to the SAR.

- **Correction and deletion**

  Under the DPA, personal data must be accurate and, where necessary, kept up to date (Principle 4), and must not be retained for longer than is necessary (Principle 5). A data subject can require a data controller to correct or supplement inaccurate or incomplete personal data held about them. Data subjects can also apply for a court order requiring the data controller to rectify, block, erase or destroy personal data that are inaccurate.

- **Objection to processing**

  A data subject has the right to object to processing, but only if it causes unwarranted and substantial damage or distress. If it does, the data subject has the right to require an organisation to stop (or not to begin) the processing. The right to object to processing is not an absolute right. In certain limited circumstances, data controllers may be required (including by court order) to stop or not begin processing a data subject's personal data. If, in the circumstances, the data controller is not required to stop (or not begin) the processing, the data controller must provide an explanation to the data subject as to why it does not have to, and will not, stop the processing.

- **Objection to marketing**

  Under the DPA, a data subject can object at any time to the processing of their personal data for marketing purposes. This is an absolute right.

- **Complaint to relevant data protection authority(ies)**

  Individuals may raise complaints with the ICO. The ICO's website provides a number of survey-style complaint forms, based on different areas of complaint, currently including nuisance marketing text messages and telephone calls. The ICO encourages individuals to use these standard online complaint forms and reporting tools. Nevertheless, data subjects can also raise complaints in writing, by email, or by telephoning the ICO. There is no charge to submit a complaint.

- *Other key rights – please specify*

  Data subjects also have rights in relation to direct marketing and cookies (see Section 7).

5 Registration Formalities and Prior Approval

5.1 In what circumstances is registration or notification required to the relevant data protection regulatory authority(ies)? (E.g., general notification requirement, notification required for specific processing activities.)

Under the DPA, a general registration requirement is imposed on data controllers. Certain exemptions apply, including: (i) for not-for-profit organisations, in certain circumstances; (ii) processing personal data for personal, family, or household affairs (the "domestic purposes exemption"); and (iii) data controllers who only process personal data for purposes of their own business relating to staff administration, advertising, marketing and public relations, and accounts and records.

5.2 On what basis are registrations/notifications made? (E.g., per legal entity, per processing purpose, per data category, per system or database.)

Registrations must be submitted for each legal entity. Each data controller that is under a duty to register must submit a registration which sets out its data processing activities.

5.3 Who must register with/notify the relevant data protection authority(ies)? (E.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation.)

Organisations subject to the DPA and not benefitting from one of the registration exemptions must register with the ICO. This therefore includes both UK organisations and foreign organisations. The latter can register through a UK branch office or an appointed UK representative.

5.4 What information must be included in the registration/notification? (E.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes.)

The following information must be included in the ICO registration: (i) name and address of the data controller (or if the data controller has nominated a representative, the name and address of the representative); (ii) legal status of the data controller (e.g., sole trader, company); (iii) sector in which the data controller operates; (iv) nature of work; (v) description of the personal data being or to be processed, and a description of the category or categories of data subject to which they relate; (vi) processing purposes; (vii) description of any recipient(s) to whom the data controller intends or may wish to disclose the data; (viii) data transfers; and (ix) description of the data controller's security measures. There are also a number of tick-box compliance questions to complete and contact details for queries must be provided.

5.5 What are the sanctions for failure to register/notify where required?

Failure to register with the ICO is a criminal offence and may lead to a fine of up to £5,000 in a magistrates' court or an unlimited fine in the Crown Court.

5.6 What is the fee per registration (if applicable)?

An initial fee and annual renewal fee apply. Data controllers with over 250 employees and a turnover of £25.9 million or more must pay a notification fee of £500. All other data controllers must pay a £35 fee. Registered charities and small occupational pension schemes are subject to the £35 fee, regardless of their size and turnover.

5.7 How frequently must registrations/notifications be renewed (if applicable)?

Registrations must be renewed annually.

5.8 For what types of processing activities is prior approval required from the data protection regulator?

No processing activities require prior approval from the ICO. However, a data controller may wish to approach the ICO informally before implementing a new processing activity, particularly if it is high-risk, novel, or uses emergent technology, the compliance of which may be something of a "grey area".

5.9 Describe the procedure for obtaining prior approval, and the applicable timeframe.

This is not applicable.

6 Appointment of a Data Protection Officer

6.1 Is the appointment of a Data Protection Officer mandatory or optional?

There is no statutory requirement to appoint a Data Protection Officer in the UK. In practice, however, many organisations do so, particularly larger organisations.

6.2 What are the sanctions for failing to appoint a mandatory Data Protection Office where required?

This is not applicable.

6.3 What are the advantages of voluntarily appointing a Data Protection Officer (if applicable)?

Voluntarily appointing a Data Protection Officer does not provide statutory exemptions from other obligations. However, it affords obvious practical compliance advantages in terms of specialist knowledge and know-how, a single contact point for data protection queries, and a designated individual with overall responsibility and oversight for data protection matters.

6.4 Please describe any specific qualifications for the Data Protection Officer required by law.

There are no particular qualifications prescribed by law. In practice, Data Protection Officers typically have experience in information management, records management, IT, data security, and/or compliance.

6.5 What are the responsibilities of the Data Protection Officer, as required by law or typical in practice?

There are no responsibilities prescribed by law. In practice, the Data Protection Officer is typically responsible for: responding to queries and requests from data subjects, the ICO, the FCA and the PRA; developing internal policies and procedures; developing staff training; advising on compliance with applicable law; reviewing and advising on new products or procedures; identifying risk areas; and advising on legal developments that may impact the organisation.

6.6 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

No. However, a contact person needs to be designated on the ICO registration, and this can be the Data Protection Officer.

7 Marketing and Cookies

7.1 Please describe any legislative restrictions on the sending of marketing communications by post, telephone, email, or SMS text message. (E.g., requirement to obtain prior opt-in consent or to provide a simple and free means of opt-out.)

Postal marketing communications are not specifically regulated, but must generally comply with the requirements of the DPA.

PECR distinguishes between live telephone calls and automated recorded calls. Live unsolicited marketing calls can be made unless the number has opted-out. Companies must therefore consult the Telephone Preferences Service, the central opt-out register, and must not call any number where the person has otherwise objected to receiving their calls. Further, organisations must always identify the caller, and provide a contact address or freephone contact number if asked.

Automated pre-recorded marketing calls require specific, prior opt-in consent. Consent to receive live calls is not sufficient as a consent to receive recorded calls. Automated calls must say who is calling and provide a contact address or freephone number.

The sending of email or SMS text message marketing requires prior opt-in consent. A limited exception, known as the "soft opt-in", allows an organisation to send an unsolicited email or SMS text message marketing communication if: (i) the organisation obtained the recipient's contact details in the course of a sale or negotiations for the sale of a product or service; (ii) the marketing communication relates to similar products and services; and (iii) the recipient is given a simple means of refusing the receipt of further marketing communications (e.g., an "unsubscribe" link or replying "STOP" to an SMS text message).

7.2 Is the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

Yes. The ICO actively encourages members of the public to report nuisance and unwanted marketing. Recent enforcement actions include monetary penalty notices in February 2016 of £350,000 issued to Prodial Ltd, a lead generation firm responsible for over 46 million automated nuisance calls (the ICO's largest ever fine) and of £80,000 issued to UKMS Money Solutions Limited, a PPI claims company, for sending more than 1.3 million spam texts.

7.3 Are companies required to screen against any "do not contact" list or registry?

Yes. A do-not-call list containing the telephone numbers of individuals who have opted-out of receiving calls for direct marketing purposes, known as the Telephone Preference Service List, is in place. In addition, the Corporate Telephone Preference Service List contains a list of business telephone numbers that have opted-out of receipt of calls for direct marketing purposes. Individuals included on such lists must not be called for marketing purposes unless the caller has received specific consent to do so.

7.4 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

The maximum penalty for sending marketing communications in breach of PECR is a civil monetary penalty of up to £500,000.

7.5 What types of cookies require explicit opt-in consent, as mandated by law or binding guidance issued by the relevant data protection authority(ies)?

Cookies and similar technologies require notice and prior opt-in consent, except where the cookie is strictly necessary for the transmission of a communication over an electronic communications network or for a service requested by the user. The "strictly necessary" exemption is narrowly interpreted and only covers a limited number of cookies.

The law does not stipulate different types of consent for different types of cookies. In practice, however, the ICO distinguishes between more and less intrusive cookies, and is more focused on the compliance of intrusive cookies such as tracking and advertising cookies, and is less focused on analytic and functional cookies.

7.6 For what types of cookies is implied consent acceptable, under relevant national legislation or binding guidance issued by the relevant data protection authority(ies)?

Consent for cookies can be implied, where sufficiently informed.

7.7 To date, has the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

The ICO has written to a number of organisations asking them how they comply with the cookie rules, but has not to date taken any enforcement action in relation to cookies. The ICO has given cookies a low consumer-threat rating compared with unwanted marketing calls and SMS text messages.

7.8 What are the maximum penalties for breaches of applicable cookie restrictions?

The maximum penalty is £500,000.

8 Restrictions on International Data Transfers

8.1 Please describe any restrictions on the transfer of personal data abroad?

Transfers of personal data from the UK to outside of the EEA are generally prohibited, unless an adequate level of data protection is assured or a relevant derogation applies. A "transfer" includes the ability to access data from outside of the UK, e.g., viewing it on a computer screen from another country.

8.2 Please describe the mechanisms companies typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions.

Adequacy can be established on the basis of: (i) a European Commission adequacy finding in respect of that country or otherwise covering that transfer; (ii) the exporting organisation making its own adequacy assessment; or (iii) the data exporter adducing adequate safeguards, including the use of Commission-approved standard contractual clauses or binding corporate rules ("**BCRs**"). Note that the U.S. Safe Harbor was declared invalid by the Court of Justice of the European Union in 2015, and at the time of writing details of the Privacy Shield, incorporating greater protections for European citizens and imposing more stringent requirements on companies, are awaiting approval.

Where an adequate level of data protection is not assured, personal data may only be transferred where a relevant derogation applies, including the unambiguous consent of the individual and transfers necessary for legal proceedings, to protect the public interest, or to protect the vital interests of the individual.

8.3 Do transfers of personal data abroad require registration/notification or prior approval from the relevant data protection authority(ies)? Describe which mechanisms require approval or notification, what those steps involve, and how long they take.

Transfers of personal data must be included in the exporting organisation's general registration with the ICO, but do not require prior approval.

9 Whistle-blower Hotlines

9.1 What is the permitted scope of corporate whistle-blower hotlines under applicable law or binding guidance issued by the relevant data protection authority(ies)? (E.g., restrictions on the scope of issues that may be reported, the persons who may submit a report, the persons whom a report may concern.)

There is no UK specific statute or guidance on hotlines restricting the scope of hotlines. However, hotlines must generally comply with the requirements of the DPA. The Article 29 Working Party opinion on the application of EU data-privacy rules to internal whistle-blowing schemes has application as non-binding general guidance only.

9.2 Is anonymous reporting strictly prohibited, or strongly discouraged, under applicable law or binding guidance issued by the relevant data protection authority(ies)? If so, how do companies typically address this issue?

As there is no UK specific statute or guidance, anonymous reporting is not strictly prohibited or strongly discouraged under binding guidance. However, it is strongly discouraged under the Article 29 Working Party opinion.

9.3 Do corporate whistle-blower hotlines require separate registration/notification or prior approval from the relevant data protection authority(ies)? Please explain the process, how long it typically takes, and any available exemptions.

Hotlines do not require separate registration or prior authorisation. However, organisations can choose to include their hotline in their ICO registration.

9.4 Do corporate whistle-blower hotlines require a separate privacy notice?

Employees should be informed of the existence of, the purposes served by, and the rights associated with a whistle-blowing hotline before it is implemented. Specifically, the notice should provide information regarding the scope of the hotline, how it should be used and the handling of complaints, including any rights that an employee may have in, and to, the data. Whilst whistle-blowing hotlines do not strictly require a separate privacy notice in the UK, it is recommended. In any event, the information should be provided in writing, for evidential purposes.

9.5 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

Only to the extent required under the terms of any trade union agreement in place.

10 CCTV and Employee Monitoring

10.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies)?

Use of CCTV does not require prior authorisation or separate registration, but must be specifically mentioned in the general registration.

10.2 What types of employee monitoring are permitted (if any), and in what circumstances?

Employee monitoring is subject to the general requirements of the DPA. Additionally, the Regulation of Investigatory Powers Act 2000 ("**RIPA**") and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 ("**LBP Regulations**") apply where data are accessed or reviewed in the course of transmission.

RIPA has the potential to cover the interception by an employer of an employee's use of email, text messaging, instant messaging, telephone and the Internet. It is generally an offence to intercept any communication without consent.

Under the LBP Regulations, interception may be authorised in the following circumstances: (i) monitoring business communications to ascertain whether business standards are being complied with and establishing the existence of facts; (ii) national security; (iii) preventing or detecting crime; (iv) detecting unauthorised use; or (v) ensuring the effective operation of the system. The broad grounds for lawful interception without consent provided in the LBP Regulations are restricted by the requirement that the interception must be effected solely for the purposes of monitoring of communications that are relevant to the business, i.e., the LBP Regulations do not cover the interception of any personal communications of employees.

10.3 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Accessing and reviewing an employee's communications, files, work laptops, etc., is generally prohibited unless the consent of the employee is obtained. Employee monitoring can be conducted in limited circumstances without consent if there are appropriate policies and procedures in place notifying employees that accessing, monitoring or reviewing may take place. Such notice may be provided by means of a separate monitoring/electronic communications policy or included in an employee handbook, and should clearly define the nature and extent of potential monitoring. Under Section 29 of the DPA, personal data processed for the prevention or detection of crime are exempt from the requirement to give notice of the monitoring and the requirement to provide individuals with access to personal data. Devices owned personally by an employee may only be seized by an employer if the prior consent of the owner has been obtained, or a court order allowing the employer to carry out such seizure has been obtained.

10.4 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

Only to the extent required under the terms of any trade union agreement in place.

10.5 Does employee monitoring require separate registration/notification or prior approval from the relevant data protection authority(ies)?

No, it does not.

11 Processing Data in the Cloud

11.1 Is it permitted to process personal data in the cloud? If so, what specific due diligence must be performed, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

Processing personal data in the cloud is permitted. The ICO published cloud computing guidance in September 2012 which emphasises that the general requirements of the DPA equally apply in the context of cloud processing. The guidance prompts data controllers using cloud services to consider whether such usage could result in processing additional personal data, e.g., usage statistics and transaction history metadata. The guidance specifically advises data controllers using cloud services to: create a clear record of the categories of personal data in the cloud; select an appropriate cloud provider, particularly in terms of confidentiality and integrity of the data; and be wary of "take it or leave it" standard terms, which may not be fully compliant with the requirements of the DPA. The guidance specifically advises data controllers using cloud services to: (i) create a clear record of the categories of personal data in the cloud; (ii) select an appropriate cloud provider, particularly in terms of confidentiality and integrity of the data; and (iii) be wary of "take it or leave it" standard terms, which may not be fully compliant with the requirements of the DPA.

11.2 What specific contractual obligations must be imposed on a processor providing cloud-based services, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

There are no specific terms that must be imposed on cloud providers, in addition to the general contractual obligations (of data security and use limitation).

12 Big Data and Analytics

12.1 Is the utilisation of big data and analytics permitted? If so, what due diligence is required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

Big data and analytics are permitted. Where data are anonymous, the DPA does not apply. The ICO issued a binding code of practice on anonymisation in November 2012. Under the code of practice, data are considered to be anonymous and no longer personal data where the data: (i) could not be re-identified by a reasonably competent third party having access to resources and using other available information; and (ii) are essentially "put beyond use" by the data controller itself and will not be later re-identified by the data controller.

13 Data Security and Data Breach

13.1 What data security standards (e.g., encryption) are required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

The DPA requires data controllers to put in place appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. The level of security must be appropriate given the nature of the data (i.e., a higher level of security for sensitive personal data) and the potential risk of harm to data subjects if the security safeguards were breached. Specific standards are not stipulated by law or binding guidance, however, the ICO expects organisations to have internal controls, including: appropriate policies and procedures; access controls; training and awareness; and technical controls, including: (i) password-protected devices; (ii) use of encryption technologies; and (iii) secure disposal of IT assets.

13.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.

There is no general legal requirement to report data breaches under the DPA. However, the ICO expects data controllers to report significant breaches to its office and will take any failure to do so into account in determining any applicable monetary penalty.

PECR contains breach reporting requirements that apply specifically to providers of public electronic communication services (e.g., Internet service providers and telecommunication providers), under which they must report breaches to the ICO via a secure PECR security breach notification web form within 24 hours of becoming aware of the breach. As soon as a service provider has enough information to confirm that there has been a breach and provide some basic facts, they must notify, even if they cannot yet provide full details. The initial notification must always include the following summary information: (i) name of the service provider; (ii) name and contact details of the data protection officer or other contact point where more information can be obtained; (iii) date and time of the breach (or an estimate) and the date and time of detection; (iv) circumstances of the breach (e.g., theft, loss, copying); (v) nature and content of the personal data concerned; (vi) security measures applied (or to be applied) to the affected personal data; and (vii) details of the use of other providers (where applicable).

13.3 Is there a legal requirement to report data breaches to individuals? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.

There is no general legal requirement to notify affected data subjects of data breaches under the DPA. However, the ICO expects data controllers to report significant breaches to affected data subjects, particularly where there is a risk of harm and there are steps that data subjects could take to mitigate the potential harm.

13.4 What are the maximum penalties for security breaches?

The maximum penalty is £500,000.

14 Enforcement and Sanctions

14.1 Describe the enforcement powers of the data protection authority(ies):

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
Monetary penalty notices	Up to £500,000 for serious breaches of the DPA and PECR.	This is not applicable.
Undertakings	While the ICO has no formal powers of undertakings under the DPA, in practice the ICO requests organisations to give undertakings, committing to a particular course of action in order to improve their compliance with the DPA.	This is not applicable.
Enforcement notices	The ICO can issue enforcement notices and "stop now" orders for breaches of the DPA, requiring organisations to take specified steps in order to ensure they comply with the law.	This is not applicable.
Prosecution	This is not applicable.	The ICO liaises with the Crown Prosecution Service to bring criminal prosecutions against organisations and individuals for breaches of the DPA.

14.2 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

The ICO is regarded as a pragmatic rather than punitive regulator, and sees its role as educating organisations and the public on the DPA and other relevant legislation, as well as enforcing it. Nevertheless, the ICO will take action to ensure organisations meet their data protection obligations, including monetary penalties, enforcement notices, and prosecutions.

Examples of recent enforcement action brought by the ICO include:

- **Failure to register**: In July 2014, a legal advice company, Global Immigration Consultants Limited, was prosecuted for failing to notify with the ICO. It was fined £300, and ordered to pay costs and a victims' surcharge.
- **Serious data security breach**: The Crown Prosecution Service was fined £200,000 by the ICO in November 2015 after laptops containing videos of police interviews were stolen from a private film studio. The ICO ruled that the CPS was negligent when it failed to ensure the videos were kept safe and did not take into account the substantial distress that

would be caused if the videos were lost. In February 2014, the ICO fined the British Pregnancy Advice Service, a not-for-profit charity, £200,000 for a security flaw on its website that led to the data of over 10,000 women being accessed by a hacker. In January 2013, the ICO issued Sony Computer Entertainment Europe Limited with a monetary penalty of £250,000 in relation to a serious hacking incident.

- **Persistent errors in use of personal data**: In November 2012, Prudential Assurance Company was issued with a monetary penalty of £50,000 for repeatedly confusing two customers' accounts with the same name.
- **Unlawful spamming**: In February 2016, the ICO issued a fine of £350,000 issued to Prodial Ltd, a lead generation firm responsible for over 46 million automated nuisance calls (the ICO's largest ever fine) and of £80,000 issued to UKMS Money Solutions Limited, a PPI claims company, for sending more than 1.3 million spam texts. In November 2012, monetary penalties amounting to £440,000 (overruled on appeal) were served on two individuals who owned a marketing company which had sent millions of unlawful spam texts to the public over a three-year period. Other recent ICO fines for breaches of the marketing rules include a £90,000 fine issued to Kwik Fix Plumbers Limited for continually making nuisance calls to vulnerable victims, and a £70,000 fine issued to Parklife Manchester Ltd for sending unsolicited marketing text messages.

15 E-discovery / Disclosure to Foreign Law Enforcement Agencies

15.1 How do companies within your jurisdiction respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

The disclosure of personal data and the transfer of personal data are both processing activities requiring notice and a valid legal basis. Companies typically provide a general notice at the time of collection, e.g., stating in their privacy policies that the collected personal data may be disclosed in relation to legal proceedings or in response to law enforcement access requests. For non-sensitive personal data, UK companies typically rely on the legitimate interest basis to disclose the data. For sensitive personal data, UK companies typically try to obtain the explicit consent of the affected data subjects.

15.2 What guidance has the data protection authority(ies) issued?

The ICO has not issued specific guidance on this issue. The Article 29 Working Party Working Document on pre-trial discovery for cross-border civil litigation has application as non-binding general guidance.

16 Trends and Developments

16.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

Nuisance calls and spam texts remain a continuing concern for consumers and a key area of action for the ICO. The ICO has issued civil monetary penalties totalling approximately £1,056,000 since April 2015, with £370,000 total penalties being issued in November 2015 alone. In January 2016, the ICO had over 100 cases under investigation, and issued 52 third party information notices. Recent enforcement actions include monetary penalty notices in February 2016 of £350,000 issued to Prodial Ltd, a lead generation firm responsible for over 46 million automated nuisance calls (the ICO's largest ever fine) and of £80,000 issued to UKMS Money Solutions Limited, a PPI claims company, for sending more than 1.3 million spam texts. The ICO also fined Direct Security Marketing Ltd £70,000 in February 2016 for making almost 40,000 automated calls in just one day in an attempt to sell burglar alarms, almost 10,000 of which were made between 1am and 6am.

Enforcement action for data breaches is another enforcement trend. For examples of recent cases of enforcement action taken by the ICO for failure to comply with Principle 7 of the DPA, see question 14.2. Other notable fines include Staysure.co.uk, an online holiday insurance company, fined £175,000 by the ICO after IT security failings let hackers access more than 5,000 customer records, and the British Pregnancy Advice Service, a not-for-profit charity, fined £200,000 for a security flaw on its website that led to the data of over 10,000 women being accessed by a hacker.

16.2 What "hot topics" are currently a focus for the data protection regulator?

EU General Data Protection Regulation and the Directive on data protection and law enforcement: With final drafts due in the first few months of 2016, the ICO is now stepping up its work to understand the implications of the new legislation and what more it will need to do to prepare for implementation in order to understand the guidance and advice data controllers may need, and how the new regulatory process will need to work.

Privacy seals: The ICO is developing a privacy seal certification which will enable organisations which have been awarded a privacy seal to use the seal externally to show that they are demonstrating best practice when processing personal data. It will function as a trust mark. The ICO is working with the UK Accreditation Service ("**UKAS**") and other stakeholders to develop a framework criteria to select privacy seal scheme operators to which an organisation will make its application for a privacy seal.

Release of consumer data: Another government initiative, the Midata programme, encourages the release of consumer data back to individuals in reusable form. Bank customers can now download a file of their financial transactions and use this to find the best current account for them, and this is now being adopted by energy providers. The ICO is actively advising on the programmes' privacy concerns.

Bridget Treacy
Hunton & Williams
30 St Mary Axe
London, EC3A 8EP
United Kingdom

Tel: +44 207 220 5600
Fax: +44 207 220 5772
Email: btreacy@hunton.com
URL: www.hunton.com

Bridget Treacy leads Hunton & Williams' UK Privacy and Cybersecurity team and is also the Managing Partner of the firm's London office. Her practice focuses on all aspects of privacy, data protection, information governance and e-commerce issues for multinational companies across a broad range of industry sectors. Bridget's background in complex technology transactions enables her to advise on the specific data protection and information governance issues that occur in a commercial context. Bridget is the editor of the specialist privacy journal, *Privacy and Data Protection*, and has contributed to a number of published texts. According to *Chambers UK*, "she is stellar, one of the leading thinkers on data protection, providing practical solutions to thorny legal issues".

Stephanie Iyayi
Hunton & Williams
30 St Mary Axe
London, EC3A 8EP
United Kingdom

Tel: +44 207 220 5608
Fax: +44 207 220 5772
Email: siyayi@hunton.com
URL: www.hunton.com

Stephanie Iyayi is an Associate in Hunton & Williams' UK Privacy and Cybersecurity team. She advises clients on all areas of UK and EU data protection law. Stephanie works on large multi-jurisdictional data protection compliance projects, including data breach incidents, employee monitoring and data retention, cross-border data transfers and other technology, media and telecommunications matters.

HUNTON& WILLIAMS

Hunton & Williams' Global Privacy and Cybersecurity practice is a leader in its field. It has been ranked by *Computerworld* for four consecutive years as the top law firm globally for privacy and data security. *Chambers & Partners* ranks Hunton & Williams as the top privacy and data security practice in its *Chambers & Partners UK*, *Chambers Global*, *Chambers Europe* and *Chambers USA* guides.

The team of more than 25 privacy professionals, spanning three continents and five offices, is led by Lisa Sotto, who was named among the *National Law Journal*'s "100 Most Influential Lawyers". With lawyers qualified in six jurisdictions, the team includes internationally-recognised partners Bridget Treacy and Wim Nauwelaerts, former FBI cybersecurity counsel Paul Tiao, and former UK Information Commissioner Richard Thomas.

In addition, the firm's Centre for Information Policy Leadership, led by Bojana Bellamy, collaborates with industry leaders, consumer organisations and government agencies to develop innovative and pragmatic approaches to privacy and information security.

USA

Aaron P. Simpson

Hunton & Williams

Chris D. Hydak

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

There is no comprehensive, consolidated data protection law in the U.S. Data protection in the U.S. is primarily regulated through a number of (i) sector specific federal laws, and (ii) state laws.

1.2 Is there any other general legislation that impacts data protection?

Section 5 of the Federal Trade Commission Act prohibits "unfair or deceptive acts or practices in or affecting commerce". The Federal Trade Commission ("FTC") has brought several enforcement actions under Section 5 of the FTC Act related to data processing practices which it considers unfair or deceptive.

1.3 Is there any sector specific legislation that impacts data protection?

Yes, there are several sector specific laws that impact data protection. For example, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") applies to protected health information and the Gramm-Leach-Bliley Act ("GLB") applies to financial institutions and "nonpublic personal information." Below are additional examples of federal sector specific laws that impact data protection:

- The Children's Online Privacy Protection Act ("COPPA") regulates the online collection and processing of the personal data of children under the age of 13.
- The Telecommunications Act regulates telecommunications carriers' use of customer information.
- The Fair Credit Reporting Act ("FCRA") and the Fair and Accurate Credit Transactions Act govern data protection in the consumer reporting industry.
- The Video Privacy Protection Act restricts certain entities from processing personal data that identifies a consumer as having requested or obtained specific video materials or services.

1.4 What is the relevant data protection regulatory authority(ies)?

There are a number of regulatory authorities with respect to data protection, including the FTC, the Consumer Financial Protection Bureau, the Department of Health and Human Services ("HHS") and the 50 state Attorneys General.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **"Personal Data"**

  There is no overarching definition of "personal data" under relevant U.S. laws. Each law has its own definition of personal data.
- **"Sensitive Personal Data"**

  U.S. laws generally do not define "sensitive personal data". Certain U.S. laws, however, do provide heightened requirements for certain elements of personal data. For example, many state laws restrict an entity's ability to process Social Security numbers. State laws often impose notification requirements when there are security breaches involving certain data elements deemed sensitive.
- **"Processing"**

  Relevant U.S. laws generally do not define "processing", but in practice processing typically includes collection, usage, storage, disclosure and disposal.
- **"Data Controller"**

  Relevant U.S. laws do not define "data controller". There are similar concepts under certain U.S. laws, however. For example, U.S. state breach notification laws often include the concept of "data owners", which are typically entities that own or license the pertinent information.
- **"Data Processor"**

  Relevant U.S. laws do not define "data processor". Similar to "data controller", however, there are similar concepts under certain U.S. laws.
- **"Data Subject"**

  Relevant U.S. laws do not define "data subject".
- *Other key definitions – please specify (e.g., "Pseudonymous Data", "Direct Personal Data", "Indirect Personal Data")*
  - **"Pseudonymous Data"**

    Relevant U.S. laws do not define "pseudonymous data".
  - **"Direct Personal Data"**

    Relevant U.S. laws do not define "direct personal data".
  - **"Indirect Personal Data"**

    Relevant U.S. laws do not define "indirect personal data".

- **"Data Owner"**

  Certain U.S. laws (e.g., state breach notification laws) refer to data owners. Typically, these are entities that own or license the relevant information (i.e., not data subjects or service providers).

3 Key Principles

3.1 What are the key principles that apply to the processing of personal data?

- **Transparency**

  There are no overarching principles derived from law for processing personal data. Certain U.S. laws require entities to provide notice when they collect or process certain data. For example, two state laws (i.e., the California Online Privacy Protection Act ("CalOPPA") and the Delaware Online and Personal Privacy Protection Act ("DOPPPA")) require operators of websites and mobile apps to include a notice detailing certain of their information processing practices for data collected through the website or mobile app.

- **Lawful basis for processing**

  There is no overarching requirement to have a lawful basis to process personal data. U.S. laws do, however, restrict an entity's ability to process personal data in certain circumstances. For example, certain state laws restrict retailers from collecting or processing personal data at the point-of-sale when a customer purchases merchandise with a payment card.

- **Purpose limitation**

  There is no overarching principle regarding purpose limitation but certain U.S. laws do require entities to notify individuals of the purposes for which they may collect and process their personal data. In addition, the FTC regularly brings enforcement actions against companies that materially deviate from the purposes for which they collected the information (as articulated in their privacy notice).

- **Data minimisation**

  While there is no overarching principle regarding data minimisation, the FTC has recommended that companies adhere to the principle by only collecting data needed for a specific purpose.

- **Proportionality**

  There is no overarching principle regarding proportionality.

- **Retention**

  There are over 13,000 records retention laws at the state and federal level in the U.S. These laws generally are not specific to personal data but are important to comply with in order to appropriately safeguard records containing personal data.

- *Other key principles – please specify*

  There are no other key principles in particular.

4 Individual Rights

4.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Access to data**

  U.S. laws generally do not provide individuals with a right to access their data. Certain U.S. laws (e.g., HIPAA), however, do provide individuals with access rights.

- **Correction and deletion**

  U.S. laws generally do not provide individuals with a right to correct or delete their data. Certain U.S. laws (e.g., FCRA), however, do grant individuals the right to dispute incomplete or inaccurate information and impose a duty on certain entities to correct the inaccurate or incomplete information.

- **Objection to processing**

  U.S. laws generally do not provide individuals with a right to object to the processing of their data.

- **Objection to marketing**

  Many sector specific U.S. laws allow individuals to object to being contacted for marketing purposes. For example, the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM") requires that entities sending marketing or promotional emails to consumers provide a mechanism for consumers to opt out from future marketing or promotional emails.

- **Complaint to relevant data protection authority(ies)**

  U.S. consumers may report violations of relevant privacy laws to government regulators, such as the FTC and state Attorneys General, but there are no data protection-specific regulators in the U.S. at this time.

- *Other key rights – please specify*

  There are no other key rights in particular.

5 Registration Formalities and Prior Approval

5.1 In what circumstances is registration or notification required to the relevant data protection regulatory authority(ies)? (E.g., general notification requirement, notification required for specific processing activities.)

There are no circumstances in which an organisation has to register or notify a data protection authority prior to the general processing of personal data. There are notification requirements with respect to data breaches, as discussed in section 13.

5.2 On what basis are registrations/notifications made? (E.g., per legal entity, per processing purpose, per data category, per system or database.)

This is not applicable.

5.3 Who must register with/notify the relevant data protection authority(ies)? (E.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation.)

This is not applicable.

5.4 What information must be included in the registration/notification? (E.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes.)

This is not applicable.

5.5 What are the sanctions for failure to register/notify where required?

This is not applicable.

5.6 What is the fee per registration (if applicable)?

This is not applicable.

5.7 How frequently must registrations/notifications be renewed (if applicable)?

This is not applicable.

5.8 For what types of processing activities is prior approval required from the data protection regulator?

This is not applicable.

5.9 Describe the procedure for obtaining prior approval, and the applicable timeframe.

This is not applicable.

6 Appointment of a Data Protection Officer

6.1 Is the appointment of a Data Protection Officer mandatory or optional?

There is no U.S. law with respect to appointing a Data Protection Officer. "Covered entities" under HIPAA, however, must appoint a privacy officer.

6.2 What are the sanctions for failing to appoint a mandatory Data Protection Officer where required?

This is not applicable.

6.3 What are the advantages of voluntarily appointing a Data Protection Officer (if applicable)?

This is not applicable.

6.4 Please describe any specific qualifications for the Data Protection Officer required by law.

This is not applicable.

6.5 What are the responsibilities of the Data Protection Officer, as required by law or typical in practice?

This is not applicable.

6.6 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

This is not applicable.

7 Marketing and Cookies

7.1 Please describe any legislative restrictions on the sending of marketing communications by post, telephone, email, or SMS text message. (E.g., requirement to obtain prior opt-in consent or to provide a simple and free means of opt-out.)

Post – This is not applicable.

Telephone and SMS text message – Among other relevant laws, the Telephone Consumer Protection Act ("TCPA") requires that entities obtain the "prior express written consent" of a consumer before marketing to him or her via a telephone call or SMS text message to a mobile phone sent using auto dialling equipment or a prerecorded or artificial voice. The TCPA also requires "prior express written consent" for calls to residential lines using an artificial or prerecorded voice.

Email – CAN-SPAM requires entities marketing via email to provide consumers with a clear and conspicuous mechanism for opting out of future marketing emails.

7.2 Is the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

The FTC is active in enforcing violations of the Telemarketing Sales Rule ("TSR"), which is similar to the TCPA in that it requires prior consumer consent for telemarketing calls. In addition, the Federal Communications Commission ("FCC") is somewhat active in enforcing the TCPA but, as the TCPA contains a private right of action, the vast majority of TCPA litigation is initiated by private plaintiffs, not the FCC. Accordingly, entities that conduct telemarketing are generally more concerned with the TCPA than the TSR because the TCPA (i) provides aggrieved consumers with a private right of action, and (ii) is broader in scope than the TSR. The FTC also is active in enforcing against companies that use personal data, including with respect to marketing, in ways that materially deviate from representations they have made in public.

7.3 Are companies required to screen against any "do not contact" list or registry?

Generally, telemarketers are required to screen against the national do-not-call registry.

7.4 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

Each email that violates CAN-SPAM is subject to a maximum penalty of $16,000. Each telephone call or text message that violates the TCPA is subject to a maximum penalty of $1,500.

7.5 What types of cookies require explicit opt-in consent, as mandated by law or binding guidance issued by the relevant data protection authority(ies)?

No type of cookies requires opt-in consent.

7.6 For what types of cookies is implied consent acceptable, under relevant national legislation or binding guidance issued by the relevant data protection authority(ies)?

There is no U.S. law specifically addressing consent to cookies. CalOPPA and DOPPPA do require, in certain circumstances, operators of commercial websites and online services that collect personal data to disclose (i) how the operator responds to "do not track" signals from web browsers, and (ii) whether third parties on the operator's website or online service may collect personal data about users' online activities over time and across third-party websites.

7.7 To date, has the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

The FTC has brought enforcement actions related an entity's information processing practices that included cookie use. For example, the FTC has brought enforcement actions against companies alleged to have violated COPPA or Section 5 of the FTC Act through, in part, their use of cookies.

7.8 What are the maximum penalties for breaches of applicable cookie restrictions?

There is no U.S. law that specifically addresses cookies.

8 Restrictions on International Data Transfers

8.1 Please describe any restrictions on the transfer of personal data abroad?

There are no restrictions on cross-border transfers of personal data.

8.2 Please describe the mechanisms companies typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions.

This is not applicable.

8.3 Do transfers of personal data abroad require registration/notification or prior approval from the relevant data protection authority(ies)? Describe which mechanisms require approval or notification, what those steps involve, and how long they take.

This is not applicable.

9 Whistle-blower Hotlines

9.1 What is the permitted scope of corporate whistle-blower hotlines under applicable law or binding guidance issued by the relevant data protection authority(ies)? (E.g., restrictions on the scope of issues that may be reported, the persons who may submit a report, the persons whom a report may concern.)

The Sarbanes-Oxley Act ("SOX") requires publicly listed companies to implement a whistle-blowing hotline or other complaint notification system for the receipt of complaints related to accounting, internal accounting controls or auditing matters. SOX also provides protections to restrict retaliatory actions against whistle-blowers. There are no limitations, however, imposed by data protection or other laws on the scope of whistle-blower hotlines with respect to (i) issues that may be reported, (ii) the persons who may submit a report, or (iii) the persons whom a report may concern.

9.2 Is anonymous reporting strictly prohibited, or strongly discouraged, under applicable law or binding guidance issued by the relevant data protection authority(ies)? If so, how do companies typically address this issue?

This is not applicable.

9.3 Do corporate whistle-blower hotlines require separate registration/notification or prior approval from the relevant data protection authority(ies)? Please explain the process, how long it typically takes, and any available exemptions.

This is not applicable.

9.4 Do corporate whistle-blower hotlines require a separate privacy notice?

This is not applicable.

9.5 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

If a workforce is unionised, the trade union would need to be notified or consulted only if the agreement between the union and the employer requires notification or consultation, which is unlikely.

10 CCTV and Employee Monitoring

10.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies)?

No, it does not.

10.2 What types of employee monitoring are permitted (if any), and in what circumstances?

All types of employee monitoring (e.g., monitoring phone calls, computer use, email use, etc.) are permitted if the monitoring is for a legitimate business purpose. In addition, employee monitoring without a legitimate business purpose may be permitted in certain circumstances (e.g., with notice and consent). However, certain monitoring activities that would be highly offensive, such as using CCTV in the employee lavatory, are generally not permitted.

10.3 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Certain U.S. laws require employers to provide notice of electronic employee monitoring. Neither notice for other forms of monitoring nor consent is strictly required to monitor employees for a legitimate

business purpose. Many employers in the U.S., however, provide notice and obtain consent to their monitoring practices to help ensure that data subjects clearly understand that monitoring is occurring. Notice and consent is typically obtained via an employee policy (e.g., an Acceptable Use Policy or specific monitoring policy) and/or a network login banner.

10.4 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

There is no data protection requirement to notify or consult with works councils, trade unions or employee representatives.

10.5 Does employee monitoring require separate registration/notification or prior approval from the relevant data protection authority(ies)?

No, it does not.

11 Processing Data in the Cloud

11.1 Is it permitted to process personal data in the cloud? If so, what specific due diligence must be performed, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

Yes, processing personal data in the cloud is permitted. There are no specific laws regarding processing personal data in the cloud.

11.2 What specific contractual obligations must be imposed on a processor providing cloud-based services, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

This is not applicable.

12 Big Data and Analytics

12.1 Is the utilisation of big data and analytics permitted? If so, what due diligence is required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

Yes, it is permitted. There is no specific diligence required under applicable law or binding guidance to use big data and analytics in the U.S.

13 Data Security and Data Breach

13.1 What data security standards (e.g., encryption) are required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

There are no overarching data security standards imposed by U.S. law. Certain sector specific federal laws impose data security requirements on particular entities. For example, GLB requires financial institutions to implement an information security programme, and regularly monitor and test the information security programme. HIPAA requires covered entities and business associates to take specific steps to safeguard electronically protected health information, including the implementation of administrative, physical and technical safeguards. In addition, some U.S. states have enacted laws imposing minimum information security requirements on entities that process information about a resident of those states. The most stringent of these state laws is the Massachusetts law, which requires, among other items, that applicable organisations develop, implement and maintain a comprehensive and written information security programme. The Massachusetts law requires the encryption of (i) files containing personal data that are transmitted across public networks, and (ii) data containing personal data that is transmitted wirelessly.

13.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.

Yes, there is a legal requirement to report data breaches to certain data protection authorities. Approximately 20 states require entities to report data breaches to the relevant state regulator, such as the Attorney General. The exact requirements regarding the details and timeframe vary among the state laws. Most states do not include a requirement to provide notification within a prescribed timeframe, but some do. For example, Puerto Rico's breach notification law requires notice to the relevant regulator within 10 days after the incident has been detected and Vermont's law requires a preliminary notice within 14 business days of the date of discovery. The requirements regarding the content of the notice to government regulators vary, but generally include a description of the breach, the types of information impacted and what the entity has done to mitigate risk to affected individuals.

In addition, certain sector specific federal laws require entities to notify regulators in the event of a data breach. For example, the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice requires financial institutions to notify their primary federal regulator. The Health Information Technology for Economic and Clinical Health ("HITECH") Act requires entities to notify HHS immediately for breaches that affect the protected health information of more than 500 individuals. Breaches that affect the protected health information of fewer than 500 individuals must be reported to HHS annually. HHS provides an electronic form for entities to report breaches. The form requests information such as a description of the breach and the subsequent actions taken by the entity to respond to the breach.

13.3 Is there a legal requirement to report data breaches to individuals? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.

Forty-seven U.S. states, the District of Columbia, Guam, Puerto Rico and the U.S. Virgin Islands have enacted data breach notification statutes requiring entities to notify affected individuals in the event of a data breach. The laws vary but generally require notification to affected individuals in the most expedient time possible and without unreasonable delay. Some state laws, however, require notification within a prescribed timeframe (e.g., 30 days in Florida). The content requirements regarding what information must be contained

in the notice to affected individuals vary among the relevant laws. Generally, however, the state data breach notification laws require the notice to contain a general description of the incident, the types of information affected and contact information where affected individuals may obtain additional information. With respect to federal laws, the HITECH Act requires notification to affected individuals within 60 days.

13.4 What are the maximum penalties for security breaches?

There are no penalties simply for suffering a data breach. There can be penalties, however, if a breached company did not or does not comply with relevant federal or state data breach notification statutes, information security statutes or other applicable laws. In addition, there can be penalties associated with a breach if a company was negligent, reckless, made deceptive comments about its information security practices or its information security practices were lax enough to be deemed "unfair".

Penalties can include enforcement actions from government regulators and class action lawsuits initiated by impacted individuals. The maximum penalties depend on the law at issue.

14 Enforcement and Sanctions

14.1 Describe the enforcement powers of the data protection authority(ies):

The data protection authorities have wide-ranging enforcement powers, including the authority to issue civil investigative demands, subpoenas and generally investigate a company's information processing practices. Additionally, the enforcement authorities can impose sanctions, such as monetary penalties, and affirmative obligations, such as a mandate to implement a comprehensive information security programme, submit to independent audits and submit compliance reports on a regular basis to the relevant data protection authority. Often the requirement to implement a comprehensive information security programme includes monitoring by the authority for a lengthy period (e.g., 20 years).

14.2 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

There are numerous regulators with authority to bring actions related to data protection and they do not follow a common approach. The FTC is the most active federal regulator in the data protection arena. A recent federal court decision related to an FTC enforcement action against a large hotel chain regarding the hotel chain's information security practices buttressed the FTC's authority to bring enforcement actions related to information security standards and practices. As a result of the decision, the FTC (and potentially other government regulators) may be more emboldened to bring future actions related to information security and data protection.

15 E-discovery / Disclosure to Foreign Law Enforcement Agencies

15.1 How do companies within your jurisdiction respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

There is no particular rule regarding how U.S. companies may respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies.

15.2 What guidance has the data protection authority(ies) issued?

No guidance has been used.

16 Trends and Developments

16.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

During the previous 12 months, there have been a few trends with respect to the enforcement of data protection laws. For example, it is becoming rather common, at both the federal and state levels, for regulators to send organisations that suffered a data breach written request for information regarding the breach, such as what specific information security measures the organisation had in place prior to the breach and what information security measures the organisation is implementing to correct any vulnerabilities identified as a result of the breach. Also within the previous 12 months, the FTC has brought several privacy and data security-related enforcement actions. For example, the FTC brought and settled enforcement actions against (i) a technology company that allows retailers to track consumer movement in-store alleging that the technology company misrepresented consumers' ability to opt out of such in-store tracking, and (ii) multiple data brokers alleging that the data brokers failed to provide reasonable security to protect consumer financial information. The FTC also recently released a report on the Internet of Things ("IoT"), which stated that the FTC will use its enforcement authority to bring actions against entities in the IoT space that violate laws the FTC has the authority to enforce.

In addition, the FCC has entered the information security arena. In October 2014, the FCC brought its first enforcement actions related to information security against two telecommunications carriers for allegedly failing to adequately safeguard their customers' personal data. In November 2015, the FCC settled its first information security-related enforcement action against a cable provider after the cable provider was the target of a cyberattack that compromised the personal data of certain of the provider's current and former customers.

16.2 What "hot topics" are currently a focus for the data protection regulator?

As described in question 16.1 above, cybersecurity remains a "hot topic" in the U.S. and is a priority for the Obama administration. In addition, Congress passed the Cybersecurity Information Sharing Act ("CISA"), which President Obama signed into law on December 18, 2015. CISA facilitates and encourages the sharing of Internet traffic information between and among the private sector and the federal government to prevent cyberattacks. The mobile ecosystem and the IoT are "hot topics" as well.

The transfer of personal data from the European Union ("EU") to the U.S. became a "hot topic" in October 2015 when the Court of Justice of the European Union ruled the U.S.-EU Safe Harbour invalid. Subsequent to the invalidation of Safe Harbour, the U.S. Department of Commerce and the European Commission reached agreement on the Privacy Shield, which will (if implemented) replace Safe Harbour as a valid basis for transferring personal data from the EU to the U.S. The European Commission released the legal texts that will implement the Privacy Shield on February 29, 2016. These legal texts must be approved by the College of Commissioners before the Privacy Shield is implemented.

Aaron P. Simpson
Hunton & Williams
200 Park Avenue
New York, NY 10166
USA

Tel: +1 212 309 1126
Email: asimpson@hunton.com
URL: www.hunton.com

Aaron P. Simpson is a partner in the New York office of Hunton & Williams. He advises clients on a broad range of complex privacy and cybersecurity matters, including state, federal and international privacy and data security requirements, and the remediation of large-scale data security incidents. He helps clients identify, evaluate and manage risks associated with their collection and use of information. Aaron is well-known as a top privacy professional and has been recognised by *Chambers & Partners*, *New York Super Lawyers*, *Computerworld* and *The Legal 500* for his work on behalf of clients. He is a sought-after media resource on privacy issues and has been quoted in publications such as *Bloomberg Businessweek Magazine*, *DataGuidance* and *TIME Magazine*. Aaron regularly speaks before industry groups, legal organisations, government agencies and educational institutions at conferences, seminars, roundtables and webinars. He has written and co-written numerous articles, book chapters and handbooks on privacy and cybersecurity issues.

Chris D. Hydak
Hunton & Williams
200 Park Avenue
New York, NY 10166
USA

Tel: +1 212 309 1012
Email: chydak@hunton.com
URL: www.hunton.com

Chris D. Hydak is an associate in the New York office of Hunton & Williams. He assists clients in identifying and managing privacy and information security risks, and advises clients on federal, state and international privacy obligations. His practice includes advising a wide array of clients including financial services businesses, technology companies, media companies, retailers, manufacturers and telecommunications companies. He has also assisted clients in the aftermath of a data breach, including in connection with a Federal Trade Commission investigation and subsequent enforcement action in federal court.

HUNTON& WILLIAMS

Hunton & Williams' Global Privacy and Cybersecurity practice is known throughout the world for its deep experience, breadth of knowledge and outstanding client service. *Chambers & Partners*, *The Legal 500* and *Computerworld* have named Hunton & Williams as a top firm for privacy and cybersecurity. In addition to our legal practice, we distinguish ourselves through our Centre for Information Policy Leadership, which boasts the active participation of more than 35 leading multinational corporations. For the latest resources in privacy, data protection and cybersecurity, visit www.huntonprivacyblog.com and www.huntonregulationtracker.com.