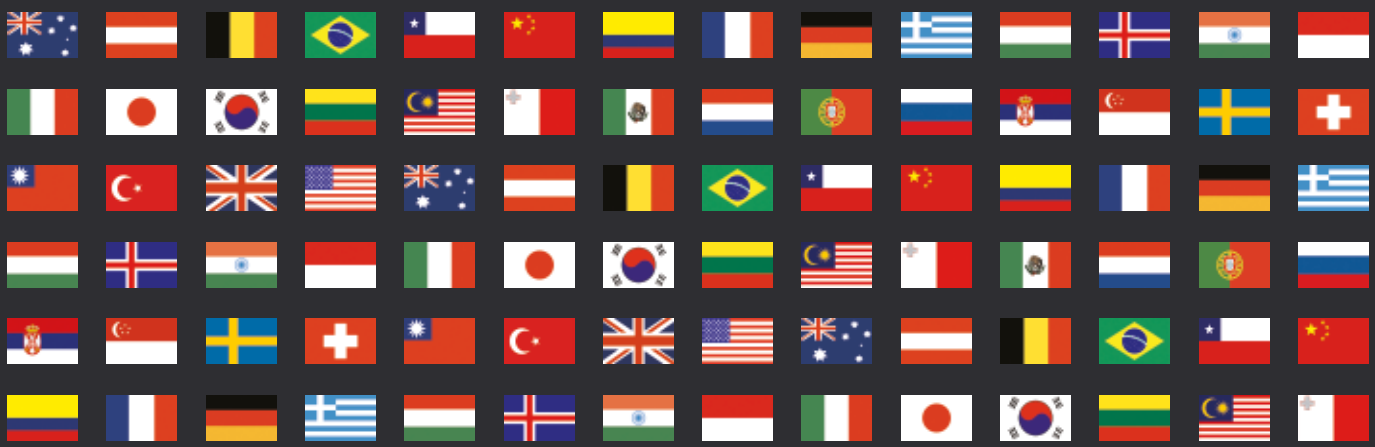
Data Protection & Privacy 2020

Contributing editors
Aaron P Simpson and Lisa J Sotto
Hunton Andrews Kurth LLP



LEXOLOGY
Getting The Deal Through

HUNTON
ANDREWS KURTH

© Law Business Research 2019

HUNTON
ANDREWS KURTH

Leaders in Privacy and Cybersecurity

Keep the trust you've earned.

Complying with global privacy, data protection and cybersecurity rules is challenging, especially for businesses that operate across borders. Our top-ranked privacy team, in combination with the firm's Centre for Information Policy Leadership, advises on all aspects of US and European data protection law and cybersecurity events. We help businesses develop global compliance frameworks addressing regulatory obligations in the US, the EU and across the world. The firm is widely recognized globally as a leading privacy and data security firm.

For more information, visit www.huntonprivacyblog.com.

©2019 Hunton Andrews Kurth LLP | HuntonAK.com

© Law Business Research 2019

Publisher
Tom Barnes
tom.barnes@lbresearch.com

Subscriptions
Claire Bagnall
claire.bagnall@lbresearch.com

Senior business development managers
Adam Sargent
adam.sargent@gettingthedealthrough.com

Dan White
dan.white@gettingthedealthrough.com

Published by
Law Business Research Ltd
87 Lancaster Road
London, W11 1QQ, UK
Tel: +44 20 3780 4147
Fax: +44 20 7229 6910

The information provided in this publication is general and may not apply in a specific situation. Legal advice should always be sought before taking any legal action based on the information provided. This information is not intended to create, nor does receipt of it constitute, a lawyer–client relationship. The publishers and authors accept no responsibility for any acts or omissions contained herein. The information provided was verified between June and July 2019. Be advised that this is a developing area.

© Law Business Research Ltd 2019
No photocopying without a CLA licence.
First published 2012
Eighth edition
ISBN 978-1-83862-146-9

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112

Data Protection & Privacy

2020

Contributing editors
Aaron P Simpson and Lisa J Sotto
Hunton Andrews Kurth LLP

Lexology Getting The Deal Through is delighted to publish the eighth edition of *Data Protection and Privacy*, which is available in print and online at www.lexology.com/gtdt.

Lexology Getting The Deal Through provides international expert analysis in key areas of law, practice and regulation for corporate counsel, cross-border legal practitioners, and company directors and officers.

Throughout this edition, and following the unique Lexology Getting The Deal Through format, the same key questions are answered by leading practitioners in each of the jurisdictions featured. Our coverage this year includes new chapters on Hungary, Iceland, Indonesia and Malaysia.

Lexology Getting The Deal Through titles are published annually in print. Please ensure you are referring to the latest edition or to the online version at www.lexology.com/gtdt.

Every effort has been made to cover all matters of concern to readers. However, specific legal advice should always be sought from experienced local advisers.

Lexology Getting The Deal Through gratefully acknowledges the efforts of all the contributors to this volume, who were chosen for their recognised expertise. We also extend special thanks to the contributing editors, Aaron P Simpson and Lisa J Sotto of Hunton Andrews Kurth LLP, for their continued assistance with this volume.

LEXOLOGY
Getting The Deal Through

London
July 2019

Reproduced with permission from Law Business Research Ltd
This article was first published in August 2019
For further information please contact editorial@gettingthedealthrough.com

© Law Business Research 2019

Contents

© Law Business Research 2019

© Law Business Research 2019

United Kingdom

Aaron P Simpson, James Henderson and Jonathan Wright
Hunton Andrews Kurth LLP

LAW AND THE REGULATORY AUTHORITY

Legislative framework

1 Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?

The primary legal instruments include the UK's Data Protection Act 2018 (DPA) and the EU's General Data Protection Regulation 2016/679 (GDPR) on the protection of individuals with regard to the processing of PII and the free movement of data. The UK is a signatory to Treaty 108 of the Council of Europe. The UK has no national constitutional privacy provisions but is bound by the EU Charter of Fundamental Rights.

In the 2016 referendum, the UK voted to leave the EU. In March 2017, the UK's government formally notified the EU of the UK's referendum decision, triggering Article 50 of the EU's Lisbon Treaty. This signalled the beginning of the process of leaving the EU. The UK had been due to leave the EU on 29 March 2019, two years after it started the exit process by invoking Article 50. However, the withdrawal agreement reached between the EU and UK has been rejected three times by UK MPs. Having granted an initial extension of the Article 50 process until 12 April 2019, EU leaders have now backed a six-month extension until 31 October 2019, at which point the UK is expected to leave the EU. That said, the UK will leave before this date if the withdrawal agreement is ratified by the UK and the EU before this date. While the process of 'Brexit' is under way, it remains unclear what future trading arrangements will be agreed between the UK and the EU. If the UK seeks to remain part of the EEA, it will need to continue to adopt EU laws, including the GDPR. If the UK is outside the EU or EEA, the UK has confirmed that it will seek adequacy status to enable data flows between the UK and the EEA. This will require data protection laws that are essentially equivalent to EU data protection laws (ie, GDPR) but may be complicated by the UK's Investigatory Powers Act 2016, which permits the type of bulk surveillance practices that the Court of Justice of the European Union believes fail to respect data protection principles. Further, non-EU controllers or processors that process the PII of EU data subjects in the context of offering goods or services to them or monitoring their behaviour will be subject to the GDPR in any event.

Data protection authority

2 Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

The DPA and the GDPR are supervised by the Information Commissioner's Office (ICO). The ICO may:

- seek entry to premises subject to a warrant issued by a court;
- require the provision of information by service of information notices;
- by notice, require government departments to undergo a mandatory audit (referred to as 'assessment'); and
- conduct audits of private sector organisations with the consent of the organisation.

Cooperation with other data protection authorities

3 Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches??

The ICO participates in the 'one-stop shop' under the GDPR, under which organisations with a main establishment in the EU may primarily be regulated by the supervisory authority of the jurisdiction in which the main establishment is located (lead supervisory authority). The DPA and the GDPR confer on the ICO powers to participate in the GDPR's one-stop shop, to cooperate with other concerned supervisory authorities, to request from and provide mutual assistance to other concerned supervisory authorities, and to conduct joint operations, including joint investigations and joint enforcement actions with other concerned supervisory authorities. The status of the ICO's participation in the EU's one-stop shop once the UK has left the EU is currently not clear, but in the absence of an agreement stating otherwise, the ICO will no longer be permitted to participate in the GDPR's one-stop shop mechanism. This eventuality would impact UK-based data controllers or data processors that are currently carrying out cross-border processing of PII, across EU member state borders.

The DPA also requires the ICO, in relation to third countries and international organisations, to take steps to develop cooperation mechanisms to facilitate the effective enforcement of legislation relating to the protection of personal data, to provide international mutual assistance in the enforcement of legislation for the protection of personal data, to engage relevant stakeholders in discussion and activities, and to promote the exchange and documentation of legislation and practice for the protection of personal data.

Breaches of data protection

4 Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

The ICO has a number of enforcement powers. Where a data controller or a data processor breaches data protection law, the ICO may:

- issue undertakings committing an organisation to a particular course of action to improve its compliance with data protection requirements;

© Law Business Research 2019

- serve enforcement notices and 'stop now' orders where there has been a breach, requiring organisations to take (or refrain from taking) specified steps, to ensure they comply with the law; and
- issue fines of up to the greater of €20 million or 4 per cent of annual worldwide turnover, depending on the nature of the violation of the DPA and GDPR.

A number of breaches may lead to criminal penalties. The following may constitute criminal offences:

- making a false statement in relation to an information notice validly served by the ICO;
- destroying, concealing, blocking or falsifying information with the intention of preventing the ICO from viewing or being provided with the information;
- unlawfully obtaining PII;
- knowingly or recklessly re-identifying PII that is de-identified without the consent of the data controller responsible for that PII;
- altering PII so as to prevent disclosure of the information in response to a data subject rights request;
- requiring an individual to make a subject access request; and
- obstructing execution of a warrant of entry, failing to cooperate or providing false information.

Criminal offences can be prosecuted by the ICO or by or with the consent of the Director of Public Prosecutions.

SCOPE

Exempt sectors and institutions

5 Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

Exemptions from the full rigour of the law apply in some circumstances and for some instances of processing. A wide exemption applies to processing by individuals for personal and domestic use, but no sectors or institutions are outside the scope of the law. Recent European case law has clarified that this exemption applies only to 'purely domestic' or household activities, with no connection to a professional or commercial activity. This means that if PII is only used for such things as writing to friends and family or taking pictures for personal enjoyment, such use of PII will not be subject to the GDPR.

The GDPR and the DPA apply to private and public sector bodies. That said, the processing of PII by competent authorities for law enforcement purposes is outside the scope of the GDPR (e.g. the police investigating a crime). Instead, this type of processing is subject to the rules in Part 3 of the DPA. In addition, PII processed for the purposes of safeguarding national security or defence is also outside the scope of the GDPR. However, it is covered by Part 2, Chapter 3 of the DPA (also known as the 'applied GDPR'), which contains an exemption for national security and defence.

Communications, marketing and surveillance laws

6 Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

Electronic marketing is specifically regulated by the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) (as amended), although the GDPR and the DPA often apply to the same activities, to the extent that they involve the processing of PII. Interception and state surveillance are covered by the Investigatory Powers Act 2016 and the Regulation of Investigatory Powers Act 2000. The interception of business communications is regulated by the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

Other laws

7 Identify any further laws or regulations that provide specific data protection rules for related areas.

The law includes many provisions dealing with information; for example, the regulation of credit files is covered in the Consumer Credit Act 1974. Laws on e-commerce include provisions linked to the regulation of PII. Laws on defamation, copyright and computer misuse also affect data protection. However, there is no specific data protection sectoral legislation. The UK has a range of 'soft law' instruments, such as codes of practice for medical confidentiality or the management of information held for policing, that apply in specific sectoral areas.

The DPA requires the ICO to draw up and publish codes of practice that relate to data sharing, direct marketing, age-appropriate design and data protection and journalism.

While not specifically related to the protection of PII, the Network and Information Systems Regulations 2018 (NIS Regulations) are intended to establish a common level of security for network and information systems. The NIS Regulations aim to address, among other things, the threats posed by cyberattacks.

PII formats

8 What forms of PII are covered by the law?

The GDPR and the DPA cover PII held in electronic form plus such information held in structured files, called 'relevant filing systems'. In order to fall within this definition, the file must be structured by reference to individuals or criteria relating to them, so that specific information about a particular individual is readily accessible.

Ultimately, whether a manual file is part of a relevant filing system is a matter of fact as well as law, and must be considered on a case-by-case basis.

Extraterritoriality

9 Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

Organisations that are data controllers or data processors fall within the scope of the law if they are established in the UK and process PII in the context of that establishment, or if they are not established in the EU but offer goods or services to individuals located in the UK, or monitor the behaviour of individuals located in the UK.

A data controller or data processor is 'established' in the UK if it is resident in the UK, is incorporated or formed under the laws of England and Wales, Scotland or Northern Ireland, or maintains and carries on activities through an office, branch, agency or other stable arrangements in the UK. Where a data controller or data processor is established in the UK, the DPA will apply regardless of whether the processing takes place in the UK or not.

Data controllers established outside the EU that are subject to the GDPR and the DPA must nominate a representative in the UK.

© Law Business Research 2019

Covered uses of PII

10 Is all processing or use of PII covered? Is a distinction made between those who control or own PII and those who provide PII processing services to owners? Do owners', controllers' and processors' duties differ?

The GDPR and the DPA are applicable to data controllers (ie, those that decide the purposes and the means of the data processing) and data processors (who merely process PII on behalf of data controllers). As such, the data controllers are the main decision-makers and they exercise overall control over the purposes and means of the processing of PII. Data processors act on behalf of, and only on the instructions of, the relevant data controller.

LEGITIMATE PROCESSING OF PII

Legitimate processing – grounds

11 Does the law require that the holding of PII be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

The GDPR requires data controllers to rely on a legal ground set forth in the GDPR for all processing of PII. Additional conditions must also be satisfied when processing sensitive PII (see question 12).

The grounds for processing non-sensitive PII are:

- consent of the individual;
- performance of a contract to which the individual is party or in order to take steps at the request of the data subject prior to entering into a contract;
- compliance with a legal obligation, other than a contractual obligation (a legal obligation arising under the laws of a non-EU jurisdiction is not sufficient for the purposes of this ground);
- protection of the vital interests of the individual (ie, a life or death situation);
- the processing is necessary for carrying out public functions; or
- the processing is necessary for the legitimate interests of the data controller (or third parties to whom the PII is disclosed), unless overridden by the individual's fundamental rights, freedoms and legitimate interests.

Legitimate processing – types of PII

12 Does the law impose more stringent rules for specific types of PII?

Distinct grounds for legitimate processing apply to the processing of sensitive PII (also known as 'special categories of PII'). 'Sensitive' PII is defined as PII relating to:

- racial or ethnic origin;
- political opinions;
- religious or similar beliefs;
- trade union membership;
- physical or mental health;
- sex life or sexual orientation;
- genetic data;
- biometric data (when processed for the purpose of uniquely identifying a natural person);
- commissioning or alleged commissioning of any offence; or
- any proceedings for committed or alleged offences, the disposal of such proceedings of sentence of any court.

The GDPR sets forth a number of grounds that may be relied upon for the processing of sensitive PII, including:

- explicit consent of the individual;
- performance of employment law obligations;
- protection of the vital interests of the individual (ie, a life or death situation);
- processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the PII are not disclosed outside that body without the consent of the data subjects;
- the processing relates to PII that is manifestly made public by the data subject;
- the exercise of public functions;
- processing in connection with legal proceedings, legal advice or in order to exercise legal rights;
- processing for medical purposes;
- processing necessary for reasons of public interest in certain specific areas; or
- processing necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

In addition to the grounds set forth in the GDPR, the DPA sets forth a number of additional grounds that also may be relied upon, including:

- processing necessary for monitoring and ensuring equality of opportunity or treatment;
- preventing or detecting unlawful acts;
- preventing fraud;
- processing to comply with regulatory requirements relating to establishing whether a person has committed unlawful acts or has been involved in dishonesty, malpractice or other seriously improper conduct; and
- in connection with administering claims under insurance contracts or exercising rights and complying with obligations arising in connection with insurance contracts.

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PII

Notification

13 Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?

Data controllers are obliged to notify individuals of:

- the data controller's identity and contact information and, where applicable, the identity and contact information of its representative;
- the contact details of the data controller's data protection officer, if it has appointed one;
- the purposes for which the PII will be processed and the legal basis for processing;
- the legitimate interests pursued by the data controller, if applicable;
- the recipients or categories of recipients of the PII;
- the fact that the data controller intends to transfer the PII to a third country and the existence or absence of an adequacy decision by the European Commission, and a description of any safeguards (eg, EU Model Clauses) relied upon and the means by which individuals may obtain a copy of them;
- the period for which PII will be stored or the criteria used to determine that period;
- a description of the rights available to individuals;
- the existence of the right to withdraw consent at any time;
- the right to lodge a complaint with an EU data protection supervisory authority;

© Law Business Research 2019

- whether the provision of PII is a statutory or contractual requirement, or is necessary to enter into a contract, as well as whether the individual is obliged to provide the PII and of the consequences of failure to provide such PII; and
- the existence of automated decision-making and, if so, meaningful information about the logic involved as well as the significance and envisaged consequences of the processing for the individual.

When PII is obtained from a source other than the individual concerned, the data controller must also inform individuals of the source from which the PII originated and the categories of PII obtained.

Notice must be provided at the time the PII is collected from the data subject. When PII is obtained from a source other than the data subject it relates to, the data controller needs to provide the data subject with the notice:

- within a reasonable period of obtaining the PII and no later than one month;
- if the data controller uses the data to communicate with the data subject, at the latest, when the first communication takes place; or
- if the data controller envisages disclosure to someone else, at the latest, when the data controller discloses the data.

Exemption from notification

14 | When is notice not required?

Where PII is obtained from a source other than the data subject, then provision of notice is not required if:

- the individual already has the information;
- the provision of such information would be impossible or require disproportionate effort (in which case the data controller shall take appropriate measures to protect data subjects, including making the relevant information publicly available);
- the provision of the information would render impossible or seriously impair the achievement of the objectives of the processing
- obtaining or disclosure of the PII is required by EU law to which the data controller is subject; or
- where the PII is subject to an obligation of professional secrecy under UK or EU law.

Control of use

15 | Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

Individuals have a number of rights in relation to PII held by data controllers:

- to obtain confirmation of whether the data controller processes PII about the individual and to obtain a copy of that PII (also known as 'the right of access');
- to rectify PII that is inaccurate;
- to have PII erased in certain circumstances; for example, when the PII is no longer necessary for the purposes for which it was collected by the data controller;
- to restrict the processing of PII;
- to obtain a copy of PII in a structured, commonly used and machine-readable format, and to transmit that PII to a third-party data controller without hindrance, to the extent that it is technically feasible (also known as 'the right to data portability');
- to object to the processing of PII in certain circumstances; and
- not to be subject to decisions based solely on the automated processing of PII, except in particular circumstances.

Data processors are not required to comply with data subject rights requests, but are required to provide assistance to data controllers on whose behalf they process PII to respond to any such requests.

Data accuracy

16 | Does the law impose standards in relation to the quality, currency and accuracy of PII?

The data controller must ensure that PII is relevant, accurate and, where necessary, kept up to date in relation to the purpose for which it is held.

Amount and duration of data holding

17 | Does the law restrict the amount of PII that may be held or the length of time it may be held?

The data controller must ensure that PII is adequate, relevant and not excessive in relation to the purpose for which it is held. This means that the data controller should not collect or process unnecessary or irrelevant PII. The DPA and GDPR do not impose any specified retention periods. PII may be held only for as long as is necessary for the purposes for which it is processed.

Finality principle

18 | Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

PII may only be used for specified and lawful purposes, and may not be processed in any manner incompatible with those purposes. The purposes must be specified in the notice given to the individual.

In addition, recent case law has confirmed the existence of a tort of 'misuse of private information'. Under this doctrine, the use of private information about an individual for purposes to which the individual has not consented may give rise to a separate action in tort against the data controller, independent of any action taken under the DPA.

Use for new purposes

19 | If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

PII may not be processed for new purposes unless the further purposes are lawful (ie, based on a lawful ground; see question 11). It may be processed for a new purpose as long as that purpose is not incompatible with the original purpose, but notice of the new purpose must be provided to the individual. Where a new purpose would be incompatible with the original purpose, it must be legitimised by the consent of the individual unless an exemption applies. For example, PII may be further processed for certain specified public interest purposes, including the prevention of crime or prosecution of offenders and processing for research, historical or statistical purposes.

SECURITY

Security obligations

20 | What security obligations are imposed on PII owners and service providers that process PII on their behalf?

The DPA and GDPR do not specify the types of security measures that data controllers and data processors must take in relation to PII. Instead, data controllers and data processors must have in place 'appropriate technical and organisational measures' to protect against 'unauthorised or unlawful processing of [PII] and against accidental loss or destruction of, or damage to, [PII]'. In addition, the GDPR provides

© Law Business Research 2019

several examples of security measures that data controllers and data processors should consider implementing, including:

- the pseudonymisation and encryption of PII;
- the ability to restore the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability of and access to PII in a timely manner in the event of a physical or technical incident; and
- a process for regularly testing, assessing and evaluating the effectiveness of the measures implemented.

Under the relevant provisions, in assessing what is 'appropriate' in each case, data controllers and processors should consider the nature of the PII in question and the harm that might result from its improper use, or from its accidental loss or destruction. The data controller and processor must take reasonable steps to ensure the reliability of its employees.

Where a data controller uses an outsourced provider of services to process PII, it must choose a data processor providing sufficient guarantees of security, take reasonable steps to ensure that these are delivered, require the data processor to enter into a contract in writing under which the data processor will, among other things, act only on the instructions of the controller and apply equivalent security safeguards to those imposed on the data controller.

Notification of data breach

21 Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

The GDPR requires data controllers to notify the ICO of a data breach within 72 hours of becoming aware of the breach, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. In addition, data controllers must notify affected individuals of a breach without undue delay if the breach is likely to result in a high risk to the rights and freedoms of affected individuals. Data processors are not required to notify data breaches to supervisory authorities or to affected individuals, but data processors must notify the relevant data controller of a data breach without undue delay.

In addition to notifying breaches to the ICO and to affected individuals, data controllers must also document all data breaches and retain information relating to the facts of the breach, its effects and the remedial action taken.

INTERNAL CONTROLS

Data protection officer

22 Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

The GDPR requires data controllers and data processors to appoint a data protection officer if:

- the core activities of the data controller or data processor consist of processing operations that require regular and systematic monitoring of data subjects on a large scale; or
- the core activities of the data controller or processor consist of processing sensitive PII (see question 12) or PII relating to criminal offences and convictions on a large scale.

If appointed, the data protection officer is responsible for:

- informing and advising the data controller or data processor and its employees of their obligations pursuant to data protection law;
- monitoring compliance with the GDPR, awareness raising, staff training and audits;
- providing advice with regard to data protection impact assessments;
- cooperating with the ICO and other EU data protection supervisory authorities; and
- acting as a contact point for the ICO on issues relating to processing PII.

Organisations may also elect to appoint a data protection officer voluntarily, although such an appointment will need to comply with the requirements of the GDPR.

Record keeping

23 Are owners or processors of PII required to maintain any internal records or establish internal processes or documentation?

Data controllers and data processors are required to retain internal records that describe the processing of PII that is carried out. These records must be maintained and provided to the ICO upon request.

For data controllers, the record must include the following information:

- the name and contact details of the data controller and, where applicable, the joint controller, and of the data controller's representative and data protection officer;
- the purposes of the processing;
- the data subjects and categories of PII processed;
- the categories of recipients to whom PII has been or will be disclosed;
- a description of any transfers of PII to third countries and the safeguards relied upon;
- the envisaged time limits for erasure of the PII; and
- a general description of the technical and organisational security measures implemented.

For data processors the record must include the following information:

- the name and contact details of the processor and of each data controller on behalf of which the processor processes PII, and of the processor's representative and data protection officer;
- the categories of processing carried out on behalf of each data controller;
- a description of any transfers of PII to third countries and the safeguards relied upon; and
- a general description of the technical and organisational security measures implemented.

New processing regulations

24 Are there any obligations in relation to new processing operations?

Data controllers are required to carry out a data protection impact assessment in relation to any processing of PII that is likely to result in a high risk to the rights and freedoms of natural persons. In particular, a data protection impact assessment is required in respect of any processing that involves:

- the systematic and extensive evaluation of personal aspects relating to natural persons that is based on automated processing and on which decisions are made that produce legal effects concerning the natural person or that significantly affect the natural person;
- processing sensitive PII (see question 12) or PII relating to criminal convictions or offences on a large scale; or
- systematic monitoring of a publicly accessible area on a large scale.

A data protection impact assessment must be carried out in relation to all high-risk processing activities that meet the criteria above before the

© Law Business Research 2019

processing begins. The data protection impact assessment must include at least the following:

- a systematic description of the processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the data controller;
- an assessment of the proportionality and necessity of the processing in relation to the purposes;
- an assessment of the risks to the rights and freedoms of affected individuals; and
- information about the measures envisaged to address any risks to affected individuals (eg, safeguards, security measures, etc).

The GDPR also implements the concepts of 'data protection by design' and 'data protection by default'. In particular, this requires data controllers to implement appropriate technical and organisational measures in their processing systems to ensure that PII is processed in accordance with the GDPR, and to ensure that, by default, only PII that is necessary for each specific purpose is collected and processed. In addition, data controllers must ensure that by default PII is not made accessible to an indefinite number of persons without any intervention by the data subject.

REGISTRATION AND NOTIFICATION

Registration

25 | Are PII owners or processors of PII required to register with the supervisory authority? Are there any exemptions?

In the UK, data controllers are required to pay an annual registration fee to the ICO. There is no obligation to do so if any of the following applies:

- no processing is carried out on a computer (or other automated equipment);
- the processing is performed solely for the maintenance of a public register;
- the data controller is a not-for-profit organisation, and the processing is only for the purposes of establishing or maintaining membership or support of that organisation; or
- the data controller only processes PII for one or more of these purposes:
- staff administration;
- advertising, marketing and public relations;
- personal, family or household affairs;
- judicial functions; or
- accounts and records.

An entity that is a data processor only is not required to make this payment.

Formalities

26 | What are the formalities for registration?

There is a three-tier fee structure in the UK. Data controllers must pay a fee according to the following criteria:

- if the data controller has a maximum turnover of £632,000 or no more than 10 members of staff, £40;
- if the data controller has a maximum turnover of £36 million or no more than 250 members of staff, £60; or
- in all other cases, £2,900.

The data controller must include in the fee application its name, address, contact details of the person who is completing the fee registration and contact details of the data controller's data protection officer if it is required to appoint one, the number of staff members it has, the turnover for its financial year, and any other trading names it has. Data processors are not required to pay the registration fee.

Penalties

27 | What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

PII must not be processed unless the data controller has paid the required fee.

If the data controller has not paid a fee when required to do so or has not paid the correct fee, it may be subject to a fixed monetary penalty of 150 per cent of the highest charge payable by a data controller (ie, £4,350). As previously noted, an entity that is a data processor only (and not a data controller) is not required to register or pay the fee.

Refusal of registration

28 | On what grounds may the supervisory authority refuse to allow an entry on the register?

The ICO has no power to refuse the application provided that it is made in the prescribed form and includes the applicable fee.

Public access

29 | Is the register publicly available? How can it be accessed?

The fee register is publicly available, free of charge, from the ICO's website (https://ico.org.uk/esdwebpages/search).

A copy of the register on DVD may also be requested by sending an email to accessICOinformation@ico.org.uk.

Effect of registration

30 | Does an entry on the register have any specific legal effect?

An entry on the register does not cause the data controller to be subject to obligations or liabilities to which it would not otherwise be subject.

Other transparency duties

31 | Are there any other public transparency duties?

There are no additional public transparency duties.

TRANSFER AND DISCLOSURE OF PII

Transfer of PII

32 | How does the law regulate the transfer of PII to entities that provide outsourced processing services?

Entities that provide outsourced processing services are typically 'data processors' under the DPA and the GDPR. Data processors are subject to direct legal obligations under the DPA and GDPR in respect of the PII that they process as outsourced service providers, but nevertheless data controllers are required to use only data processors that are capable of processing PII in accordance with the requirements of the DPA and the GDPR. The data controller must ensure that each data processor it selects offers sufficient guarantees that the relevant PII will be held with appropriate security measures and take steps to ensure that these guarantees are fulfilled. The data controller must also enter into a binding contract in writing with the data processor under which the data processor must be bound to:

- act only on the instructions of the data controller;
- ensure that persons that will process PII are subject to a confidentiality obligation;

© Law Business Research 2019

- apply security controls and standards that meet those required by the GDPR;
- obtain general or specific authorisation before appointing any sub-processors, and ensure that any such sub-processors are bound by obligations equivalent to those imposed on the data processor;
- assist the data controller insofar as possible to comply with the data controller's obligation to respond to data subject rights requests;
- assist the data controller in relation to the obligations to notify personal data breaches and to carry out data protection impact assessments (and any required consultation with a supervisory authority);
- at the choice of the data controller, return the PII to the data controller or delete the PII at the end of the relationship;
- notify the data controller immediately if any instruction the data controller gives infringes the GDPR; and
- make available to the data controller all information necessary to demonstrate compliance with these obligations, and allow the data controller (or a third party nominated by the data controller) to carry out an audit.

Restrictions on disclosure

33 | Describe any specific restrictions on the disclosure of PII to other recipients.

It is a criminal offence to knowingly or recklessly obtain or disclose PII without the consent of the data controller or procure the disclosure of PII to another party without the consent of the data controller. This prohibition is subject to a number of exceptions, such as where the action was taken for the purposes of preventing or detecting crime. The staff of the ICO are prohibited from disclosing PII obtained in the course of their functions other than in accord with those functions.

There are no other specific restrictions on the disclosure of PII, other than compliance with the general principles described earlier, and the cross-border restrictions as set out in question 34.

Cross-border transfer

34 | Is the transfer of PII outside the jurisdiction restricted?

The transfer of PII outside the EEA is prohibited unless that country or territory ensures an adequate level of protection for the rights and freedoms of the individuals in relation to the processing of their PII.
Transfers are permitted where:

- the European Commission (Commission) has made a finding in relation to the adequacy of PII protection of the country or territory;
- the Commission has made a finding in relation to the relevant transfers; or
- one or more of the derogations applies.

The derogations include:

- where the data controller has the individual's explicit consent to the transfer;
- the transfer is necessary for a contract with the data subject;
- the transfer is necessary for legal proceedings;
- the transfer is necessary to protect the vital interest of the individual;
- the transfer is necessary for the purposes of the compelling legitimate interests pursued by the data controller; and
- the terms of the transfer have been approved by the ICO.

Commission findings have been made in respect of the use of approved standard form model clauses for the export of PII and the adoption of a self-regulatory scheme in the US called the EU–US Privacy Shield, which replaced the Safe Harbor mechanism that was invalidated by the Court of Justice of the European Union in October 2015. Entities within a single corporate group can enter into data transfer agreements known as binding corporate rules, which must be approved by the supervisory authorities in the relevant EU member states. In addition, an organisation can make a restricted transfer if it and the receiver have entered into a contract incorporating standard data protection clauses adopted by the Commission. These are known as the 'standard contractual clauses'. They must be entered into by the data exporter (based in the EEA) and the data importer (outside the EEA).

Notification of cross-border transfer

35 | Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

Transfer requires no specific notification to the ICO and no authorisation from the ICO.

Further transfer

36 | If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

The restrictions on transfer apply equally to transfers to data processors and data controllers.

Onward transfers are taken into account in assessing whether adequate protection is provided in the receiving country. Onward transfers are covered in the Commission-approved model clauses, and in the Privacy Shield.

Onward transfers are not controlled specifically where a transfer is made to a country that has been the subject of an adequacy finding by the Commission. It would be anticipated that the law of the recipient country would deal with the legitimacy of the onward transfer.

RIGHTS OF INDIVIDUALS

Access

37 | Do individuals have the right to access their personal information held by PII owners? Describe how this right can be exercised as well as any limitations to this right.

Individuals have the right to request access to PII that relates to them. Within one month of receipt of a valid request, the data controller must confirm that it is or is not processing the individual's PII and, if it does so, provide a description of the PII, the purposes of the processing and recipients or categories of recipients of the PII, the relevant retention period for the PII, a description of the rights available to individuals under the GDPR and that the individual may complain to a supervisory authority and any information available to the data controller as to the sources of the PII, the existence of automated decision-making (including profiling), and the safeguards it provides if it transfers PII to a third country or international organisation. The data controller must also provide a copy of the PII in an intelligible form.

A data controller must be satisfied as to the identity of the individual making the request. A data controller does not have to provide third-party data where that would breach the privacy of the third party and may reject repeated identical requests, or charge a reasonable fee taking into account the administrative costs of providing the information.

In some cases, the data controller may withhold PII to protect the individual; for example, where health data is involved, or to protect other important specified public interests such as the prevention of crime. All such exceptions are specifically delineated in the law.

In most cases, the organisation cannot charge a fee to comply with a request for access. However, where the request is manifestly

© Law Business Research 2019

unfounded or excessive an organisation may charge a 'reasonable fee' for the administrative costs of complying with the request. A reasonable fee can also be charged if an individual requests further copies of their data following a request.

Other rights

38 | Do individuals have other substantive rights?

Individuals have the following further rights:

- to rectify PII that is inaccurate;
- to have PII erased in certain circumstances, for example, when the PII is no longer necessary for the purposes for which it was collected by the data controller;
- to restrict the processing of PII;
- to obtain a copy of PII in a structured, commonly used and machine-readable format, and to transmit that PII to a third-party data controller without hindrance, to the extent that it is technically feasible;
- to object to the processing of PII in certain circumstances; and
- not to be subject to decisions based solely on the automated processing of PII, except in particular circumstances.

Compensation

39 | Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Individuals are entitled to receive compensation if the individual suffers material or non-material damage as a result of the contravention of the GDPR by a data controller or data processor. The DPA indicates that 'non-material' damage includes 'distress'.

Enforcement

40 | Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

Individuals may take action in the courts to enforce any of the rights described in questions 37–39.

The ICO has no power to order the payment of compensation to individuals. Therefore, an individual who seeks compensation must take an action to the courts. All the other rights of individuals can be enforced by the ICO using the powers described in question 2.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

41 | Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

The DPA, in accordance with the derogations permitted by the GDPR, provides exemptions from certain obligations, including:

- exemptions from the obligations that limit the disclosure of PII;
- exemptions from the obligations to provide notice of uses of PII;
- exemptions from reporting personal data breaches;
- exemptions from complying with the data protection principles;
- exemptions from the rights of access; and
- exemptions from dealing with other individual rights.

The grounds for exemption include exemptions to protect freedom of expression, to protect national security and policing, to support legal privilege, to protect the actions of regulatory authorities and to protect the collection of taxes and the position of the armed forces.

Exemptions also apply to protect individuals who may be vulnerable, such as those who are suffering from mental illness.

Further exemptions apply where the PII is made publicly available under other provisions.

Specific exemptions apply to allow the retention and use of PII for the purposes of research. Exemptions are also available under the DPA for crime, law and public protection, and finance, management and negotiations.

All exemptions are limited in scope and most apply only on a case-by-case basis.

SUPERVISION

Judicial review

42 | Can PII owners appeal against orders of the supervisory authority to the courts?

Data controllers may appeal orders of the ICO to the General Regulatory Chamber (First-tier Tribunal). Appeals must be made within 28 days of the ICO notice and must state the full reasons and grounds for the appeal (ie, that the order is not in accordance with the law or the ICO should have exercised its discretion differently).

Appeals against decisions of the General Regulatory Chamber (First-tier Tribunal) can be made (on points of law only) to the Administrative Appeals Chamber of the Upper Tribunal, appeals from which may be made to the Court of Appeal.

SPECIFIC DATA PROCESSING

Internet use

43 | Describe any rules on the use of 'cookies' or equivalent technology.

It is unlawful to store information (such as a cookie) on a user's device, or gain access to such information, unless the user is provided with clear and comprehensive information about the storage of, and access to, that information, and has provided his or her consent. Consent must be validly obtained in accordance with the requirements of the GDPR. Such consent is not, however, required where the information is:

- used only for the transmission of communications over electronic communications networks; or
- strictly necessary for the provision of a service requested by the user.

Electronic communications marketing

44 | Describe any rules on marketing by email, fax or telephone.

It is unlawful to send unsolicited electronic marketing (ie, via technologies such as SMS, fax or email) unless the opt-in consent of the recipient has been obtained. However, an unsolicited marketing email may be sent to a recipient whose contact details were obtained in the course of a sale, or negotiation of sale, of a product or service, provided that the unsolicited marketing relates to similar products or services, the recipient is given a simple and free-of-charge means to opt out of receiving such marketing at the point their information is collected, and in all subsequent marketing communications (and has not yet opted out). Any consent obtained must comply with the GDPR's consent requirements.

It is generally permissible to make unsolicited telephone marketing calls, unless the recipient has previously notified the caller that he or she does not wish to receive such calls or the recipient's phone number is listed on the directory of subscribers that do not wish to receive such calls (known as the Telephone Preference Service). Any individuals may apply to have their telephone number listed in this directory.

© Law Business Research 2019

Separate requirements

Separate rules around marketing to corporate subscribers (ie, an individual in his or her professional capacity) apply, and will need to be considered for business-to-business marketing.

Cloud services

45 | Describe any rules or regulator guidance on the use of cloud computing services.

There are no specific rules or legislation that govern the processing of PII through cloud computing, and such processing must be compliant with the DPA. The ICO has released guidance on the subject of cloud computing, which discusses the identity of data controllers and data processors in the context of cloud computing, as well as the need for written contracts, security assessments, compliance with the DPA and the use of cloud providers from outside the UK. This guidance was published under the old law (ie, Data Protection Act 1998). The ICO has confirmed that, while much of the guidance remains relevant, it intends to update the guidance in line with the GDPR.

HUNTON ANDREWS KURTH

Aaron P Simpson
asimpson@HuntonAK.com

James Henderson
jhenderson@HuntonAK.com

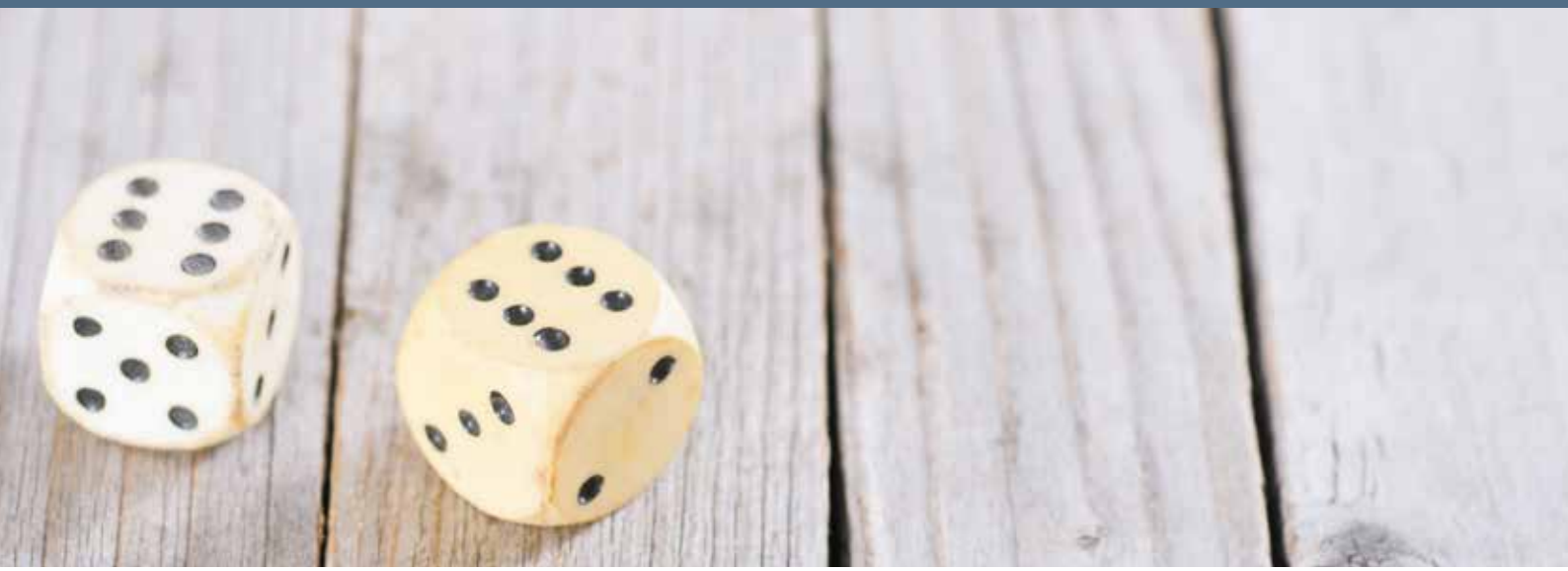
Jonathan Wright
wrightj@HuntonAK.com

30 St Mary Axe
London EC3A 8EP
United Kingdom
Tel: +44 20 7220 5700
Fax: +44 20 7220 5772
www.HuntonAK.com

© Law Business Research 2019

HUNTON
ANDREWS KURTH

Leaders in Handling High-Stakes Cybersecurity Events



Luck is not a strategy.

Increase your company's resilience and responsiveness to cyber attacks.

Hunton Andrews Kurth LLP's privacy and cybersecurity practice assists global organizations in managing data through every step of the information life cycle. We help businesses prepare for and respond to cybersecurity incidents all over the world. The firm is ranked as a top law firm globally for privacy and data security.

For more information, visit www.huntonprivacyblog.com.

©2019 Hunton Andrews Kurth LLP | HuntonAK.com

© Law Business Research 2019

Other titles available in this series

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Appeals
Arbitration
Art Law
Asset Recovery
Automotive
Aviation Finance & Leasing
Aviation Liability
Banking Regulation
Cartel Regulation
Class Actions
Cloud Computing
Commercial Contracts
Competition Compliance
Complex Commercial Litigation
Construction
Copyright
Corporate Governance
Corporate Immigration
Corporate Reorganisations
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Defence & Security Procurement
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
e-Commerce
Electricity Regulation
Energy Disputes
Enforcement of Foreign Judgments
Environment & Climate Regulation
Equity Derivatives
Executive Compensation & Employee Benefits
Financial Services Compliance
Financial Services Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gaming
Gas Regulation
Government Investigations
Government Relations
Healthcare Enforcement & Litigation
High-Yield Debt
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Joint Ventures
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Litigation Funding
Loans & Secured Financing
M&A Litigation
Mediation
Merger Control
Mining
Oil Regulation
Patents
Pensions & Retirement Plans
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Banking & Wealth Management
Private Client
Private Equity
Private M&A
Product Liability
Product Recall
Project Finance
Public M&A
Public Procurement
Public-Private Partnerships
Rail Transport
Real Estate
Real Estate M&A
Renewable Energy
Restructuring & Insolvency
Right of Publicity
Risk & Compliance Management
Securities Finance
Securities Litigation
Shareholder Activism & Engagement
Ship Finance
Shipbuilding
Shipping
Sovereign Immunity
Sports Law
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Technology M&A
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

lexology.com/gtdt

ISBN 978-1-83862-146-9

© Law Business Research 2019