DATA PROTECTION & PRIVACY

United Kingdom

LEXOLOGY
Getting The Deal Through

Consulting editor
Hunton Andrews Kurth LLP

Data Protection & Privacy

Consulting editors

Aaron P Simpson, Lisa J Sotto

Hunton Andrews Kurth LLP

Quick reference guide enabling side-by-side comparison of local insights into the legislative framework; relevant authorities; treatment of breaches; legitimate processing; data handling responsibilities of PII owners; security obligations; internal controls, including the data protection officer; registration formalities transfer and disclosure of PII; rights of individuals; judicial supervision; specific data processing use cases such as cookies, electronic communications marketing, and cloud services; and recent trends.

Generated 05 August 2022

Table of contents

Contributors

United Kingdom

Aaron P Simpson
asimpson@hunton.com
Hunton Andrews Kurth LLP

James Henderson
jhenderson@HuntonAK.com
Hunton Andrews Kurth LLP

Jonathan Wright
wrightj@HuntonAK.com
Hunton Andrews Kurth LLP

LAW AND THE REGULATORY AUTHORITY

Legislative framework

Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

The primary legal instruments include the UK's Data Protection Act 2018 (DPA 2018) and Regulation (EU) 2016/679 (the General Data Protection Regulation) as transposed into national law of the United Kingdom by the UK European Union (Withdrawal) Act 2018 and amended by the UK Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (the UK GDPR).

Law stated - 30 June 2022

Data protection authority

Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

DPA 2018 and the UK 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.

Law stated - 30 June 2022

Cooperation with other data protection authorities

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?

Following the UK's exit from the European Union, the ICO no longer participates in the GDPR's 'one-stop-shop' mechanism, under which organisations with a main establishment in the European Union may primarily be regulated by the supervisory authority of the jurisdiction in which the main establishment is located (lead supervisory authority).

DPA 2018 requires the ICO, concerning third countries and international organisations, to take steps to develop cooperation mechanisms to facilitate the effective enforcement of legislation relating to the protection of PI, to provide international mutual assistance in the enforcement of legislation for the protection of PI, to engage relevant stakeholders in discussion and activities, and to promote the exchange and documentation of legislation and practice for the protection of PI.

Law stated - 30 June 2022

Breaches of data protection law

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

The ICO has several 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;
- 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 €17.5 million or 4 per cent of annual worldwide turnover, depending on the nature of the violation of DPA 2018 and UK GDPR.

Several breaches may lead to criminal penalties. The following may constitute criminal offences:

- making a false statement concerning an information notice validly served by the ICO;
- destroying, concealing, blocking or falsifying information to prevent the ICO from viewing or being provided with the information;
- unlawfully obtaining PI;
- knowingly or recklessly re-identifying PI that is de-identified without the consent of the data controller responsible for that PI;
- altering PI 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 the 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.

Law stated - 30 June 2022

Judicial review of data protection authority orders

Can PI owners appeal to the courts against orders of the data protection authority?

Yes. The UK GDPR gives each natural or legal person the right to an effective judicial remedy against a legally binding decision of ICO that concerns them. In addition, where an individual has lodged a complaint with the ICO, the UK GDPR and DPA 18 give the individual the right to an effective judicial remedy where the ICO does not handle the complaint or does not inform the individual within three months on the progress or outcome of the complaint.

Law stated - 30 June 2022

SCOPE

Exempt sectors and institutions

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 the 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 PI is only used for such things as writing to friends and family or taking pictures for personal enjoyment, such use of PI will not be subject to the UK General Data Protection Regulation (the UK GDPR).

The UK GDPR and the Data Protection Act 2018 (DPA 2018) apply to private and public sector bodies. That said, the processing of PI by competent authorities for law enforcement purposes is outside the scope of the UK GDPR (eg, the police investigating a crime). Instead, this type of processing is subject to the rules in Part 3 of DPA 2018. Also, PI processed to safeguard national security or defence is also outside the scope of the UK GDPR. However, it is covered by Part 2, Chapter 3 of DPA 2018 (the applied GDPR), which contains an exemption for national security and defence. Part 4 of DPA 2018 sets out a separate data protection regime for the intelligence services (eg, MI5, SIS (sometimes known as MI6) and GCHQ).

Law stated - 30 June 2022

Interception of communications and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

Electronic marketing is specifically regulated by the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) (as amended), although the UK GDPR and DPA 2018 often apply to the same activities, to the extent that they involve the processing of PI. 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.

Law stated - 30 June 2022

Other laws

Are there 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 PI. Laws on defamation, copyright and computer misuse also affect data protection. However, there is no specific data protection sectoral legislation. The United Kingdom 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 2018 requires the Information Commissioner's Office (ICO) to draw up and publish codes of practice that relate to data sharing, direct marketing, age-appropriate design and data protection, and journalism. A number of these codes are not yet in force and are in the consultation phase. The ICO's Age Appropriate Design Code came into force on 2 September 2020, and following a 12-month transition period, organisations are now expected to conform to its requirements (as of 2 September 2021). In addition, the ICO's Data Sharing Code of Practice came into force on 5 October 2021. This code provides practical guidance for organisations regarding how to share PI in a manner that complies with DPA 2018 and UK GDPR.

The PECR sits alongside DPA 2018 and the UK GDPR. They give individuals specific privacy rights concerning electronic communications. In particular, the PECR sets out requirements for:

- making marketing calls, sending marketing emails and texts;
- the use of cookies (and similar technologies) on individuals' devices;
- keeping communications services secure; and
- customer privacy regarding traffic and location data, itemised billing, line identification and directory listings.

The United Kingdom has implemented the Network and Information Systems Regulations 2018 (the NIS Regulations). The UK NIS regime also includes an implementing act for digital service providers (the DSP Regulation) and specifies security requirements and incident reporting thresholds for certain organisations. While the UK GDPR concerns PI, the NIS Regulations concern the security of network and information systems. That said, there is a significant crossover between the UK GDPR and NIS Regulations, in particular owing to the UK GDPR's security requirements. In this respect, the application of the NIS Regulations is broader as it applies to digital data and not just PI.

The NIS Regulations apply to operators of essential services (OES) and relevant digital service providers (RDSPs) and are intended to address the threats posed to network and information systems. To this end, its primary focus is on cybersecurity measures. In particular, the NIS Regulations require RDSPs and OES to take appropriate and proportionate measures to manage the risks posed to the security of network and information systems.

Law stated - 30 June 2022

PI formats

What categories and types of PI are covered by the law?

The UK GDPR and DPA 2018 cover PI held in electronic form plus such information held in structured files, called 'relevant filing systems'. 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.

Law stated - 30 June 2022

Extraterritoriality

Is the reach of the law limited to PI owners and processors physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

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

A data controller or data processor is 'established' in the United Kingdom if it is resident in the United Kingdom, 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 United Kingdom. Where a data controller or data processor is established in the United Kingdom, UK GDPR and DPA 2018 will apply regardless of whether the processing takes place in the United Kingdom or not.

Data controllers established outside the United Kingdom that are subject to the UK GDPR and DPA 2018 must nominate a representative in the United Kingdom.

Law stated - 30 June 2022

Covered uses of PI

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

The UK GDPR and DPA 2018 apply to data controllers (ie, those who decide the purposes and the means of the data processing) and data processors (who process PI 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 PI. Data processors act on behalf of, and only on the instructions of, the relevant data controller.

Law stated - 30 June 2022

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

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

The UK General Data Protection Regulation (the UK GDPR) requires data controllers to rely on a legal ground outlined in the UK GDPR for all processing of PI. Additional conditions must also be satisfied when processing sensitive PI.

The grounds for processing non-sensitive PI are:

- consent of the individual;
- performance of a contract to which the individual is party or to take steps at the request of the data subject before entering into a contract;
- compliance with a legal obligation, other than a contractual obligation (a legal obligation arising under the laws of a non-UK 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 PI is disclosed) unless overridden by the individual's fundamental rights, freedoms and legitimate interests.

Law stated - 30 June 2022

Legitimate processing – types of PI

Does the law impose more stringent rules for processing specific categories and types of PI?

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

- 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 to uniquely identify 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.

Where a controller processes sensitive PI it must establish a ground for processing both non-sensitive PI (eg, consent and the performance of a contract) and a separate condition for processing sensitive PI. The GDPR sets forth several conditions that may be considered in connection with the processing of sensitive PI, 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 former members of the body or to persons who have regular contact with it in connection with its purposes, and that the PI is not disclosed outside that body without the consent of the data subjects;
- the processing relates to PI, which is manifestly made public by the data subject;
- the exercise of public functions;
- processing in connection with legal proceedings, legal advice or 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 conditions outlined in the UK GDPR, the Data Protection Act 2018 sets forth several additional conditions 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.

Law stated - 30 June 2022

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

Does the law require owners of PI to provide information to individuals about how they process PI? 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 PI 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 PI;
- the fact that the data controller intends to transfer the PI 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 how individuals may obtain a copy of them;
- the period for which PI 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 a European Union data protection supervisory authority;
- whether the provision of PI 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 PI and of the consequences of failure to provide such PI; 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 PI is obtained from a source other than the individual concerned, the data controller must also inform individuals of the source from which the PI originated and the categories of PI obtained.

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

- within a reasonable period of obtaining the PI 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.

Law stated - 30 June 2022

Exemptions from transparency obligations

When is notice not required?

Where PI 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 PI is required by UK law to which the data controller is subject; or

- where the PI is subject to an obligation of professional secrecy under UK law.

Law stated - 30 June 2022

Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PI?

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

Law stated - 30 June 2022

Data minimisation

Does the law restrict the types or volume of PI that may be collected?

The data controller must ensure that PI is adequate, relevant and not excessive concerning the purpose for which it is held. This means that the data controller should not collect or process unnecessary or irrelevant PI. The Data Protection Act 2018 and the UK General Data Protection Regulation do not impose any specified retention periods. PI may be held only for as long as is necessary for the purposes for which it is processed.

Law stated - 30 June 2022

Data retention

Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

Yes. The UK GDPR requires PI to be retained for no longer than is necessary for the purposes for which it was originally collected. The UK GDPR does not, however, set specific time limits for different types of PI. It is the data controller's responsibility to determine how long it needs to retain PI, and this will depend on how long it needs the PI for its specified purposes. The data controller must be able to justify its chosen retention period, and it will rarely, if ever, be justifiable to retain PI on a just-in-case basis or indefinitely.

Law stated - 30 June 2022

Purpose limitation

Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

PI 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 Data Protection Act 2018 or UK General Data Protection Regulation.

PI may not be processed for new purposes unless the further purposes are lawful (ie, based on a lawful ground). 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, PI 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.

Law stated - 30 June 2022

Automated decision-making

Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

Yes. The UK GDPR gives individuals the right not to be subject to solely automated decisions, including profiling, which have a legal or similarly significant effect on them. The decision-making must be entirely automated and exclude any human influence on the outcome. A process will not be solely automated if a person weighs up and interprets the result of an automated decision before applying it to the individual (ie, reviews the decision and has discretion to alter it). The decision-making may, however, still be considered solely automated if a human inputs the PI to be processed and the decision-making is then carried out by an automated system. This restriction on automated decision-making applies only where the automated decision produces a legal or similarly significant effect. A decision producing a legal effect is something that affects an individual's legal status or their legal rights. This may include a decision that affects an individual's legal status under a contract (eg, cancellation of a contract). A decision that has a similarly significant effect is something that has an equivalent impact on an individual's circumstances, behaviour or choices. For example, similarly significant effects include automatic refusal of an online credit application or e-recruiting practices without human intervention.

Where a data controller is undertaking these types of automated decisions, such decisions are only permitted where:

- the decision is necessary for the performance of a contract with the individual;
- the decision is authorised by UK law; or
- the decision is based on the individual's explicit consent.

Where the automated decision involves sensitive PI additional protections apply, and the relevant automated decision-making can only take place where:

- the individual has given his or her explicit consent; or
- the processing is necessary for reasons of substantial public interest.

Law stated - 30 June 2022

SECURITY

Security obligations

What security obligations are imposed on PI owners and service providers that process PI on their behalf?

The Data Protection Act 2018 and the UK General Data Protection Regulation (the UK GDPR) do not specify the types of security measures that data controllers and data processors must take concerning PI. Instead, data controllers and

data processors must have in place 'appropriate technical and organisational measures' to protect against 'unauthorised or unlawful processing of [PI] and against accidental loss or destruction of, or damage to, [PI]'. In addition, the UK GDPR provides several examples of security measures that data controllers and data processors should consider implementing, including:

- the pseudonymisation and encryption of PI;
- 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 PI promptly 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 PI in question and the harm that might result from its improper use, or 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 PI, 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.

Law stated - 30 June 2022

Notification of data breach

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 UK GDPR requires data controllers to notify the Information Commissioner's Office (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 affected individuals but must notify the relevant data controller of a data breach without undue delay.

In addition to notifying breaches to the ICO and 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.

Law stated - 30 June 2022

INTERNAL CONTROLS

Accountability

Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

Yes. The UK General Data Protection Regulation (the UK GDPR) requires data controllers to be responsible for, and able

to demonstrate compliance with, the UK GDPR. This requires data controllers to be proactive and organised about their approach to data protection, and be able to evidence the steps they have taken to comply with the UK GDPR. This may include, for example, implementing policies and procedures governing how PI is processed within the organisation, and ensuring staff are appropriately trained so as to ensure they are aware of their obligations when processing PI.

Law stated - 30 June 2022

Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

The UK GDPR requires data controllers and data processors to appoint a data protection officer (DPO) 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 PI or PI relating to criminal offences and convictions on a large scale.

If appointed, a DPO is responsible for:

- informing and advising the data controller or data processor and its employees of his or her obligations under data protection law;
- monitoring compliance with the UK GDPR, awareness-raising, staff training and audits;
- providing advice concerning data protection impact assessments;
- cooperating with the Information Commissioner's Office (ICO) and other European Union data protection supervisory authorities; and
- acting as a contact point for the ICO on issues relating to processing PI.

Organisations may also elect to appoint a DPO voluntarily; although, such an appointment will need to comply with the requirements of the UK GDPR.

Law stated - 30 June 2022

Record-keeping

Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

Under article 30 of the UK GDPR, data controllers and data processors are required to retain internal records that describe the processing of PI 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 DPO;

- the purposes of the processing;
- the data subjects and categories of PI processed;
- the categories of recipients to whom PI has been or will be disclosed;
- a description of any transfers of PI to third countries and the safeguards relied upon;
- the envisaged time limits for erasure of the PI; 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 each data controller on behalf of which the processor processes PI, and of the processor's representative and DPO;
- the categories of processing carried out on behalf of each data controller;
- a description of any transfers of PI to third countries and the safeguards relied upon; and
- a general description of the technical and organisational security measures implemented.

DPA 2018 sets out several conditions for the processing of sensitive PI. To satisfy several of these conditions, data controllers must have an appropriate policy document in place. If a data controller processes sensitive PI under a condition that requires an appropriate policy document, the data controller must document the following information as part of its processing activities:

- the procedures for complying with the data protection principles in connection with the processing of the sensitive PI; and
- its policies regarding the retention and erasure of the sensitive PI, indicating how long such sensitive PI is likely to be retained.

Data controllers must review and retain the policy document when processing the relevant sensitive PI, and then for at least six months afterwards. The policy document must also be made available on request to the ICO.

Where appropriate policy documentation is required, the data controller's records of processing activities under article 30 of the UK GDPR must include:

- details of the relevant condition relied on, as set out in Parts 1 to 3 of Schedule 1 of DPA 2018;
- how processing satisfies article 6 of the UK GDPR (lawfulness of processing); and
- details of whether the sensitive PI is retained and erased following the appropriate policy documentation (and if not the reasons why not).

Law stated - 30 June 2022

Risk assessment

Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

Data controllers are required to carry out a data protection impact assessment (DPIA) concerning any processing of PI that is likely to result in a high risk to the rights and freedoms of natural persons. In particular, a DPIA 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 PI or PI relating to criminal convictions or offences on a large scale; or
- systematic monitoring of a publicly accessible area on a large scale.

A DPIA must be carried out concerning all high-risk processing activities that meet the criteria above before the processing begins. The DPIA 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 concerning 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 and security measures).

Law stated - 30 June 2022

Design of PI processing systems

Are there any obligations in relation to how PI processing systems must be designed?

The UK GDPR 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 PI is processed under the UK GDPR, and to ensure that, by default, only PI that is necessary for each specific purpose is collected and processed. In addition, data controllers must ensure that by default PI is not made accessible to an indefinite number of persons without any intervention by the data subject.

Law stated - 30 June 2022

REGISTRATION AND NOTIFICATION

Registration

Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

In the United Kingdom, data controllers are required to pay an annual registration fee to the Information Commissioner's Office (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 to establish or maintain membership or support of that organisation; or
- the data controller only processes PI for one or more of these purposes, and not for any other 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.

Law stated - 30 June 2022

Other transparency duties

Are there any other public transparency duties?

There are no additional public transparency duties.

Law stated - 30 June 2022

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

How does the law regulate the sharing of PI with entities that provide outsourced processing services?

Entities that provide outsourced processing services are typically data processors under the Data Protection Act 2018 and the UK General Data Protection Regulation (the UK GDPR). Data processors are subject to direct legal obligations under the UK GDPR in respect of the PI that they process as outsourced service providers, but nevertheless, data controllers are required to use only data processors that are capable of processing PI under the requirements of the UK GDPR. The data controller must ensure that each data processor it selects offers sufficient guarantees that the relevant PI will be processed subject to 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 PI are subject to a confidentiality obligation;
- apply security controls and standards that meet those required by the UK 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 concerning 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 PI to the data controller or delete the PI at the end of the relationship;
- notify the data controller immediately if any instruction the data controller gives infringes the UK 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.

Law stated - 30 June 2022

Restrictions on third-party disclosure

Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

It is a criminal offence to knowingly or recklessly obtain or disclose PI without the consent of the data controller or procure the disclosure of PI to another party without the consent of the data controller. This prohibition is subject to several exceptions, such as where the action was taken to prevent or detect crime. The staff of the Information Commissioner's Office (ICO) are prohibited from disclosing PI obtained in the course of their functions other than as necessary for those functions.

There are no other specific restrictions on the disclosure of PI, other than compliance with general principles and the cross-border restrictions.

Law stated - 30 June 2022

Cross-border transfer

Is the transfer of PI outside the jurisdiction restricted?

The transfer of PI outside the United Kingdom is prohibited unless that country or territory ensures an adequate level of protection for the rights and freedoms of the individuals concerning the processing of their PI.

Transfers are permitted where:

- the recipient is located in a third country or territory or is an international organisation, covered by UK adequacy regulations;
- the transfer is covered by appropriate safeguards; 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 to perform a contract with the data subject;
- the transfer is necessary for legal proceedings;
- the transfer is necessary to protect the vital interests of the individual;
- the transfer is necessary for the compelling legitimate interests pursued by the data controller; and
- the terms of the transfer have been approved by the ICO.

UK adequacy regulations have determined the European Economic Area and all countries, territories and international organisations covered by European Commission adequacy decisions valid as of 31 December 2020 to provide an adequate level of protection for personal data. The UK government intends to review these adequacy regulations over time.

European Commission findings have been made in respect of the use of approved standard form model clauses (standard contractual clauses) for the export of PI. Following the UK's departure from the European Union, transitional arrangements have been implemented that permit UK organisations to continue to rely on the European Commission-approved model clauses that were in place at the time of the UK's departure from the EU (that is, not including the new

EU standard contractual clauses adopted in 2021) (the transitional standard clauses). The transitional standard clauses remain a valid data transfer mechanism for agreements concluded on or before 21 September 2022 and continued to provide appropriate safeguards under the UK GDPR until 21 March 2022. The ICO has published an International Data Transfer Agreement and a UK Addendum to the EU Standard Contractual Clauses. The International Data Transfer Agreement constitutes a stand-alone agreement that can be used to ensure adequacy in respect of data transfers from the UK. The UK Addendum to the EU Standard Contractual Clauses can be entered into alongside the EU standard contractual clauses and means that the EU Standard Contractual Clauses constitute adequate safeguards under UK law. The International Data Transfer Agreement and UK Addendum may be used for transfers at this point in time and must be used in respect of any new data transfers that commence on 22 September 2022 or thereafter.

Entities within a single corporate group can enter into binding corporate rules (BCRs), which must be approved by the ICO. Following the UK's departure from the European Union, new applications for UK BCRs must be submitted to the ICO using the UK BCR application forms. Organisations with existing authorised EU BCRs (ie, BCRs approved before Brexit by an EU supervisory authority) do not need to complete a new UK BCR application. However, they must still provide the ICO with a United Kingdom version of their BCRs.

The European Commission has adopted a data protection adequacy decision relating to the United Kingdom, allowing organisations in the European Economic Area to continue to transfer personal data to organisations in the United Kingdom without restriction and without needing to rely upon data transfer mechanisms to ensure an adequate level of protection.

Law stated - 30 June 2022

Further transfer

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 considered in assessing whether adequate protection is provided in the receiving country. Onward transfers are covered in the transitional clauses, the International Data Transfer Agreement and in the UK Addendum to the EU Standard Contractual Clauses.

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 United Kingdom. It would be anticipated that the law of the recipient country would deal with the legitimacy of the onward transfer.

Law stated - 30 June 2022

Localisation

Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

No. UK law does not require PI or a copy of PI to be retained within the UK.

Law stated - 30 June 2022

RIGHTS OF INDIVIDUALS

Access

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

Individuals have the right to request access to PI 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 PI and, if it does so, provide a description of the PI, the purposes of the processing and recipients or categories of recipients of the PI, the relevant retention period for the PI, a description of the rights available to individuals under the UK General Data Protection Regulation (GDPR) and that the individual may complain to the Information Commissioner's Office (ICO) and any information available to the data controller as to the sources of the PI, the existence of automated decision-making (including profiling), and the safeguards it provides if it transfers PI to a third country or international organisation. The data controller must also provide a copy of the PI 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 unless the third party has consented to the disclosure or it is reasonable in the circumstances to disclose PI relating to the third party to the requestor.

In some cases, the data controller may withhold PI in response to a request, for example, where PI is subject to legal privilege in the UK or where disclosure of the requested PI would prejudice ongoing negotiations between the data controller and the requestor. All such exceptions are specifically delineated in the law.

In most cases, the data controller cannot charge a fee to comply with an access request. However, where the request is manifestly 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.

Law stated - 30 June 2022

Other rights

Do individuals have other substantive rights?

Individuals have the following further rights:

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

Law stated - 30 June 2022

Compensation

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 Data Protection Act 2018 indicates that 'non-material' damage includes 'distress'. The Lloyd v Google decision (Lloyd v Google LLC [2021] UKSC 50]) has confirmed that compensation is not available for merely technical violations of UK data protection in the absence of financial loss or distress.

Law stated - 30 June 2022

Enforcement

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 their rights.

The ICO has no power to order the payment of compensation to individuals. Therefore, an individual who seeks compensation must take action through the courts. All the other rights of individuals can be enforced by the ICO using its enforcement powers, including requiring the provision of information, and conducting audits.

Law stated - 30 June 2022

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described?

The Data Protection Act 2018 (DPA 2018), following the derogations permitted by the UK General Data Protection Regulation, provides exemptions from certain obligations, including:

- exemptions from the obligations that limit the disclosure of PI;
- exemptions from the obligations to provide notice of uses of PI;
- 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 PI is made publicly available under other provisions.

Specific exemptions apply to allow the retention and use of PI for research. Exemptions are also available under DPA 2018 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.

Law stated - 30 June 2022

SPECIFIC DATA PROCESSING

Cookies and similar technology

Are there 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 following the requirements of the Privacy and Electronic Communications (EC Directive) Regulations 2013 (PECR). Any consent obtained must comply with the UK GDPR's standard for valid consent. 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.

Law stated - 30 June 2022

Electronic communications marketing

Are there any rules on marketing by email, fax, telephone or other electronic channels?

It is unlawful to send unsolicited electronic marketing (ie, via technologies such as text, fax or email) unless the opt-in consent of the recipient has been obtained following the requirements of PECR. 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 a 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 UK General Data Protection Regulation's (UK GDPR) standard for valid consent.

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 – the Telephone Preference Service. Any individuals may apply to have their telephone number listed in this directory. Separate requirements and 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.

Law stated - 30 June 2022

Targeted advertising

Are there any rules on targeted online advertising?

There are no specific rules relating to targeted online advertising except for the general requirements under the UK GDPR and PECR. In general, consent is required for the use of cookies and similar technologies used in the context of targeted online advertising under PECR, and organisations processing PI in connection with those activities must also

rely on consent as the legal basis for processing that personal data under the GDPR. The ICO has published, in draft form for public consultation, its Direct Marketing Code of Practice, which addresses various issues relating to online targeted advertising.

Law stated - 30 June 2022

Sensitive personal information

Are there any rules on the processing of 'sensitive' categories of personal information?

The UK GDPR requires data controllers to rely on a legal ground outlined in the UK GDPR for all processing of PI. Additional conditions must also be satisfied when processing sensitive PI.

The grounds for processing non-sensitive PI are:

- consent of the individual;
- performance of a contract to which the individual is party or to take steps at the request of the data subject before entering into a contract;
- compliance with a legal obligation, other than a contractual obligation (a legal obligation arising under the laws of a non-UK 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 PI is disclosed) unless overridden by the individual's fundamental rights, freedoms and legitimate interests.

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

- 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 to uniquely identify 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.

Where a controller processes sensitive PI it must establish a ground for processing both non-sensitive PI (eg, consent and the performance of a contract) and a separate condition for processing sensitive PI. The GDPR sets forth several conditions that may be considered in connection with the processing of sensitive PI, 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 former members of the body or to persons who have regular contact with it in connection with its purposes, and that the PI is not disclosed outside that body without the consent of the data subjects;
- the processing relates to PI, which is manifestly made public by the data subject;
- the exercise of public functions;
- processing in connection with legal proceedings, legal advice or 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 conditions outlined in the UK GDPR, the Data Protection Act 2018 sets forth several additional conditions 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.

Law stated - 30 June 2022

Profiling

Are there any rules regarding individual profiling?

There are no specific rules relating to individual profiling, but the general principles and a number of obligations are likely to be relevant. For example, data controllers are required to provide notice of any profiling that is carried out, rely on an appropriate legitimate ground for processing PI and only use sensitive PI for profiling purposes with explicit consent. In addition, profiling that involves automated decision-making that produces a legal effect or a significantly similar effect on the individual may be carried out only where necessary to enter into or perform a contract between the individual and the data controller, or with the explicit consent of the data subject. As a general matter, the use of PI for profiling is likely to require the organisation to carry out a data protection impact assessment in relation to that processing.

Law stated - 30 June 2022

Cloud services

Are there any rules or regulator guidance on the use of cloud computing services?

There are no specific rules or legislation that govern the processing of PI through cloud computing, and such processing must be compliant with the Data Protection Act 2018 (DPA 2018). The Information Commissioner's Office (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 DPA 2018 and the use of cloud providers from outside the United Kingdom. This guidance was

published under the old law (ie, the 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 UK GDPR.

Law stated - 30 June 2022

UPDATE AND TRENDS

Key developments of the past year

Are there any emerging trends or hot topics in international data protection in your jurisdiction?

In September 2021, the UK government launched a consultation on possible reforms to the UK data protection framework following the UK's departure from the EU. The stated aims of the data protection reform are to:

- support competition and innovation to drive economic growth;
- maintain high data protection standards without creating unnecessary barriers to responsible data use;
- keep pace with rapid innovation of data-intensive technologies;
- help businesses of all sizes use data responsibly without undue uncertainty or risk; and
- ensure the Information Commissioner's Office is adequately equipped to effectively regulate.

The UK government announced its proposed reform to the UK data protection framework in May 2022, and publication of a draft bill is expected later in 2022. It remains to be seen the extent to which the proposals will diverge from the data protection framework in the EU, but the UK government will need to balance the benefits of proposed reforms against the possibility of a loss of adequacy status under Regulation (EU) 2016/679 (the General Data Protection Regulation).

Law stated - 30 June 2022

Jurisdictions

Australia	Piper Alderman
Austria	Knyrim Trieb Rechtsanwälte
Belgium	Hunton Andrews Kurth LLP
Brazil	Mattos Filho Veiga Filho Marrey Jr e Quiroga Advogados
Canada	Thompson Dorfman Sweatman LLP
Chile	Magliona Abogados
China	Mayer Brown
France	Aramis Law Firm
Germany	Hoffmann Liebs Fritsch & Partner
Greece	GKP Law Firm
Hong Kong	Mayer Brown
Hungary	VJT & Partners
India	AP & Partners
Indonesia	SSEK Legal Consultants
Ireland	Walkers
Italy	ICT Legal Consulting
Japan	Nagashima Ohno & Tsunematsu
Jordan	Nsair & Partners - Lawyers
Malaysia	SKRINE
Malta	Fenech & Fenech Advocates
Mexico	OLIVARES
New Zealand	Anderson Lloyd
Pakistan	S.U.Khan Associates Corporate & Legal Consultants
Poland	Kobylanska Lewoszewski Mednis
Portugal	Morais Leitão, Galvão Teles, Soares da Silva & Associados

Singapore	Drew & Napier LLC
South Korea	Bae, Kim & Lee LLC
Switzerland	Lenz & Staehelin
Taiwan	Formosa Transnational Attorneys at Law
Thailand	Formichella & Sritawat Attorneys at Law
Turkey	Turunç
United Arab Emirates	Bizilance Legal Consultants
United Kingdom	Hunton Andrews Kurth LLP
USA	Hunton Andrews Kurth LLP