COUNTRY COMPARATIVE GUIDES 2024

The Legal 500 Country Comparative Guides

United Kingdom

DATA PROTECTION & CYBERSECURITY

Contributor

Orrick, Herrington & Sutcliffe (UK) LLP

Kelly Hagedorn

Partner | khagedorn@orrick.com

Anna O'Kelly

Associate | anna.okelly@orrick.com

This country-specific Q&A provides an overview of data protection & cybersecurity laws and regulations applicable in United Kingdom.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

UNITED KINGDOM
DATA PROTECTION & CYBERSECURITY

1. Please provide an overview of the legal and regulatory framework governing data protection, privacy and cybersecurity in your jurisdiction (e.g., a summary of the key laws; who is covered by them; what sectors, activities or data do they regulate; and who enforces the relevant laws).

Data protection and privacy

The UK transposed the contents of the EU General Data Protection Regulation (EU GDPR) into domestic legislation following its exit from the EU on 31 January 2020, with some technical changes to make it work more effectively in a UK context. This transposed and adapted version, known as the "UK GDPR", sits alongside the Data Protection Act 2018 (DPA 2018), which tailors and supplements the application of the UK GDPR within the country.

The DPA 2018 and UK GDPR are not sector-specific. Anyone who falls within the material and territorial scope of the UK GDPR and processes "personal data" will need to comply with the data protection regime. This includes most businesses and organisations, whatever their size. Purely personal or household activities are not caught by the scope of the UK GDPR.

Personal data is any information relating to a living individual (the "**data subject**") who can be directly identified (for instance by their name and/or contact details) or indirectly identified (for instance, by reference to an online identifier such as an IP address, cookie data and/or location data).

"**Processing**" is defined broadly under the DPA 2018 and the UK GDPR. It covers almost any use of data, including collection, recording, organisation, structuring or storage, adaptation or alteration, retrieval, consultation or use, erasure or destruction.

The Privacy and Electronic Communications (EC Directive) Regulations 2003, as amended (PECR), sit alongside the DPA 2018 and UK GDPR. PECR implements the European e-Privacy Directive 2002/58/EC in the UK and sets out specific rules on marketing calls, emails, texts and faxes and the use of cookies and similar technologies, as well as cybersecurity requirements for public electronic communications services (PECS) providers.

Cybersecurity

Currently, there is no stand-alone cybersecurity legislation in the UK. General (i.e., non sectorspecific) data security requirements concerning the processing of personal data and notification obligations in the event of a network security breach are imposed by the UK GDPR and DPA 2018.

Further sector-specific legislation sets out additional notification requirements. While some of these laws also apply to incidents impacting personal data (e.g., PECR), some apply to incidents that impact service operation and/or delivery (e.g., the Communications Act 2003, the Network and Information Systems Regulations 2018 (NIS)), and others apply to both personal data and service operation and/or delivery where an incident has a 'significant impact' (e.g., the Electronic Identification Regulation (EU/910/2014) (eIDAS)).

Broadly speaking, sector-specific laws setting out cybersecurity requirements focus on key sectors such as telecoms, communications and internet service providers (PECR and the Communications Act 2003), operators of essential services in the energy field (electricity, oil and gas), transport (air, water, rail and road), health, drinking water (supply and distribution) and digital infrastructure sectors and digital service providers (including online marketplaces, online search engines and cloud computing services) (NIS).

Regulatory authorities

The Information Commissioner's Office (ICO) is the regulatory authority for data protection in the UK. The ICO provides guidance and promotes good data

protection practices. It also conducts audits and advisory visits, considers complaints and breach reports, monitors compliance and takes enforcement action where appropriate.

The ICO is the relevant body to whom cybersecurity incidents impacting personal data are reported (i.e., notifications mandated under the UK GDPR and PECR). Legislation also sets out other UK sector-specific regulators that are the competent authorities to receive notifications. For example, Ofcom, the UK's communications regulator, is the competent authority to receive notifications under the Communications Act 2003. For notifications made under NIS, the competent authority will depend on the sector of the notifying entity, and a list of such competent authorities is scheduled to the legislation.

Guidance issued at the European level by the Article 29 Working Party and the European Data Protection Board is no longer directly relevant to the UK regime but, given that UK data protection legislation currently mirrors EU laws, they are still considered to help provide guidance for compliance with the UK GDPR and DPA 2018.

2. Are there any expected changes in the data protection, privacy or cybersecurity landscape in 2024–2025 (e.g., new laws or regulations coming into effect, enforcement of such laws and regulations, expected regulations or amendments (together, "data protection laws"))?

Several draft laws are currently proposed, both to update the UK's existing data protection, privacy and cybersecurity laws and to introduce new legislation, including:

- the Data Protection and Digital Information (No.2) Bill; and
- a proposal to expand the scope of the UK NIS Directive.

(for further information, see question 43).

Both proposed legislative changes have been in discussion for some time. There is currently no indication of when any such changes may be adopted.

3. Are there any registration or licensing requirements for entities covered by these data protection laws, and if so what are the requirements? Are there any exemptions?

Data Protection

Yes. Under the Data Protection (Charges and Information) Regulations 2018, individuals and organisations that determine the purposes and means of the processing of personal data (known as "controllers") need to pay a data protection fee to the ICO, unless they are exempt. There is a three-tier system of fees, ranging from £40 to £2,900, calculated based on the number of employees of the relevant organisation, or its turnover. Public authorities should categorise themselves according to staff numbers only and not turnover. A controller will be exempt from the requirement to pay fees if it only processes personal data for certain limited purposes, including "core" business purposes such as staff administration, advertising, marketing and public relations and accounts and records.

A fixed penalty regime (ranging from £400 to £4,000) applies when a controller should have notified and paid the appropriate fee to the ICO and has not. Aggravating factors (such as a failure to engage or cooperate with the ICO) may lead to an increase in the fine up to the statutory maximum of £4,350.

NIS

Yes. Organisations that fall under NIS (online search engines, online marketplaces and cloud computing services) that have a head office in the UK and are not a micro or small enterprise must register with the ICO. There is no fee to register with the ICO as a NIS 'relevant digital service provider', but this is a separate process to registering with the ICO under data protection legislation.

4. How do these data protection laws define "personal data," "personal information," "personally identifiable information" or any equivalent term in such legislation (collectively, "personal data") versus special category or sensitive personal data? What other key definitions are set forth in the data protection laws in your jurisdiction?

The DPA 2018 and the UK GDPR use the terms "personal data" and "special categories of personal data". These concepts are not identical in scope to the term "personally identifiable information" (PII).

Personal data means any information relating to a living individual who can be identified, directly or indirectly, in

particular by reference to an identifier (such as a name, an identification number, location data or an online identifier), or one or more factors specific to that individual's physical, physiological, genetic, mental, economic, cultural or social identity. When considering whether an individual is identifiable, the controller will need to take into account the information it is processing or to which it has access, together with all the means reasonably likely to be used to identify that individual. This can include, for instance, crossreferencing with information held by a third party.

"**Identifying**" an individual does not require the ability to name that individual—the ability to link records relating to an individual or draw inferences about an individual would be sufficient to make information "personal data" for the purposes of UK data protection law. Completely anonymised information is not personal data. "Anonymisation" is not defined in the UK GDPR; however, given the broad definition of "personal data", effective anonymisation would require mitigating the risk of re-identification so that, taking into account all relevant factors, it is sufficiently remote that the information could not reasonably be linked to an individual.

Even if an individual is identified or identifiable, directly or indirectly, from the data, it is not personal data unless it "relates to" the individual. Guidance from the ICO states that when considering whether information "relates to" an individual, the controller needs to take into account a range of factors, including the content of the information, the purpose or purposes of processing and the likely impact or effect of that processing on the individual.

"Special categories of personal data" are types of personal data which the data protection legislation identifies as requiring a higher level of protection. These are:

- personal data revealing racial or ethnic origin; o personal data revealing political opinions; o personal data revealing religious or philosophical beliefs; o personal data revealing trade union membership; o genetic data; o biometric data (where used for identification purposes); o data concerning health; o data concerning a person's sex life; and o data concerning a person's sexual orientation.

Additional rules also apply to the processing of personal data relating to criminal convictions and offences or related security measures.

Other key definitions include:

- "controller": the person who determines the purposes and the means by which the personal data is processed;
- "processor": the person who processes personal data on behalf of the controller; o "data subject": the individual to whom the personal data relates.

5. What are the principles related to the general processing of personal data in your jurisdiction? For example, must a covered entity establish a legal basis for processing personal data, or must personal data only be kept for a certain period? Please outline any such principles or "fair information practice principles" in detail.

Under the UK GDPR, general processing of personal data must take place in accordance with the key principles. These state that personal data must be:

- processed lawfully, fairly and in a transparent manner in relation to individuals ("lawfulness, fairness and transparency");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ("purpose limitation");
- adequate, relevant and limited to what is necessary in relation to the purposes of the processing ("data minimisation");
- accurate and, where necessary, kept up to date ("accuracy");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ("storage limitation"); and
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("integrity and confidentiality").

In addition, the data controller shall be responsible for, and must be able to demonstrate compliance with, the above principles ("accountability").

A key element of "lawfulness, fairness and transparency" is the need to establish a valid ground for processing personal data. The six available grounds for processing are:

- The data subject has given consent to the

processing of their personal data for one or more specific purposes.
- The processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (for instance providing a quote).
- The processing is necessary for the data controller to comply with legal obligations (not including contractual obligations).
- The processing is necessary to protect the vital interests (i.e., the life) of the data subject or another person.
- The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. The relevant task, function or authority must have a clear basis in law.
- The processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data. This ground is likely to be most appropriate where the controller uses the subject's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.

Most lawful bases require that processing is "necessary" for a specific purpose. If the controller could reasonably achieve the same purpose without the processing, they will not have a lawful basis for processing the data. The basis for processing needs to be determined before processing takes place, and it should be documented.

Processing of special categories of personal data is prohibited unless one of the additional conditions set out in Article 9(2) of the UK GDPR also applies (as set out in the response to question 8).

6. Are there any circumstances for which consent is required or typically obtained in connection with the general processing of personal data?

Consent is one of the lawful grounds for processing personal data. The UK GDPR sets a high standard for what constitutes valid consent (as further detailed in the following question 7). It is, therefore, not simple to establish valid consent as a ground for processing, and the individual can withdraw their consent at any time. As a result, it is often preferable to rely on another lawful basis for processing, if one is available.

There are, however, certain types of processing where consent is the only valid lawful basis available to the controller. In particular, processing of personal data collected through nonessential cookies and similar trackers or the processing of contact details for the sending of unsolicited electronic marketing messages should be based on consent. Each of these activities require consent under PECR, and the ICO takes the view that processing of personal data in connection with these activities cannot be based on a lawful basis other than consent.

Processing special categories of personal data also requires the "explicit consent" of the individual unless one of the other exemptions under Article 9(2) UK GDPR applies (as further detailed in question 8). When assessing whether to rely on consent, there are a number of context-specific questions that should be considered. For example, the requirement for consent to be "freely given" (meaning that data subjects must have a genuine choice) may be difficult to satisfy in certain circumstances, for example, if:

- performance of a contract is conditional on consent to the processing of personal data that is not necessary for the performance of that contract; or
- there is a clear imbalance between the data subject and the controller; or the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment, such as in the context of an employment relationship.

7. What are the rules relating to the form, content and administration of such consent? For instance, can consent be implied, incorporated into a broader document (such as a terms of service) or bundled with other matters (such as consents for multiple processing operations)?

Under the UK GDPR, the threshold for establishing valid consent is high. To be valid, the consent must be:

- Freely given – i.e., the consent is voluntary, and no detriment will be suffered if the data subject chooses not to consent. This also means that individuals must have an ongoing choice and control over how their personal

data is used, including the right to withdraw consent at any time.
- Specific – i.e., separate consents are required for different purposes and different types of processing.
- Informed – i.e., the data subject must be provided with sufficient information detailing what they are consenting to. For consent to be "informed", the data subject must be notified, as a minimum, of the controller's identity, the purposes of processing and the types of processing activity.
- Unambiguous – i.e., there must be a clear affirmative action by the data subject such as ticking a box to consent. It is not sufficient to imply consent from an individual's actions, using pre-ticked boxes or similar mechanisms.

Consent requests must be prominent, unbundled from other terms and conditions, concise, easy to understand and user-friendly.

Withdrawing consent will not affect the lawfulness of the processing preceding the withdrawal.

Records of consents obtained should be kept to demonstrate compliance with the principles.

8. What special requirements, if any, are required for processing sensitive personal data? Are any categories of personal data prohibited from collection or disclosure?

Additional considerations apply to the processing of "special categories of data" (as defined under question 4 above) and data related to criminal offences and/or convictions.

To process special category data lawfully, the controller must identify both a lawful basis and a separate condition for processing. The conditions for processing of special category data are set out in the UK GDPR, as tailored by the DPA 2018, and are:

- explicit consent;
- necessary for performing obligations or protecting rights in the field of employment, social security and social protection (if authorised by law);
- necessary to protect vital interests; o processing carried out by not-for-profit bodies; o data made public by the data subject; o necessary to establish, exercise or defend legal claims or judicial acts; o reasons of substantial public interest (with a basis in law); o necessary for health or social care (with a basis in law); o necessary for reasons of public health (with a basis in law); or o necessary for archiving, research and statistics (with a basis in law).

Where the additional conditions for processing special categories of personal data require a basis or authorisation in law, the DPA 2018 also sets out associated conditions and requirements.

Reliance on the substantial public interest condition would also require satisfying one of the specific substantial public interest conditions set out in the DPA 2018.

To process personal data about criminal convictions or offences, the controller must have a lawful basis and, in addition, either process the data in an official capacity or comply with the additional safeguards set out in the DPA 2018.

9. How do the data protection laws in your jurisdiction address health data?

Health data comes under the definition of special category data (see question 4 above). As such, there is no specific legislation that applies to health data outside of the provisions of the UK GDPR and DPA 2018.

However, there are certain special exemptions to the disclosure of health data in relation to a data subject access request or third-party request, as set out in the DPA 2018. These exemptions allow controllers to refuse to comply with a request for disclosure of health data in certain circumstances where:

- it would go against the wishes and expectations of the data subject (usually relevant to requests made by someone with parental responsibility over a minor or to requests for disclosure made by a court to manage the affairs of an individual who has been deemed as incapable of managing their own affairs); or
- it would be likely to cause serious harm to the physical or mental health of any individual.

10. Do the data protection laws in your jurisdiction include any derogations, exclusions or limitations other than those already described? If so, please describe the relevant provisions.

The DPA 2018 and UK GDPR set out exemptions from

some rights and obligations under the data protection regime. Controllers should not routinely rely on exemptions but instead should consider them on a case-by-case basis. If a controller relies on an exemption, it should justify and document its reasons for doing so.

Various exemptions are detailed in Schedules 2 to 4 of the DPA 2018. These exemptions can relieve a controller of some of its obligations, for instance in relation to the right to be informed, the right of access, dealing with other individuals' rights and complying with the data protection principles. How the exemptions are applied, and the extent of the exemption, will differ depending on the purpose for which a controller is processing the personal data.

Types of purposes that may rely on an exemption in the DPA 2018 include:

- for the prevention and detection of crime, apprehension and prosecution of offenders and assessment or collection of a tax or duty;
- information required to be disclosed by law or in connection with legal proceedings; o discharging functions designed to protect the public; o discharging a regulatory function conferred under specific legislation; o processing for journalistic, academic, artistic or literary purposes; and o processing for scientific or historical research purposes or for statistical purposes. There are also exemptions relating to the processing of health (as detailed in part in question 9 above) and social work data in certain circumstances.

Some exemptions only apply to the extent that compliance with the DPA 2018 would prejudice the purpose for which a controller is using the data or where it would prevent or seriously impair the controller from the necessary processing of personal data for its purpose. If this is not the case, then a controller must comply with the DPA 2018 as normal. Some exemptions have additional provisions that must be met before the exemption can be relied upon.

Processing of personal data for purely personal or household activity, with no connection to a professional or commercial activity, is outside the scope of the DPA 2018 and UK GDPR.

11. Do the data protection laws in your jurisdiction address children's and teenagers' personal data? If so, please describe how.

Data Protection Laws

The DPA 2018 and UK GDPR recognise that children need particular protection when their personal data is being collected and processed, as they may be less aware of the risks involved or their rights.

As with adults, there needs to be a lawful basis for processing personal data. If relying upon consent as the lawful basis for processing, the controller needs to ensure that the child can understand what they are consenting to, otherwise the consent is not "informed" and therefore is invalid. Any information and communication about processing addressed to a child should be in clear and in plain language that the child can easily understand.

In relation to the offer of online services directly to a child ("information society services"), the data subject must be at least 13 years old (in the UK) to consent to processing of their personal data. Where the child is under 13 years old, processing shall be lawful only if consent is given or authorised by the person with parental responsibility over the child. This will not apply if the information society services offered to the child are preventative or counselling services. Other European countries have different (and higher) age limits, so online businesses need to know the location of the child to ensure the right rules can be applied.

Extra protections apply where businesses intend to use children's personal data for marketing purposes, which includes both sending direct marketing messages to individual children and using personal data to display targeted adverts in an online context.

Children have the same individual rights as adults in relation to the processing of their data. The right to erasure of data is particularly relevant if they gave their consent to the processing when they were a child.

The ICO has published an Age-Appropriate Design Code (or "Children's Code") for providers of online services that may be accessed by children in the UK. For the purposes of the Children's Code, a child is anyone under the age of 18. The Children's Code sets out 15 standards to ensure that online services appropriately safeguard children's data and addresses how to design data protection safeguards into online services to ensure they are appropriate for use by, and meet the development needs of, children.

A service provider's conformance with the Children's Code will be taken into account by the ICO or a court when assessing whether that provider has complied with

their obligations under the DPA 2018, the UK GDPR and PECR. Although failure to comply with the Children's Code would therefore not in itself be a breach of UK data protection law, a service provider is unlikely to be able to satisfy the ICO or a court that they comply with the DPA 2018, the UK GDPR or PECR if they have not followed the standards in the Children's Code.

Online Safety

The UK passed the Online Safety Act (OSA) in October 2023, designed to make the internet safer by ensuring that "user-to-user services" and "search services" (Services) take practical steps to ensure their terms of service adequately protect children and adults online. Services will be categorised as either Category 1, Category 2A, or Category 2B, depending on the number of users and functionality of the Service, with various duties applying to each category. While the legislation covers online harms relevant to adults and children, one of the legislation's core aims is to identify, manage and mitigate risks arising from content and activity that is harmful to children (defined as those under the age of 18). The OSA also seeks to secure higher standards of protection for children, than for adults, online.

The OSA sets out specific measures that must be taken where Services are likely to be accessed by children, including:

- Conducting a child safety risk assessment for the Services or any significant change to the Services (note that this needs to be more detailed for Category 1 Services). The risk assessment must take into account:
    - the Service's user base, including the number of users who are children in different age groups; o the risk of children encountering various risk categories of content, and the accompanying risk of harm, giving separate consideration to children in different age groups and harm which particularly affects individuals with a certain characteristic or members of a certain group; o children's different age groups, and in particular algorithms used by the service and how easily, quickly and widely content may be disseminated by means of the service; o the extent to which the Service's design affects the level of risk of harm that might be suffered by children; o whether adults can search for or contact other users of the Service (including children); o functionalities or other features of the service that affect how much children use the service and any corresponding harm that might be suffered by children;
    - the nature, and severity, of the harm that might be suffered by children in different age groups; and o how the design and operation of the Service may reduce or increase any risks identified.
- Having measures in place that include age verification to prevent children from accessing harmful content. Any such verification must be highly effective at correctly determining whether or not a particular user is a child.
- Providing information regarding child protection measures in Services' terms of service, including how children:
    - are prevented from accessing harmful content; and
    - that are not prevented from accessing harmful or potentially harmful content, are protected from encountering it.

12. Do the data protection laws in your jurisdiction address online safety? Are there any additional legislative regimes that address online safety not captured above? If so, please describe.

The OSA sets out specific obligations which apply when Services may be accessed by children (Please refer to question 11 above). However, the OSA also sets out more general measures to combat online harms, depending on whether a Service is Category 1, 2A or 2B:

- All Services must use proportionate measures relating to the design and/or operation of the service to:
    - Prevent individuals from encountering illegal content.
    - Mitigate and manage the risk of someone using the service to facilitate a "priority offence" (e.g., offences relating to terrorism or child exploitation and abuse).
    - Effectively mitigate and manage the risks of harm to individuals.

- All Services must use proportionate systems and processes to:
    - Minimise the length of time any illegal content is present on the Service.
    - Swiftly take down illegal content when made aware of it.
- Services must also ensure that the following are designed to help protect individuals online:
    - Functionalities, algorithms, and other features. o Content moderation tools.
    - User empowerment technologies to enable individuals to filter out content and/or non-verified users.
    - User support and reporting mechanisms.
    - Staff policies and practices (as well as any other relevant internal policies).
- Terms of service must be applied consistently and must:
    - Explicitly state how individuals are to be protected from illegal content.
    - State whether any proactive technology is being used and if so, explain that technology.
    - Be drafted clearly and accessibly.
- All Services must also carry out and publish risk assessments and transparency reports related to illegal and harmful content on their services. Category 1 Services must summarise the findings of these risk assessments in their terms of service.
- Category 1 and 2A Services also have duties relating to online advertising, including:
    - Preventing individuals from encountering fraudulent advertisements in or via search results.
    - Minimising the length of time users see fraudulent advertisements.
    - Swiftly ensuring individuals no longer encounter fraudulent advertisements if alerted by an individual that such content may be on the platform.

In addition to the above, the OSA also introduced several new criminal offences for posters of content that is (i) a harmful or false communication (ii) a threatening communication (iii) cyberflashing (sending unsolicited sexual messages via data sharing / social media services), (iv) flashing (designed to stop epilepsy trolling) and (v) assisting or encouraging self-harm. Companies and senior managers of Services may also be criminally liable under the OSA if a Service fails to comply with enforcement notices or in relation to child sexual abuse and exploitation. Senior managers may also be criminally liable for failing to provide information requested by Ofcom.

13. Is there any regulator in your jurisdiction with oversight of children's and teenagers' personal data, or online safety in general? If so, please describe, including any enforcement powers. If this regulator is not the data protection regulator, how do those two regulatory bodies work together?

Ofcom, the UK's communications regulator, is responsible for enforcing the OSA. Under the OSA, Ofcom may fine Services up to £18 million or 10% of their annual global turnover, whichever is greater. In addition, with the agreement of the UK courts, Ofcom will also be able to require payment providers, advertisers, and internet service providers to stop working with a Service, preventing it from generating money or being accessed from the UK in the most extreme cases.

Obligations under the OSA sit alongside relevant obligations under the data protection laws, and accordingly Ofcom's enforcement powers sit alongside the ICO's enforcement remit relating to personal data.

14. Are there any expected changes to the online safety landscape in your jurisdiction in 2024–2025?

For the time being, stakeholders are focused on guidance to the OSA and supplementary legislation to be produced by the UK government.

Ofcom has announced that it will provide guidance on how organisations may comply with the OSA in three stages. In November 2023, Ofcom published draft codes and guidance on organisations' duties related to online harms. Further guidance on child safety is expected in Spring 2024, with guidance on the protection of women and girls expected in Spring 2025.

In addition, Ofcom must produce a register of categorised services (i.e., Category 1, 2A or 2B services) which will be determined under certain thresholds set out in secondary legislation to be made by the UK government. Assuming that this secondary legislation is forthcoming, Ofcom will publish a register of categorised

services by the end of 2024.

15. Does your jurisdiction impose 'data protection by design' or 'data protection by default' requirements or similar? If so, please describe the requirement(s) and how businesses typically meet such requirement(s).

Yes, controllers have a legal requirement under Article 25 of the UK GDPR, as well as under the DPA 2018 to consider privacy and data protection issues at the design phase of any system, service, product or process and then throughout the lifecycle ("data protection by design") and only process the data that is necessary to achieve their specific purpose ("data protection by default").

How controllers meet these requirements will depend on their circumstances. However, the ICO recommends that controllers should take an organisational approach to ensure that:

- data protection issues are considered as part of the design and implementation of systems, services, products and business practices which includes the deployment of adequate cybersecurity measures proportionate to the organisation's risk exposure and activities;
- data protection is an essential component of the core functionality of processing systems and services;
- processing is limited to the personal data that the controller needs in relation to its purposes(s), and data is only used for those purposes;
- personal data is automatically protected in any IT system, service, product, and/or business practice;
- the identity and contact information of those responsible for data protection are available both within the organisation and to individuals;
- there is a "plain language" policy for any public documents relating to personal data; o individuals have the tools to determine how the controller is using their personal data; and
- controllers offer strong privacy defaults, user-friendly options and controls, and respect user preferences.

16. Are controllers and/or processors of personal data required to maintain any internal records of their data processing activities or establish internal processes or written documentation? If so, please describe how businesses typically meet such requirement(s).

Under the UK GDPR, organisations with 250 or more employees must maintain a record of all processing activities, whether they are controllers or processors. Organisations with fewer than 250 employees need only maintain a record of processing activities that are likely to result in a risk to the rights and freedoms of data subjects, are not occasional, or include special categories of data or data related to criminal convictions or offences. Organisations may need to make their records available to the ICO on request.

Records of processing must contain:

- the name and contact details of the organisation (and where applicable, of other controllers, the organisation representative and their data protection officer);
- the purposes of the processing; o a description of the categories of individuals and categories of personal data; o the categories of recipients of personal data;
- details of any transfers to third countries including documenting the transfer mechanism safeguards in place;
- retention periods; and o a description of any technical and organisational security measures.

Controllers must also document the lawful basis relied on for the processing of personal data and any additional conditions relied on for processing special categories of personal data or data relating to criminal convictions.

A controller should more generally document its policies and processes so that it may comply with the "accountability" principle and meet its data protection by design/default obligations. A controller should also have a range of policies tailored to its business such as a data protection policy, retention and disposal policy, data breach policy, marketing policy, consent records, data maps, training materials and processes to comply with the data protection principles and to enable individuals to exercise their rights.

17. Do the data protection laws in your jurisdiction require or recommend data retention and/or data disposal policies and

procedures? If so, please describe such requirement(s).

One of the fundamental principles of the UK GDPR is that of storage limitation, as set out under Article 5(1)(e). This stipulates that personal data cannot be kept for longer than necessary for the purpose for which it was collected.

The UK GDPR does not specify a time limit, rather companies need to assess how long they require the data for their specified purpose(s).

When setting retention periods, companies should consider whether:

- the stated purpose(s) for the processing of personal data are still applicable; o a record of a relationship with the individual is needed once the relationship ends; o the information is required to defend possible future legal claims;
- there are any legal or regulatory requirements that require the retention of records (e.g., for income tax or audit purposes); and
- there are any industry standards or guidelines that can be used (although note that industry standards do not guarantee compliance).

Any personal data that is no longer needed should be erased or anonymised (see question 4 above).

18. Under what circumstances is a controller operating in your jurisdiction required or recommended to consult with the applicable data protection regulator(s)?

Under the UK GDPR, a controller must carry out a data protection impact assessment (DPIA) if the processing is likely to result in a high risk to individuals. If the DPIA identifies a high risk that the controller cannot mitigate or reduce, they must consult with the ICO prior to commencing the processing. When consulting the ICO, a controller shall provide details of:

- where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;
- the purposes and means of the intended processing;
- the measures and safeguards provided to protect the rights and freedoms of data subjects;
- where applicable, the contact details of the data protection officer; o the DPIA; and o any other information requested by the ICO.

The ICO will respond within eight weeks of the request for consultation and provide written advice to the controller. This may be extended by six weeks in complex cases. The ICO will provide a written response advising whether the risks are acceptable, or whether it is necessary to take further action. Where appropriate, the ICO can issue a formal warning not to process the personal data.

19. Do the data protection laws in your jurisdiction require or recommend risk assessments in connection with data processing activities and, if so, under what circumstances? How are these risk assessments typically carried out?

Yes, a DPIA should be carried out where the intended processing is “likely to result in high risks” to data subjects according to Article 35 of the UK GDPR.

It will be necessary to carry out a DPIA if the controller plans to:

- use systematic and extensive profiling with significant effects; o process special category or criminal offence data on a large scale; or o systematically monitor publicly accessible places on a large scale.

The current ICO guidance also indicates a DPIA should be conducted if the controller will:

- use innovative technology; o use profiling or special category data to decide on access to services; o profile individuals on a large scale; o process biometric data;
- process genetic data; o match data or combine datasets from different sources;
- collect personal data from a source other than the individual without providing them with a privacy notice (“invisible processing”);
- track individuals’ location or behaviour; o profile children or target marketing or online services at them; or
- process data that might endanger the individual’s physical health or safety in the event of a security breach.

The ICO also recommends that controllers should carefully consider carrying out a DPIA for any other

processing that is large scale, involves profiling or monitoring, decides on access to services or opportunities, or involves sensitive data or vulnerable individuals, or for any major new project involving the use of personal data.

The assessment should be carried out prior to any processing and contain at least:

- a description of the proposed processing, including its nature, scope, context and purposes;
- an assessment of the necessity and proportionality of the processing operations; o an assessment of the risks to the rights and freedoms of data subjects; and o the measures envisaged to address the risks.

The controller should also seek the advice of the data protection officer (if it has one) when carrying out the above assessment. When appropriate, the controller should seek the views of the data subjects (or their representatives) on the intended processing. If the DPIA indicates the processing will result in a high risk due to the absence of available measures to mitigate the risk, the controller should consult with the ICO as detailed under question 18 above.

20. Do the data protection laws in your jurisdiction require a controller's appointment of a data protection officer, chief information security officer, or other person responsible for data protection, and what are their legal responsibilities?

Under Article 37 of the UK GDPR, a person must appoint a data protection officer (DPO) if:

- it is a public authority or body (except for courts acting in their judicial capacity);
- its core activities require large scale, regular and systematic monitoring of individuals (for example, online behaviour tracking); or
- its core activities consist of large-scale processing of special categories of data or data relating to criminal convictions and offences.

This requirement applies to both controllers and processors. A group of undertakings can select a single DPO provided that the DPO is easily accessible from each establishment. A single DPO may also be designated for several public bodies/authorities. The DPO does not have direct personal liability under the DPA 2018 and the UK GDPR.

If a decision is made to appoint a DPO voluntarily, the business should be aware that the same requirements of the position and tasks apply had the appointment been mandatory.

The DPO's tasks are:

- to inform and advise on data protection laws;
- to monitor compliance with data protection laws, and with the business' data protection polices, including training staff and conducting internal audits;
- to advise on, and to monitor, DPIAs; o to cooperate with the ICO and other supervisory authorities; and
- to be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc.).

Where an organisation is within the scope of the UK GDPR but has no offices, branches or other establishments in the UK, it will need to appoint a UK representative. The UK representative acts primarily as a local contact point for correspondence and enquiries from individuals and the ICO. Note that this is a separate obligation to the equivalent requirement under the EU GDPR to appoint an EEA-based representative.

21. Do the data protection laws in your jurisdiction require or recommend employee training related to data protection? If so, please describe such training requirement(s).

The ICO makes clear in its guidance that it expects organisations to implement an all-staff data protection and information governance training programme. It provides the following recommendations for meeting its expectations:

- providing staff with comprehensive training on key areas of data protection such as handling data subject requests, data sharing, information security, personal data breaches and records management;
- a data protection governance structure is implemented whereby certain individuals are assigned specific responsibilities for managing and delivering data protection employee training;
- regular, accurate and targeted training is provided to employees; o maintaining and updating training records and materials; and o carrying our regular awareness of data protection policies, procedures and materials.

22. Do the data protection laws in your jurisdiction require controllers to provide notice to data subjects of their processing activities? If so, please describe such notice requirement(s) (e.g., posting an online privacy notice).

Under Articles 13 and 14 of the UK GDPR, individuals have the right to be informed about the collection and use of their personal data.

At the time personal data is obtained from a data subject, a controller must provide the data subject with all of the following privacy information:

- the identity and the contact details of the controller and, where applicable, the controller's representative; o the contact details of the data protection officer, where applicable;
- the purposes of the processing, as well as the legal basis for the processing; o the legitimate interests pursued by the controller or by a third party where the

"legitimate interests" lawful basis is being used; o the recipients or categories of recipients of the personal data, if any; o the source of the data; o the retention periods; o details of the individual's rights, including the right to withdraw consent; o the right to lodge a complaint with a supervisory authority;

- if there is a statutory or contractual obligation to provide certain details and the consequences of not providing these;
- if automated decision making or profiling is being conducted with meaningful information about the logic used and the intended consequences of the processing; and
- where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the mechanism that is being relied upon to allow the transfer, and where relevant, how to obtain a copy.

When personal data is obtained from a source other than the individual it relates to, the individual needs to be provided with the above privacy information:

- within a reasonable period of obtaining the personal data and no later than one month;
- if the data are used to communicate with the individual, at the latest when the first communication takes place; or
- if it is envisaged that the data will be disclosed to someone else, at the latest when the data is disclosed.

The controller must actively provide privacy information to individuals. It can meet this requirement by putting the information on its website, but it must make individuals aware of it and give them an easy way to access it, including at the point of when their data was collected. For all audiences, information must be concise, transparent, intelligible, easily accessible and in clear and plain language.

When providing the information to individuals, it is permissible to use a combination of techniques such as a layered approach to presenting the information, privacy dashboards, just in time notices and icons. A controller must regularly review, and where necessary, update its privacy information, and bring any new uses of an individual's personal data to their attention before starting any processing.

23. Do the data protection laws in your jurisdiction draw any distinction between the controllers and the processors of personal data, and, if so, what are they?

The law distinguishes between "controllers" and "processors". A controller is the main decision-maker who exercises control over how and why personal data is collected and the use of the data. The controller has the highest level of responsibility when it comes to complying with the DPA 2018 and the UK GDPR. It must make sure that the processing of that data complies with data protection law. UK controllers are also required to pay a data protection fee to the ICO unless exempt (see question 3 above).

A processor is the person who processes data on behalf of the controller and in accordance with their instructions. Processors do not have to pay the data protection fee. However, they have some statutory legal obligations in their own right under the UK GDPR and DPA 2018, although these are more limited than the controller's obligations. These include obligations in relation to processing contracts, security measures, security breach notifications, data protection officers and record-keeping.

Processors may also be:

- subject to investigation by their supervisory authority (such as the ICO); o fined for breaches of their direct obligations under the DPA 2018 and the UK GDPR; o contractually liable to the controller for breach of contract;

and/or
- subject to a claim in the courts for damage caused by their processing (including nonmaterial damage such as distress). However, they will only be liable insofar as they have failed to comply with the provisions specifically relating to processors, or they have acted without the controller's lawful instructions or against those instructions.

24. Do the data protection laws in your jurisdiction place obligations on processors by operation of law? Do the data protection laws in your jurisdiction require minimum contract terms with processors of personal data?

Obligations under law

Processors have some direct legal obligations under data protection laws. However, these are more limited, to reflect the fact that they have less autonomy and independence over the data they process. Obligations include:

- Activities limited to the controller's instructions: processors can only process personal data on the controller's instructions, or unless otherwise required by law.
- Mandatory Processor contracts: processors must enter into a binding contract with the controller (see below); however this is an obligation that primarily lies with the controller.
- Sub-processors: processors must not engage another processor (i.e., a sub-processor) without the controller's prior specific or general written authorisation. If authorisation is given, the processor must put in place a contract with the sub-processor with terms that offer an equivalent level of protection for the personal data as those in the contract between the original processor and the controller.
- Security: processors must implement appropriate technical and organisational measures to ensure the security of personal data, including protecting against accidental or unlawful destruction or loss, alteration, unauthorised disclosure or access.
- Notification of personal data breaches: processors must notify a controller if they become aware of a personal data breach without undue delay. Importantly, processors are required to notify controllers of data breaches regardless of the harm threshold. In effect, this means that processors must notify controllers of any security breach involving the controller's personal data. It is then for the controller to undertake any required risk of harm analysis and to decide the next steps. Processors must also assist the controller in complying with its obligations regarding personal data breaches (including any notifications to regulators or individuals).
- Notification of potential data protection infringements: processors must notify the controller immediately if any of its instructions would lead to a breach of data protection laws.
- Accountability obligations: processors must comply with accountability obligations, such as maintaining records and appointing a data protection officer.
- International transfers: processors must ensure that any transfer outside the UK is authorised by the controller and complies with the UK GDPR's transfer provisions.
- Cooperation with supervisory authorities: processors are also obliged to cooperate with the ICO to assist in the performance of its duties.

Contractual provisions

The UK GDPR specifies minimum contractual provisions that any contract between a controller and a processor must contain. These include:

- a requirement that the processor may only process personal data in line with the contractor's documented instructions;
- a restriction on appointing sub-processors without the controller's prior specific or general written authorisation. If a sub-processor is to be engaged under a general authorisation, then proposed changes must be notified in advance to give controllers a chance to object;
- a requirement to "flow-down" obligations under the contract between the controller and processor to any agreement with a sub-processor, so that the sub-processor contract offers an equivalent level of protection for the personal data;
- requirements for processors to assist with many of the obligations imposed on controllers (such as controllers' obligations to respond to the exercise of data subject rights, data security and other governance obligations);

- a direct statutory "policing" obligation, to "immediately inform" the controller if, in the processor's opinion, an instruction infringes relevant data protection laws; and
- "end-of-contract" provisions requiring the processor to delete or return all personal data at the end of the contract term.

Failing to include mandatory contractual provisions is in itself a breach of the UK GDPR.

Where a processor is located outside of the UK or the EU, the controller must ensure that contractual provisions adequately govern the transfer of the data flow between controller and processor (please see question 27 below for further information on international data transfers).

If data is being shared between two independent controllers, an appropriate data sharing agreement should be entered into by the parties as a matter of good practice but is not mandatory.

25. Are there any other restrictions relating to the appointment of processors (e.g., due diligence, privacy and security assessments)?

The controller may only use processors who provide sufficient guarantees that processing will meet the relevant data protection requirements and protect data subjects' rights. A controller will therefore need to conduct due diligence on a proposed processor to enable it to show how it has sought to comply with the data protection principles, including the security measures that the processor has in place, such as cybersecurity provisions proportionate to the processor's level of risk exposure and profile of the processor's and the controller's business.

26. Please describe any restrictions on monitoring, automated decision-making or profiling in your jurisdiction, including through the use of tracking technologies such as cookies. How are these terms defined, and what restrictions on their use are imposed, if any?

Automated decision-making is the making of a decision, about an individual, based solely on automated means without any human involvement.

The UK GDPR defines "profiling" as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements".

Controllers may generally engage in automated decision-making and profiling if they have a lawful basis for processing the personal data, comply with their transparency obligations and abide by the data subject's right to object. However, data subjects have the right not to be subject to a decision when it is based solely on automated processing (including profiling) if the decision produces legal effects or similarly significantly affects them. Such a process can only be carried out by an organisation if the decision is:

- necessary for entering into or performance of a contract between the organisation and the individual;
- authorised by law (for example, for the purposes of fraud or tax evasion); or o based on the individual's explicit consent.

Where the processing is carried out for contractual purposes or is based on the data subject's consent, the controller must implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, including at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

In addition, if special category personal data is involved, the controller can only carry out such processing if it takes suitable measures to safeguard the data subject's rights and:

- if it has the individual's explicit consent; or
- if the processing is necessary for reasons of substantial public interest and is provided for by law and must include measures to protect the interests of the individuals.

Automated decision-making in respect of children is generally prohibited, although the guidelines issued at the European level on automated decision-making and profiling indicate that there are narrow exemptions to this.

The PECR set out rules on the use of "cookies". A business must tell people if it uses cookies, and clearly explain what the cookies do and why. Cookies and similar technologies which are used to store or gain access to information on a device can only be used with the consent of the individual. As under the UK GDPR and DPA 2018 (and further explained in question 7 above),

consent must be freely given, specific and informed, and must be provided by way of a clear positive action. There is an exception for cookies that are essential to provide an online service at someone's request. Under the DPDI, the UK government is proposing to extend this exception to cookies that collect statistical information to make improvements, enable the appearance or function of a website to reflect user preferences, install necessary security updates to software on a device and identify the individual's geolocation in an emergency.

Cookie data may also be data which allows an individual to be identified, therefore falling within the rules on personal data in the DPA 2018 and UK GDPR.

27. Please describe any restrictions on targeted advertising and/or cross-contextual behavioral advertising. How are these terms or any similar terms defined?

UK data protection law does not define nor set out any specific rules with regards to crosscontextual behavioural advertising. However, any processing of personal data in the context of cross-contextual behavioural advertising would need to comply with the UK GDPR and PECR, including:

- rules relating to the use of cookies and similar tracking technologies (such as pixels and mobile SDKs);
- information and transparency requirements; and
- obligations relating to the validity of consent (namely ensuring such consent is sufficiently specific, freely given and informed, including with respect to potential recipients of the personal data).

28. Please describe any data protection laws in your jurisdiction addressing the sale of personal data. How is the term "sale" or such related terms defined, and what restrictions are imposed, if any?

"Sale" does not have a specific meaning in the context of the UK GDPR or DPA 2018. Selling personal data in the ordinary sense is not prohibited under UK data protection law. However, there is still an overarching obligation for organisations to comply with their general obligations under the UK GDPR. For example, organisations must have established a legal basis for the processing of the personal data it intends to sell and must comply with its transparency obligations (i.e., by providing clear details of the data sharing to the data subject at the point of collection of the personal data) and the purpose limitation principle (i.e., ensuring that data is not used for purposes incompatible with the purposes for which the data was originally collected).

29. Please describe any data protection laws in your jurisdiction addressing telephone calls, text messaging, email communication, or direct marketing. How are these terms defined, and what restrictions are imposed, if any?

Marketing activities using personal data must comply with the DPA 2018, UK GDPR and PECR.

Where personal data is processed for the purposes of direct marketing, the data subject has an absolute right to object to the processing. This right should be explicitly brought to the attention of the data subject at the time their data is collected and presented clearly and separately from any other information.

Where the data subject objects to processing for direct marketing purposes, the business should not continue to process the data for such purposes (including any profiling relating to such direct marketing).

In addition, PECR prohibits the sending of unsolicited electronic marketing messages unless the recipient has given their consent. "Electronic" messages cover email and text message, as well as any other message stored electronically (such as messages sent via social media). The rules also apply to automated voice calls (but not live voice calls).

"Consent" in this context must be of a GDPR standard, namely specific, informed and freely given. When relying on consent to market a business, it should therefore specify the different methods they want to use (e.g., by email, by text, by fax, by phone or by recorded call). In addition, it must ask for specific consent if it wants to pass details to other companies, and it must name or describe those companies in detail.

A business should also keep clear records of consent and keep a "do not contact" list of anyone who objects, opts out or withdraws their consent.

A limited exception to the consent requirement, known as "soft-opt", may apply where contact details are collected in the context of a sale or a negotiation for a sale, and:

- the marketing relates to the same/similar goods/services as those purchased or

negotiated;
- the customer is given the opportunity to opt-out of receiving marketing communications at the time of the purchase or negotiation and in every communication thereafter; and
- the marketing comes directly from the contracting entity/controller who has sold or is negotiating for the sale of the goods/services. The marketing must relate to similar products or services.

The marketing rules set out in PECR apply not only to the person sending the marketing messages but also to the person "instigating" those messages. A person using third-party contractors to send messages, or relying on viral marketing, therefore are still responsible for compliance with PECR in relation to those marketing messages.

There are also rules relating to telephone marketing which prohibit live unsolicited calls to:

- anyone who has already objected to the calls; or
- any number registered with the Telephone Preference Service, unless the recipient has specifically consented to receive the call.

Enforcement action relating to non-compliance with email, text and phone marketing rules in the UK has been frequent in the last few years, and the majority of fines issued by the ICO relate to nuisance phone calls and emails. Such fines can be large: from April 2023 to April 2024, the ICO issued a number of fines ranging from £100,000 to £250,000 for breaches of PECR.

30. Please describe any data protection laws in your jurisdiction addressing biometrics, such as facial recognition. How are such terms defined, and what restrictions are imposed, if any?

Under Article 4(14) of the UK GDPR, biometric data is "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data".

Biometric data will also be special category data if it is processed "for the purpose of uniquely identifying a natural person". This means that there will be additional requirements affecting processing, including the need for any consent to be "explicit" if consent is relied on as the lawful ground for processing.

Large-scale use of biometric data is likely to trigger the need for a DPIA, on the basis that the processing is likely to result in a high risk to the rights and freedoms of natural persons.

31. Please describe any data protection laws in your jurisdiction addressing artificial intelligence or machine learning ("AI").

While general data protection laws apply to personal data used in the context of AI, there are currently no stand-alone laws that apply to the use of AI in the UK. In February 2024, the UK government published a response to a 2023 White Paper consultation on regulating AI. Following this White Paper, the UK government does not propose to implement any change in law, but has adopted a non-binding framework for regulating AI to be implemented by relevant sector regulators.

32. Is the transfer of personal data outside your jurisdiction restricted? If so, please describe these restrictions and how businesses typically comply with them (e.g., does a cross-border transfer of personal data require a specified mechanism or notification to or authorization from a regulator?)

Transfers of personal data to countries outside the UK (including to Crown dependencies or UK overseas territories, including Gibraltar) are restricted and subject to limited exceptions. These restrictions apply to all transfers, no matter the size of transfer or how often they are carried out.

The most commonly applied exceptions to the prohibition on international transfers are:

The transfer is to a country, territory or international organisation in respect of which there is an adequacy regulation in place

At the time of writing, the UK's adequacy regulations cover the same jurisdictions, territories and international organisations considered adequate by the European Commission for transfers from the European Union, as well as all Member States in the European Economic Area and Gibraltar. As part of its plans to reform data protection law in the UK, the UK Government is working in partnership with a number of priority destinations which may be the subject of adequacy regulations in the future, including Australia, Brazil, Colombia, the Dubai

International Financial Centre, India, Indonesia, Kenya and Singapore.

On 10 July 2023, the European Commission adopted an adequacy decision in respect of the EU-U.S. Data Privacy Framework, permitting transfers between the EEA and entities participating in the Data Privacy Framework without further safeguards. This position was mirrored in the UK following the adoption of the UK GDPR extension to the EU-U.S. Data Privacy Framework. In this regard, the UK Secretary of State designated the U.S. as an adequate jurisdiction for the purposes of the UK GDPR on 21 September 2023, following the U.S. designation of the UK as a "qualifying state" for the purposes of EO 14086 on 18 September 2023.

There are appropriate safeguards in place (for example Standard Contractual Clauses or the UK-specific international data transfer agreement)

The new EU Standard Contractual Clauses (published on 4 June 2021) can be used for transfers of personal data from the UK subject to an addendum that adapts the EU approved text for transfers made under the UK GDPR. The UK Secretary of State has issued an approved addendum which can be used to supplement EU Standard Contractual Clauses for transfers that involve personal data subject to the UK GDPR.

The UK has also approved its own standalone international data transfer agreement (IDTA) for transfers of personal data under the UK GDPR.

A company uses approved binding corporate rules (BCRs)

BCRs can be used to legitimise a restricted transfer within an international organisation if both the entity making the transfer and the recipient have signed up to approved BCRs. They are intended for use by multinational corporate groups, groups of undertakings or groups of enterprises engaged in joint economic activity, such as franchises, joint ventures or professional partnerships. BCRs approved for international transfers under the EU GDPR require separate approval for transfers under the UK GDPR.

One of the limited derogations under Article 49 UK GDPR can be met

Article 49 of the UK GDPR sets out certain limited derogations from the prohibition on international transfers, including:

- explicit consent of the data subject;
- the transfer is necessary for the performance of a contract between the data subject and the controller;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; o the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims; and
- the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

Derogations are limited in scope and generally require that the transfer is only occasional and other than where the transferor relies on consent, necessary for the relevant purpose stated in the derogation. They are, therefore, not suitable for regular transfers (although the restricted transfer may happen more than once).

It should be noted that for transfers where no adequacy regulation is in place or in respect of which a derogation does not apply, the UK takes the same approach as the European Union in requiring a transfer impact assessment to ensure that data subjects of the transferred data continue to have a level of protection essentially equivalent to that under the UK data protection regime. The risk assessment should take into account the protections contained in the appropriate safeguard relied on for the transfer (such as the Standard Contractual Clauses or the UK's IDTA) and the legal framework of the destination country, including laws governing public authority access to personal data. If the assessment concludes that the transfer mechanism does not provide the required level of protection, the data exporter should include additional measures.

With regards to notification, international transfers of personal data do not generally require notification to the ICO. However, where data exporters cannot rely on any derogations, adequacy decisions or other transfer mechanisms, the UK GDPR allows organisations to make a one-off restricted transfer where it is in the organisation's compelling legitimate interests, and those interests outweigh the rights and freedoms of individuals. The ICO gives the example of a transfer of personal data to protect a company's IT systems from serious immediate harm.

Where such a one-off restricted transfer is made, the transferor would need to assess the circumstances surrounding the transfer and provide suitable safeguards

to protect the personal data, such as strict confidentiality agreements, a requirement for data to be deleted soon after transfer, technical controls to prevent the use of the data for other purposes or sending pseudonymised or encrypted data.

When making a transfer based on this exception, the transferring organisation must inform the individual, explaining its compelling legitimate interest to them, and the ICO. The ICO will ask to see full details of the assessment taken by the organisation in determining whether it can rely on this exemption.

33. What security obligations are imposed on data controllers and processors, if any, in your jurisdiction?

Both the controller and processor must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks arising from the processing of personal data. This includes adequate cybersecurity measures proportionate to the risk exposure of the organisation. The parties should consider factors such as the state of the art, implementation costs and the context of processing. Such measures could include pseudonymisation, encryption of personal data and a process for regularly testing the effectiveness of wider network security measures. The legislation does not specify the level of security required, since it needs to be proportionate to the risks presented by the processing being carried out.

Measures should be put in place following an evaluation of the risks to prevent unauthorised or accidental processing and to ensure it is possible to establish the precise details of any processing that takes place. The measures must ensure the confidentiality, integrity and availability of the systems and services that process personal data, and the data itself. Such measures should enable the controller to restore the personal data in a timely manner in the event of a physical or technical incident. Recently, the ICO has commented that measures should be proportionate and accurately recorded. Organisations have faced criticism when the security measures that they claim to have in place are not adhered to. (See for example the £98,000 fine issued to Tuckers LLP in March 2022. The ICO noted in part that, while Tucker's data protection policy required two-factor authentication where available, it did not use MFA for remote access).

34. Do the data protection laws in your jurisdiction address security breaches and, if so, how do such laws define a "security breach"?

Yes. Broadly speaking, UK legislation addresses security breaches in relation to personal data, as well as service operation and/or availability (see question 1 above).

Under the UK GDPR, a "personal data breach" is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. A personal data breach can also occur if there is unauthorised access within an organisation, or if a data controller's own employee accidentally alters or deletes personal data. The PECR adopts a similar definition, with an additional caveat that such personal data breach takes place in connection with the provision of a PECS.

Other legislation with cybersecurity requirements adopts different definitions. Under NIS, an "incident" is defined as any event having an actual adverse effect on the security of network and information systems, whereas the Communications Act 2003 sets out the definition of a "security compromise" in Sections 105A, which encompasses compromises of availability, performance and functionality, as well as security compromises and loss or alteration of data.

A business should ensure it has robust breach detection, identification, investigation and internal reporting procedures in place to help it determine whether it needs to notify the personal data breach to the relevant supervisory authority (e.g., the ICO) and the affected individuals. A business must keep a record of any personal data breaches, regardless of whether it is required to notify the breach.

35. Does your jurisdiction impose specific security requirements on certain sectors, industries or technologies (e.g., telecom, infrastructure, AI)?

As referred to in question 1 above, certain providers may also have separate security or reporting obligations under the PECR, eIDAS and NIS.

For example, under NIS, digital service providers (DSPs) and operators of essential services (OESs) must comply with more stringent cybersecurity measures and notification requirements in the event of a cyber incident, including a personal data breach. This is because of their increased risk profiles and the large-scale reliance on their services, which means that a cyber incident or service outage involving such entities

would have a highly disruptive impact across the UK.

DSPs are regulated by the ICO and include three types of businesses: (i) online search engines, (ii) online marketplaces and (iii) cloud computing services. The ICO does not designate companies as DSPs, and organisations are required to determine their potential status as a DSP themselves and consequently register with the ICO.

OESs relate to organisations across five sectors: energy, transport, health, drinking water supply and distribution and digital infrastructure. Each of these sectors has a separate designated competent authority responsible for the issuance of guidance and further regulations to govern their activities, responsibilities and obligations vis-à-vis the NIS Regulations. Even though the UK has now left the EU, the European Union Agency for Cybersecurity offers useful and concrete sector-specific guidance for OESs, including industry standard and best practice documents.

In January 2022, the UK announced a review of the UK cyber security regime under the current NIS Regulations (see question 42 below).

36. Under what circumstances must a business report security breaches to regulators, impacted individuals, law enforcement, or other persons or entities? If breach notification is not required by law, is it recommended by the applicable regulator in your jurisdiction, and what is customary in this regard in your jurisdiction?

All organisations subject to the UK GDPR have a duty to report personal data breaches to the relevant supervisory authority (i.e., the ICO) unless they are unlikely to result in a risk to the rights and freedoms of individuals. Controllers must report a breach without undue delay and where feasible within 72 hours of having become aware of it. Any delay in making a notification must be accompanied by reasons for the delay. Where it is not possible to provide all the relevant information to the ICO at the time of notification, the information may be provided in phases without undue further delay. Organisations must also notify the affected individuals without undue delay if the personal data breach is likely to result in a high risk to the rights and freedoms of such individuals. The notifications must contain certain information specified in the UK GDPR.

Where industry-specific notification requirements apply under sectorial legislation, relevant organisations must comply with notification timeframes set out in that legislation and in relevant guidance:

- Under PECR, PECS providers must notify the ICO without undue delay. While this had previously been mandated as within 24 hours of detection, the ICO has indicated that it will exercise its discretion not to pursue PECS providers that take longer than 24 hours to notify an incident, provided that the incident is reported within 72 hours and is unlikely to harm data subjects.
- Under the Communications Act 2003, PECS and PECN providers must notify incidents to Ofcom, for “urgent” compromises as soon as reasonably practicable and ideally within three hours of providers becoming aware of them, and non-urgent compromises within 72 hours of providers becoming aware of them.
- Under NIS, incidents must be notified without undue delay and in any event no later than 72 hours after the controller becoming aware of the incident.
- Under eIDAS, incidents must be notified without undue delay but in any event within 24 hours of the controller having become aware of the breach of security / loss of integrity.

37. Does your jurisdiction have any specific legal requirements or guidance for dealing with cybercrime, such as in the context of ransom payments following a ransomware attack?

While UK law enforcement does not encourage, endorse or condone ransom payments in ransomware attacks, the payment of a ransom is not of itself an offence. However, an offence may be committed where a payment is made to a sanctioned entity designated by the UK Government, determined to be subject to the Proceeds of Crime Act 2002 and/or where the payment with be subject to the Terrorism Act 2000. In February 2023, the UK Office of Financial Sanctions Implementation designated seven individuals subject to sanctions who were involved with known ransomware groups.

38. Does your jurisdiction have a separate cybersecurity regulator? If so, please provide details.

The United Kingdom does not have a separate

cybersecurity regulator. As raised above, the ICO determines whether an organisation has the appropriate technical and security measures in place in respect of processing personal data. However, the National Cyber Security Centre (NCSC) plays an important role in this field by providing organisations with cybersecurity advice and support (see www.ncsc.gov.uk). The NCSC oversees the implementation of the NIS Regulations in respect of organisations subject to it.

39. Do the data protection laws in your jurisdiction provide individual data privacy rights, such as the right to access and the right to deletion? If so, please provide a general description of such rights, how they are exercised, any exceptions and any other relevant details.

Individuals have the right to be provided with certain information about the collection and use of their personal data, including the purpose for processing, the retention period and who it will be shared with, as set out in response to question 22.

There are certain exceptions, including when the data subject already has the information, or where providing the information would prejudice the prevention, investigation, detection or prosecution of criminal offences. Additional limited exemptions apply where personal data is obtained from a source other than the data subject, including where providing the information proves impossible or would involve a disproportionate effort.

Individuals also have the following rights:

- the right to access their personal data; o the right to have inaccurate personal data rectified, or completed if it is incomplete; o the right to have personal data erased (also known as the “right to be forgotten”). The right is not absolute and the request may declined on various grounds, including where the deletion is not compatible with the right of freedom of expression and information, where processing is necessary to comply with a legal obligation, or necessary for the performance of a task carried out in the public interest or in the exercise of official authority;
- the right to restrict processing of personal data (so that it may only be stored and not used). This is not an absolute right and only applies in certain circumstances;
- the right to data portability. This allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability. The right only applies to information an individual has provided to a controller;
- the right to object to the processing of their personal data in certain circumstances. Individuals have an absolute right to stop their data being used for direct marketing. In other cases where the right to object applies a controller may be able to continue processing if it can show that it has a compelling reason for doing so. Controllers must tell individuals about their right to object; and
- other rights in relation to automated individual decision-making (making a decision solely by automated means without any human involvement); and profiling (automated processing of personal data to evaluate certain things about an individual) as set out in response to question 26.

The individual may make a request in relation to the above rights either verbally or in writing. There is a period of one month in which to respond. Note that a large percentage of complaints received by the ICO relates to the exercise of data subject rights, and the ICO has increasingly been focusing on compliance with subject access requests.

Companies should be aware that when dealing with subject access requests it is not possible in most circumstances to charge a fee for complying. However, in some cases a company can refuse to comply with a subject access request, usually where: (i) a relevant exemption applies; (ii) the request is manifestly unfounded; or (iii) the request is excessive. Reasons need to be given for refusal, and the data subject needs to be informed of their right to make a complaint to the ICO or to enforce the right judicially.

40. Are individual data privacy rights exercisable through the judicial system, enforced by a regulator, or both?

The ICO has the power to take action against controllers and processors. Individuals can complain to the ICO if they believe their rights have been infringed.

Individuals can also seek remedies through the courts and can bring claims for compensation and damages against both controllers and processors.

41. Do the data protection laws in your jurisdiction provide for a private right of action and, if so, under what circumstances?

Any person who has suffered material or non-material damage as a result of an infringement of the DPA 2018 and/or UK GDPR has the right to bring a claim for compensation against a controller or processor for the damage suffered. They can also complain to the ICO and relevant supervisory authorities.

Individuals do not need to show actual material damage or monetary loss in order to bring a claim, as the UK GDPR and DPA 2018 provide for a right to compensation for non-material damage, including distress.

Representative actions, comparable to US-style class action suits, have previously been used in privacy and data protection claims against organisations. However, the decision in Lloyd v Google LLC [2021] UKSC 50 has cast some doubt on the extent to which representative actions in the UK can be used in a similar way to class actions in the U.S. Representative opt-out actions can effectively be used to establish liability for infringements, but not necessarily to establish the quantum of damages. The latter would most likely need to be pursued through an opt-in group litigation order.

It is unclear whether the split process will be economically viable for litigation funders (who fund a sizeable proportion of these types of claims), as the expense of pursuing an opt-out claim to establish liability may not be recoverable through a subsequent opt-in procedure on quantum unless a sufficiently large number of claimants signs up.

The *Lloyd v Google* case was also determined under the old statutory regime predating the DPA 2018 and the UK GDPR, and so it is unclear whether the same decision would have been reached under current legislation.

42. Are individuals entitled to monetary damages or compensation if they are affected by breaches of data protection law? Does the law require actual damage to have been sustained, or is injury to feelings, emotional distress or similar sufficient for such purposes?

Yes, individuals are entitled to monetary damages for loss. Losses may be material or nonmaterial (including distress); however, any such loss must not be 'de minimis'.

43. How are data protection laws in your jurisdiction enforced?

The ICO has a range of powers it can exercise, including restricting or stopping the processing of personal data.

In addition, the ICO can issue fines on a controller or a processor for its breach of the obligations that apply to it. The ICO can issue an:

- information notice to require any person to provide information they reasonably require for the purposes of carrying out its functions, or investigating suspected failures or offences. It is an offence for a person, in response to information notice from the ICO, to make or recklessly make, a statement which they know to be false in a material respect.
- assessment notice to permit the ICO to carry out an assessment of a business to identify if it has complied with, or is complying with, data protection legislation. This can be done through means such as allowing the ICO access to specified premises, technology and directing the ICO to certain documents, and explaining such documents; and
- enforcement notice, which requires a person to take steps specified in the notice, or refrain from taking steps specified in the notice, or both. The notice must include details of what the person has failed, or is failing, to do and the ICO's reasons for reaching that opinion.

44. What is the range of sanctions (including fines and penalties) for violation of data protection laws in your jurisdiction?

There is a two-tier system of fines reflecting the seriousness with which a breach of specified obligation is viewed. For example, breaches of the principles, conditions applicable to consent, lawful basis, individual's rights and restricted transfers provisions are subject to the higher tier of up to £17.5 million or 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher. Breaches of obligations such as maintaining the record of processing activities, conducting a DPIA, a processor's obligations, privacy by design and appointing a data protection officer (amongst others) are subject to a lower standard tier where the maximum fine is £8.7 million or up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

The ICO when issuing a fine will take account of: the

nature, gravity and duration of the infringement, any mitigating action taken, previous infringements and the intentional or negligent character of the infringement.

At the time of writing, to date the highest fine issued by the ICO was in respect of a personal data breach suffered by British Airways, which was fined £20 million (revised down from £183 million) in 2020. The ICO found that British Airways had not implemented sufficient security measures, both to prevent the cyber-attack and to detect it. Other significant fines issued by the ICO include the £18.4 million fine issued to Marriott International in 2020 and £7.5 million issued to Clearview AI in 2022.

45. Are there any guidelines or rules published regarding the calculation of such fines or thresholds for the imposition of sanctions?

In March 2024, the ICO published Data Protection Fining Guidance, which details how the ICO determines penalty notices and calculates fines under the UK GDPR and DPA 2018. The guidance sets out that, where the ICO decides to issue a fine, the fine amount will be determined by applying the following five step approach: Step 1: Assessment of the seriousness of the infringement.

- Step 2: Accounting for turnover (where the controller or processor is part of an undertaking).
- Step 3: Calculation of the starting point having regard to the seriousness of the infringement and, where relevant, the turnover of the undertaking.
- Step 4: Adjustment to take into account any aggravating or mitigating factors.
- Step 5: Assessment of whether the fine is effective, proportionate and dissuasive.

The guidance sets out in detail how the ICO will categorise its starting point for a fine based on an infringement's lower, medium or higher degree of seriousness and the ranges for adjustment based on an undertaking's turnover. In particular, this new guidance has clarified that, where a controller or processor forms part of an undertaking, (e.g., as part of a company group), the ICO will calculate the maximum fine based on the turnover of the undertaking as a whole. In addition, in the event of more than one infringement by a controller or processor, the overall fine will not exceed the maximum statutory amount applicable to the most serious of the individual infringements identified.

The ICO has previously confirmed that when assessing the amount of any fine in data protection cases (including NIS cases) involving failures to meet data security obligations, it will consider the security breach separately from the failure to report the incident. In all other cases, the ICO will adopt a 'whole case' approach when setting the amount of fine.

46. Can controllers operating in your jurisdiction appeal to the courts against orders of the regulators?

An organisation can appeal an ICO decision to the First-tier Tribunal. Individuals can also appeal to the First-tier Tribunal if they have filed a complaint with the ICO and have not received a response within 3 months.

Data subjects can also apply to court for a compliance order requiring an organisation to take steps to remedy non-compliance with the data protection legislation.

47. Are there any identifiable trends in enforcement activity in your jurisdiction?

Large fines are not necessarily restricted to personal data breaches and further enforcement actions may be taken. While the highest fines to date (see question 44) still relate to personal data breaches and issues surrounding data security, the ICO has also levied large fines for non-compliance with other UK GDPR requirements. For example in May 2023, the ICO issued a £12.7 million fine against TikTok for failing to obtain appropriate consent from the parents of under 13s when offering its services, failing to provide transparent information regarding TikTok's collection, use and sharing of personal data, as well as failing to carry out adequate checks to identify and remove underage children from its platform.

A large proportion of fines still relate to breaches of unsolicited marketing rules. In the last year, around 90% of fines issued by the ICO related to unsolicited marketing calls, texts and emails. While such fines are typically not the largest issued by the ICO, they form a large part of the ICO's enforcement activity and are not insubstantial (fines have typically ranged from £30,000 to £250,000).

The ICO continues to focus on the data protection implications related to the use of biometric technologies. The ICO has published guidance on the use of biometric technologies. The guidance includes information regarding how organisations can process personal biometric data lawfully, fairly and transparently, how to comply with accuracy principles and how to comply with rights requests, and how to keep biometric data secure.

48. Are there any proposals for reforming data protection laws in your jurisdiction currently under review? Please provide an overview of any proposed changes and the legislative status of such proposals.

UK Data Protection Reform Bill

On 8 March 2023, the UK Government's Department for Science, Innovation and Technology introduced the new Data Protection and Digital Information (No.2) Bill (the DPDI) to the UK Parliament, amending a previous Bill introduced in July 2022. The DPDI seeks to reform the UK's existing data protection regime (including the UK GDPR, DPA 2018 and PECR). The DPDI will not replace these laws but seeks to amend and supplement these laws. Among other changes, the DPDI proposes changes to the rules regarding DPIAs, data subject access requests, the requirement to appoint representatives, records of processing activity and consent to certain types of cookies. According to the UK government's announcement, the DPDI is intended to reduce red tape and to "introduce a simple, clear and business-friendly framework".

NIS 2

On 14 December 2022, the EU adopted the Network and Information Security 2 Directive (NIS 2), expanding the scope of the Network and Information Security (NIS) Directive, the EU's first cybersecurity legislation. NIS 2 builds on the NIS Directive adopted in 2016. NIS 2 will cover a larger share of the EU economy and implement additional security and reporting requirements across EU states. As EU law, NIS 2 will not be implemented in the UK. However, on 30 November 2022, the UK government announced a proposal to expand the scope of the UK NIS Directive. The proposal suggests that some changes similar to NIS 2 can be expected. The proposals remained open for response until April 2023. Proposals include:

- expanding the scope of the UK NIS to "Managed Service Providers", i.e., B2B providers of services such as security monitoring, managed network services or the outsourcing of business processes which involve regular and ongoing service management of data, IT infrastructure, IT networks and/or IT systems;
- expanding the incident reporting requirements under UK NIS to include incidents which pose a significant risk to the security and resilience of the entities and the essential services they provide; and
- establishing a 2-tier supervisory regime for digital service providers in scope of UK NIS. The regime would have a proactive supervisory regime for the most critical digital services and a reactive supervisory regime for the remaining digital services under UK NIS.

Contributors

Kelly Hagedorn
Partner
khagedorn@orrick.com

Anna O'Kelly
Associate
anna.okelly@orrick.com