The Legal 500 Country Comparative Guides

United Kingdom: Data Protection & Cyber Security

This country-specific Q&A provides an overview to data protection & cyber security laws and regulations that may occur in United Kingdom.

For a full list of jurisdictional Q&As visit here

Contributing Firm

Orrick, Herrington & Sutcliffe LLP

Authors

Keily Blair
Partner
keily.blair@orrick.com

James LLoyd
Partner
james.lloyd@orrick.com

Lewis Brady
Managing Associate
lbrady@orrick.com

1. **Please provide an overview of the legal and regulatory framework governing privacy 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)?**

   The Data Protection Act 2018 (DPA 2018) sets out the legal framework applying to the collection and use of personal data in UK. It sits alongside the General Data Protection Regulation (GDPR) and tailors and supplements the application of the GDPR in the UK. The DPA 2018 will continue to apply after the UK's exit from the EU. The UK government also intends that the GDPR will continue to form part of UK law under the European Union (Withdrawal) Act 2018, with some technical changes to make it work effectively in a UK context.

   The DPA 2018 is not sector-specific. Anyone processing 'personal data', other than for purely personal or household activities, will need to comply with the data protection regime. This includes most businesses and organisations, whatever their size.

   Personal data is any information relating to a living individual (the 'data subject') who can be directly identified (for instance by their name and/and contact details) or indirectly identified (for instance by reference to an online identifier such as an IP address, cookie data and/or location data). Completely anonymised information is not personal data. However, if the person can still be identified, including by cross-referencing with information held by a third party, then the information may constitute personal data. Even information which is public knowledge or relates to an individual's professional life can be personal data.

   'Processing' is defined broadly under the DPA 2018 and the 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) exist alongside the DPA 2018. They give people specific privacy rights in relation to electronic communications and direct marketing. They set out specific rules on marketing calls, emails, texts and faxes and use of cookies and similar technologies. The EU intends to pass a new ePrivacy Regulation but this is not yet finalised and agreed.

   The Information Commissioner's Office (ICO) is the supervisory office for data protection in the UK, including England and Wales. The ICO provides guidance and promotes good practice. It also conducts audits and advisory visits, considers complaints and breach reports, monitors compliance and takes enforcement action where appropriate.

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

   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 organisation's number of employees or turnover. Public authorities should categorise themselves according to staff numbers only and not turnover. A controller will be exempt 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 where 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 co-operate with the ICO) may lead to an increase in the fine up to the statutory maximum of £4,350.

3. **How do these laws define personal data or personally identifiable information (PII) versus special category or sensitive PII? What other key definitions are set forth in the laws in your jurisdiction?**

The DPA 2018 and the GDPR use the terms 'personal data' and 'special categories of personal data'. These concepts are not identical 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 together with all the means reasonably likely to be used to identify that 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;
- personal data revealing political opinions;
- personal data revealing religious or philosophical beliefs;
- personal data revealing trade union membership;
- genetic data;

- biometric data (where used for identification purposes);
- data concerning health;
- data concerning a person's sex life; and
- data concerning a person's sexual orientation.

Other key definitions include:

- 'controller': the person which determines the purposes and the means by which the personal data is processed.
- 'processor': the person which processes personal data on behalf of the controller.

4. **What are the principles related to, the general processing of personal data or PII?**

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');
- 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.

5. **Are there any circumstances where consent is required or typically used in connection with the general processing of personal data or PII and, if so, are there are rules relating to the form, content and administration of such consent?**

Consent is one of the lawful grounds for processing personal data. However, it is 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.

Consent is defined as 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'. Affirmative action is required to clearly indicate acceptance of the proposed processing. Consent requires a positive opt-in, so pre-ticked boxes or any other method of default consent will not suffice. Consent requests must be prominent, unbundled from other terms and conditions, concise and easy to understand, and user-friendly.

The requirement for consent to be "freely given", meaning that data subjects must have a genuine choice. This may not be the case 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;
- 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.

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.

Where the processing has multiple purposes, separate consent should be obtained for all the purposes and should be clearly distinguishable.

The data subject must also be informed of the right to withdraw at any time. This will not affect the lawfulness of the processing preceding the withdrawal.

When special categories of data are being processed, consent must be explicit. Explicit consent requires a clear statement confirming that consent has been granted.

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

6. **What special requirements, if any, are required for processing sensitive PII? Are there any categories of personal data or PII that are prohibited from collection?**

Additional considerations apply to the processing of "special categories of data" (as defined under Q3 above) and data related to criminal offences and/or convictions.

In order to lawfully process special category data, 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 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 (ifauthorisedby law)
- Necessary to protect vital interests
- Processing carried out by not-for-profit bodies
- Data made public by the data subject
- Necessary to establish, exercise or defend legal claims or judicial acts
- Reasons of substantial public interest (with a basis in law)
- Necessary for health or social care (with a basis in law)
- Necessary for reasons of public health (with a basis in law)
- Necessary for archiving, research and statistics (with a basis in law).

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.

7. **How do the laws in your jurisdiction address children's personal data or PII?**

The DPA 2018 and GDPR recognize 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 below 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 EU member states have set 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.

8. **Does the law include any derogations, exclusions or limitations other than those already described? Please describe the relevant provisions.**

The DPA 2018 and 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 individual's 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;

- discharging functions designed to protect the public;
- discharging a regulatory function conferred under specific legislation;
- processing for journalistic, academic, artistic or literary purposes; and
- processing for scientific or historical research purposes or for statistical purposes.

There are also exemptions relating to the processing of health 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 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 GDPR.

9. **Does your jurisdiction impose requirements of 'data protection by design' or 'data protection by default' or similar? If so, please describe the requirement and how businesses typically meet the requirement.**

Yes, controllers have a legal requirement under Article 25 of the GDPR and 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 that ensures that:

- data protection issues are considered as part of the design and implementation of systems, services, products and business practices;
- 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;
- 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.

10. **Are owners or processors of personal data or PII required to maintain any internal records of their data processing activities or to establish internal processes or written documentation? If so, please describe how businesses typically meet these requirements.**

    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 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.
    - The lawful basis for the processing.
    - A description of the categories of individuals and categories of personal data.
    - The categories of recipients of personal data.
    - Details of any transfers to third countries including documenting the transfer mechanism safeguards in place.
    - Retention periods.
    - A description of any technical and organisational security measures.

    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.

11. **When are you required to, or when is it recommended that you, consult with data privacy regulators in your jurisdiction?**

    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 Information Commissioner’s Office (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;
- the data protection impact assessment; and
- 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.

12. **Do the laws in your jurisdiction require or recommend conducting risk assessments regarding data processing activities and, if so, in what circumstances? How are these risk assessments typically carried out?**

Yes, a data protection impact assessment (DPIA) should be carried out where the intended processing is "likely to result in high risks" to data subjects.

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

- use systematic and extensive profiling with significant effects;
- process special category or criminal offence data on a large scale; or
- 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;
- use profiling or special category data to decide on access to services;
- profile individuals on a large scale;
- process biometric data;
- process genetic data;
- 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;
- 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 use of personal data.

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

- a description of the proposed processing, its purposes and the legitimate interest pursued by the controller;
- an assessment of the necessity and proportionality of the processing operations;
- an assessment of the risks to the rights and freedoms of data subjects; and
- 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 subject (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 11 above.

13. **Do the laws in your jurisdiction require appointment of a data protection officer (or other person to be in charge of privacy or data protection at the organization) and what are their legal responsibilities?**

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 behavior 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 providing 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.

If a decision is made to voluntarily appoint a DPO 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, data protection impact assessments;

- 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).

14. **Do the laws in your jurisdiction require businesses to providing notice to individuals of their processing activities? If so, please describe these notice requirements (e.g. posting an online privacy notice).**

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, of the controller's representative;
- the contact details of the data protection officer, where applicable;
- the purposes of the processing as well as the legal basis for the processing;
- the legitimate interests pursued by the controller or by a third party where the 'legitimate interests' lawful basis is being used;
- the recipients or categories of recipients of the personal data, if any;
- source of the data;
- retention periods;
- details of the individual's rights, including the right to withdraw consent;
- 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 you use the data to communicate with the individual, at the latest, when the first communication takes place; or
- if you envisage disclosure to someone else, at the latest, when you disclose the data.

The controller must actively provide privacy information to individuals. They can meet this requirement by putting the information on their website, but they must make individuals aware of it and give them an easy way to access it which includes at the point of collection of their data. 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 processing.

15. **Do the laws in your jurisdiction draw any distinction between the owners/controllers and the processors of personal data and, if so, what are they? (E.g. are obligations placed on processors by operation of law, or do they typically only apply through flow-down contractual requirements from the owners/controller?)**

The law distinguishes between 'controllers' and 'processors'. A controller is the main decision-maker which exercises control over how and why to collect and use the data. The controller has the highest level of responsibility when it comes to complying with the DPA 2018 and the GDPR. They must make sure that the processing of that data complies with data protection law. Controllers are also required to pay a data protection fee to the ICO unless exempt.

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 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);
- fined for breaches of their direct obligations under the DPA 2018;
- contractually liable to the controller for breach of contract;
- subject to a claim in the courts for damage caused by their processing (including non-material damage such as distress. However, they will only be liable in so far 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.

16. **Do the laws in your jurisdiction require minimum contract terms with processors of personal data or PII or are there any other restrictions relating to the appointment of processors (e.g. due diligence or privacy and security assessments)?**

Yes, the 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 authorization. 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.
- an obligation 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 must offer 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.
- "end-of-contract" provisions requiring the processor to delete all personal data at the end of the contract term.

Failing to include mandatory contractual provisions is itself a breach.

Where a sub-processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that sub-processor's obligations.

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.

If data is being shared between two independent controllers, an appropriate data sharing agreement should be entered into by the parties.

17. **Please describe any restrictions on monitoring or profiling in your jurisdiction including the use of tracking technologies such as cookies. How are these terms defined and what restrictions 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 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.

In addition, 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
- 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-taking in respect of children is generally prohibited but the guidelines issued by the Article 29 Working Party 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 GDPR and DPA 2018, consent must be freely given, specific and informed, and must 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. Cookie data may also be an identifier which allows an individual to be identified, therefore falling within the rules on personal data in the DPA 2018 and GDPR.

18. **Please describe any laws in your jurisdiction addressing email communication or direct marketing. How are these terms defined and what restrictions are imposed, if any?**

Marketing activities using personal data have to comply with the DPA 2018 (DPA 2018) and

Privacy and Electronic Communications Regulations (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, under the PECR, there are rules governing marketing by certain methods. For example, electronic messages marketing (such as by email) and text marketing can only be sent to customers with their consent unless the soft-opt in applies. There are also rules relating to telephone marketing which requires the number to be screened against the Telephone Preference Service.

The soft-opt in applies where the details are collected in the context of a sale or a negotiation for a sale and (a) the marketing relates to the same/similar goods/services as those purchased or negotiated; (b) the customer is given the opportunity to opt-out at the time of the purchase or negotiation and in every communication thereafter; and (c) the marketing comes directly from the contracting entity/controller who has sold or is negotiating for the sale of the goods/services ie the same entity. The marketing must relate to similar products or services and the marketing recipient must be given a simple means of refusing marketing at the time their data is collected.

When relying on consent to market a business should specify the different methods they want to use eg 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.

At the time of writing, a new E-Privacy Regulation is currently being prepared which will impact the above. The ICO has confirmed that PECR, together with the GDPR standard of consent, will continue to apply until the E-Privacy Regulation is finalised.

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

Under Article 4(14) of the 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.

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

Transfers of personal data to countries outside the European Economic Area ('EEA') (EU member states and Iceland, Norway and Liechtenstein) are restricted. These restrictions apply to all transfers, no matter the size of transfer or how often they are carried out.

The transfer may take place if it is to a country which is covered by an EU Commission 'adequacy decision'. This is a finding by the Commission that the legal framework in place in that country, territory, sector or international organisation provides 'adequate' protection for individuals' rights and freedoms for their personal data. Details of such countries can be found on the ICO's website at www.ico.org.uk. The adequacy finding for the USA is only for personal data transfers covered by the EU-US Privacy Shield framework. US companies certified by the scheme subject to certain obligations to protect personal data and provide for redress mechanisms for individuals.

If there is no adequacy decision, then the controller must put in place an appropriate safeguard to enable the transfer to take place, such as the EU Commission model contracts or other mechanisms such as binding corporate rules for internal group transfers.

In the absence of a EU Commission adequacy decision, or of appropriate safeguards, a transfer shall only take place if one of the specific derogations/conditions apply such as the data subject has given their explicit consent, the transfer is necessary for performance of a contract, or for important reasons of public interest or the establishment, exercise or defence of legal claims or necessary to protect the vital interests of the data subject or another where the data subject is physically or legally unable to give consent.

21. **What security obligations are imposed on personal data or PII owners/controllers and on 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. The parties should take into account 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 such measures. The legislation does not specify the level of security required, since it needs to be proportionate to the risks presented by the processing carried out.

Measures should be put in place following an evaluation of the risks in order 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.

22. **Do the laws in your jurisdiction address security breaches and, if so, how does the law define "security breach"?**

Yes. Under the DPA 2018, 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.

A business should ensure it has robust breach detection, 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 about a personal data breach. A business must keep a record of any personal data breaches, regardless of whether it is required to notify the breach.

23. **Does your jurisdiction impose specific security requirements on certain sectors or industries (e.g. telecoms, infrastructure)?**

Certain providers may also have separate security or reporting obligations under other laws the PECR, eIDAS Regulation 2014 (electronic identification and trust services) and NIS Regulation 2018 (certain digital services).

24. **Under what circumstances must a business report security breaches to regulators, to individuals, or to other persons or entities? If breach notification is not required by law, is it recommended by the regulator and what is the typical custom or practice in your jurisdiction?**

All organisations have a duty to report certain types of personal data breach to the relevant supervisory authority (i.e. the ICO). Controllers must report a breach without undue delay

and where feasible within 72 hours of having become aware of it. Where it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay. Any delay in making a notification must be accompanied by reasons for the delay. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, those individuals must be informed without delay.

25. **Does your jurisdiction have any specific legal requirement or guidance regarding dealing with cyber-crime, such as the payment of ransoms in ransomware attacks?**

    n/a

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

    n/a

27. **Do the 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 the rights, how they are exercised, what exceptions exist 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. This information needs to be provided at the time of collecting the data. There are certain exceptions, including when the data subject already has the information, where providing the information would be disproportionate, or whether there is an obligation of professional secrecy.

    Individuals also have the following rights:

    - The right to access their personal data.
    - The right to have inaccurate personal data rectified, or completed if it is incomplete.
    - 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 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 you may be able to continue processing if you can show that you have a compelling reason for doing so. You must tell individuals about their right to object.
- 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).

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. It is not possible in most circumstances to charge a fee for complying. The main grounds for refusal are: a relevant exemption; the request is manifestly unfounded; or 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.

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

The ICO has the power to take action against controllers and processors. In addition, individuals can bring claims for compensation and damages against both controllers and processors.

29. **Does the law in your jurisdiction provide for a private right of action and, if so, in what circumstances?**

Any person who has suffered as a result of an infringement of the DPA 2018 has the right to raise a claim against and the right to receive compensation from a controller or processor for the damage suffered. They can also complain to the ICO and relevant supervisory authorities.

30. **Are individuals entitled to monetary damages or compensation if they are affected by breaches of data privacy laws? Is actual damage required or is injury of feelings sufficient?**

Yes, individuals are entitled to monetary damages. Damage may be material or non-material (including distress).

31. **How are the laws governing privacy and data protection enforced?**

The Information Commissioner’s Office (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 to fail to comply with an information notice, whether intentionally or recklessly and the court can make an order to compel the person to comply with the information notice.
- assessment notice to permit the ICO to carry out an assessment of a business to identify if they have complied with, or are 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.
- an 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.

32. **What is the range of fines and penalties for violation of these laws?**

There is a two-tier system of fines reflecting the seriousness with which a breach of specified obligations 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 €20,000,000 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 data protection impact assessment, 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 €10,000,000 or up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

The ICO in 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. The maximum amount of the penalty in sterling will be determined by applying a spot rate exchange set by the Bank of England on the day on which the penalty notice is given.

33. **Can personal data or PII owners/controller appeal to the courts against orders of the regulators?**

An organisation can appeal if they consider that a decision notice issued by the ICO is wrong. They can also appeal against certain decisions made under the DPA 2018.