Chambers

GLOBAL PRACTICE GUIDE

Definitive global law guides offering comparative analysis from top ranked lawyers

Data Protection & Cybersecurity

Second Edition

Contributing Editor
Sidley Austin LLP

chambers.com

2019

Law and Practice

Contributed by Sidley Austin LLP

Contents

Sidley Austin LLP is a premier law firm with a practice attuned to the ever-changing international landscape. The firm advises clients around the globe, with more than 2,000 lawyers worldwide. Sidley maintains a commitment to providing quality legal services and to offering advice in litigation, transactional and regulatory matters spanning virtually every area of law. The firm's lawyers have wide-reaching legal backgrounds and are dedicated to teamwork, collaboration and superior client service. Sidley's lawyers help a range of businesses address some of the most challenging matters concerning data protection, privacy, information security and incident response, data commercialisation, internet and computer law, intellectual property, information management and records retention, e-commerce, consumer protection and cyber-crimes. Lawyers advise clients with extensive operations in Europe, as well as in the US, Asia and elsewhere, on developing and implementing global data-protection programmes.

The authors would like to acknowledge Francesca Blythe and Vishnu Shankar for their assistance with this chapter.

Authors

William RM Long is a global co-leader of Sidley's highly ranked Privacy and Cybersecurity practice and also leads the EU data protection practice at Sidley. William advises international clients on a wide variety of GDPR, data protection, privacy, information security, social media, e-commerce and other regulatory matters. William has been a member of the European Advisory Board of the International Association of Privacy Professionals (IAPP) and on the DataGuidance panel of data protection lawyers. He is also on the editorial board of e-Health Law & Policy and also assists with dplegal ("data privacy" legal), a networking group of in-house lawyers in life sciences companies examining international data protection issues. William has also published widely on data protection matters. William was previously in-house counsel to one of the world's largest international financial services groups. He has been a member of a number of working groups in London and Europe looking at the EU regulation of e-commerce and data protection and spent a year at the UK's Financial Law Panel (established by the Bank of England), as assistant to the Chief Executive working on regulatory issues with online financial services. William has published widely on data protection and cybersecurity.

Geraldine Scali practises mainly in the areas of data protection, privacy, e-commerce and information technology. Geraldine advises international clients on the implementation of global compliance data protection and privacy projects, social media and on a broad range of data protection and privacy issues. In particular, Geraldine has experience with regard to cross-border transfers including Binding Corporate Rules, cybersecurity, security breach responses, the use of whistle-blowing hotlines and cloud computing. Geraldine also has experience in assisting clients on the drafting and negotiation of software development, software licence and services and outsourcing agreements. In addition, she regularly speaks on data protection, cybersecurity and cloud computing and writes for a number of journals. In 2013, Geraldine co-founded Women in Privacy®, an international networking group established for women working as in-house counsel, compliance officers and other professionals in the field of privacy. Prior to joining Sidley, Geraldine practised in France in leading French and English law firms focusing on computer law, e-commerce, data protection, privacy and communication law. She is a dual-qualified lawyer, admitted as a Solicitor in England and Wales in 2014, and a French lawyer admitted to the Paris bar in 2005.

1. Basic National Legal Regime

1.1 Laws

The EU General Data Protection Regulation 2016/679 (GDPR) came into force on 25 May 2018 and regulates the collection and processing of personal data of individuals in the EU, by imposing obligations on controllers, ie, organisations that determine the means and purposes of processing, and processors, which process personal data on behalf of the controller, when processing personal data of EU individuals.

As a directly applicable Regulation, the legal obligations contained in the GDPR have direct effect in the UK without any national implementing measures. However, the GDPR contains a number of derogations that provide EU Member States with discretion to introduce specific derogations on how certain provisions of the GDPR will apply in Member State law.

The UK has introduced specific derogations in UK law through the UK Data Protection Act 2018 ('DPA 2018'). The DPA 2018 repealed the UK Data Protection Act 1998, which had implemented the EU Data Protection Directive 95/46/EC into UK law. The DPA 2018 supplements the adoption of the GDPR into UK law by dealing with UK derogations and the transposition of the Law Enforcement Directive 2016/680, as well as implementing national security provisions and setting out the powers and duties of the national data supervisory authority, the UK's Information Commissioner's Office (ICO).

In light of the UK's scheduled departure from the EU on 29 March 2019 ('Brexit'), the UK government has introduced the draft Data Protection, Privacy and Electronic Communications (Amendments, etc) (EU Exit) Regulations 2019 ('Draft Regulations'), which make amendments to the DPA 2018 to ensure UK data protection law functions effectively post-Brexit. For example, the Draft Regulations replace references to EU Member States and EU institutions, practices and procedures that will no longer be directly relevant to UK data protection law post-Brexit, with UK equivalents. In addition, references to the GDPR have been amended to refer to the UK GDPR and references to the ICO's obligations to co-operate with other Member State data supervisory authorities have been revoked under the Draft Regulations.

The Draft Regulations also maintain the extra-territorial application of the GDPR for the UK. As such, controllers and processors established outside of the UK who are processing the personal data of individuals in the UK for the purposes of providing goods or services to, or monitoring the behaviour of, individuals in the UK will be subject to the UK GDPR.

The Draft Regulations also impose a requirement for organisations, outside of the UK who are subject to the UK GDPR by virtue of its extra-territorial application, to appoint a data protection representative in the UK, (ie, in line with Article 27 of the GDPR). To the extent there is a 'no deal' Brexit (see Section 1.3 for further information) the requirement to appoint a UK data protection representative would extend to companies in the EU.

The Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended by the Privacy and Electronic Communications (EC Directive) (Amendments) Regulations 2011) (PECR) regulate direct marketing in the UK, but also the processing of location and traffic data and the use of cookies and similar technologies. The PECR has implemented Directive 2002/58/EC (as amended by Directive 2009/136/EC) (the e-Privacy Directive). The Draft Regulations amend PECR to introduce the GDPR definition of consent (ie, a freely given, specific, informed and unambiguous indication of the individual's wishes).

The European Commission, European Council and European Parliament are currently in negotiations on the replacement of the e-Privacy Directive with the e-Privacy Regulation. The e-Privacy Regulation, which will complement the GDPR and have direct effect in Member States, aims to reinforce trust and security in the digital single market by updating the legal framework on e-Privacy and provides additional sector-specific rules including in relation to online marketing and the use of website cookies. However, the e-Privacy Regulation is not expected to come into force until late 2021 at the earliest, by which point the UK will no longer be an EU Member State, should Brexit occur.

The UK's Freedom of Information Act 2000 (FOIA) creates a public 'right of access' to information held by public authorities. The full provisions of the FOIA came into force on 1 January 2005 alongside the Environmental Information Regulations 2004, which is a UK statutory instrument (SI 2004 No 3391) that provides a statutory right of access to environmental information held by UK public authorities.

1.2 Regulators

The UK's national data supervisory authority is the ICO, headed by the Information Commissioner. The ICO is a non-governmental public body that reports directly to the UK parliament and is sponsored by the UK government's department for digital, culture, media and sport (DCMS). It is the independent regulatory office dealing with the DPA 2018, PECR, the FOIA and the Environmental Information Regulations 2004 in England, Wales and Northern Ireland and, to a limited extent, in Scotland.

The ICO has several enforcement powers under the DPA 2018 in the UK, including, inter alia, the power to issue the following:

- *information notices* – requiring controllers and processors to provide the ICO with information that the Information Commissioner reasonably requires in order to assess compliance with the GDPR and/or DPA 2018;
- *assessment notices* – requiring the controller or processor to permit the ICO to carry out an assessment of whether the controller or processor is in compliance with the GDPR and/or DPA 2018 (this may include the power of the ICO to conduct an audit, where the assessment notice permits the ICO to enter specified premises, inspect or examine documents, information and material, and observe the processing of personal data on the premises);
- *notice of intent* – where the ICO issues a notice of intent to fine the controller or processor in relation to a breach of the GDPR and/or the DPA 2018 after conducting its investigation. Such a notice sets out the ICO's areas of concern with respect to potential non-compliance with the GDPR and/or the DPA 2018, and grants the controller or processor the right to make representations. After such representations have been carefully considered, the ICO reaches its final decision on any enforcement action in the form of an enforcement notice;
- *enforcement notices* – such notices are issued where the ICO has concluded that the controller or processor has failed to comply with the GDPR and/or the DPA 2018, and sets out the consequences of non-compliance, which could include a potential ban on processing all or certain categories of personal data; and
- *penalty notices* – if the ICO is satisfied that the controller or processor has failed to comply with the GDPR and/or the DPA 2018, or has failed to comply with an information notice, an assessment notice or an enforcement notice, the ICO may, by written notice, require a penalty to be paid for such failure. Under the GDPR, such monetary penalties can amount to EUR20 million (GBP17 million) or 4% of annual worldwide turnover.

As the DPA 2018 came into effect on 23 May 2018, any information notices issued by the ICO to commence possible investigations or assessment or enforcement notices served prior to 23 May 2018 and thus under the Data Protection Act 1998, continue to have effect under the DPA 2018.

In a speech at the data protection practitioners' conference on 9 April 2018, the Information Commissioner, Elizabeth Denham, stated that "enforcement is a last resort" and that she has "no intention of changing the ICO's proportionate and pragmatic approach after the 25th of May." She added: "Hefty fines will be reserved for those organisations that persistently, deliberately or negligently flout the law," and that "those organisations that self-report, engage with us to resolve issues and can demonstrate effective accountability arrangements can expect this to be a factor when we consider any regulatory action." See **1.4 Key Developments** for further information on the fines issued by the ICO.

In addition, the ICO is responsible for promoting public awareness and in particular raising awareness amongst controllers and processors of their obligations under the GDPR and DPA 2018. The ICO has published extensive guidance on complying with the GDPR, and an overview of the DPA 2018.

1.3 Multilateral and Subnational Issues

On 23 June 2016, the UK voted in a referendum to leave the European Union by 51.9% to 48.1%. On 29 March 2017, the UK Government invoked Article 50 of the Treaty on European Union (TEU), which triggered a two-year withdrawal process from the EU, with the UK scheduled to depart the EU on 29 March 2019.

On 26 June 2018, the European Union (Withdrawal) Act 2018 was given royal assent and officially became law, repealing the European Communities Act 1972, the Act that provided the legal basis for the UK's accession to the then European Community.

On 15 January 2019, the UK Parliament rejected the draft Withdrawal Agreement, negotiated by Britain's Prime Minister Theresa May and the EU, by 432 votes to 202. Under the terms of the Withdrawal Agreement, the UK would have remained a member of the EU until 31 December 2020 (ie, the transitional period).

As it currently stands, the UK Government is in negotiations with the EU to try to secure further amendments to the Withdrawal Agreement, in order to gain approval from the UK Parliament in a second vote.

In the event of a 'no deal,' a valid international data transfer solution will need to be put in place in order to legitimise transfers of personal data from the EU to the UK (eg, European Commission approved standard contractual clauses or 'model contracts'). In the long term, the UK is hoping for an adequacy decision from the European Commission to permit the free flow of personal data from the EU to the UK, post-Brexit. However, the UK is unlikely to be prioritised in this regard in the event of a no deal. Importantly, the UK Government has confirmed that no restrictions will be put in place for the transfer of personal data from the UK to the EU.

As is the case currently, post-Brexit transfers of personal data from the UK to outside of the EEA will still require a valid international data transfer solution. Currently, in relation to transfers of personal data to the US, the EU–US Privacy Shield enables the free flow of personal data from the EEA to US participant organisations that commit to adhering to Privacy Shield principles. Even though, post-Brexit, the UK will no longer be an EU Member State, the ICO has recently issued guidance stating UK organisations will continue to be able to rely on the Privacy Shield in the event of a no-deal Brexit, provided the US participant organisations have

updated their public commitments to state expressly that those commitments also apply to transfers of personal data from the UK as well as the EU. Such public commitments are usually given in a privacy policy.

1.4 Key Developments

As of February 2019, the ICO had published one enforcement action under the DPA 2018, which was against a global data services company. The ICO imposed a total ban on its processing of personal data due to its failure to comply with the data protection principles under the DPA 2018.

The ICO has also continued to take other enforcement action under the previous Data Protection Act 1998, due to the timing of the relevant breach and the legislation in place at the time, including, inter alia:

- in November 2018, fining a ride-sharing company GBP385,000 for inadequate technical and organisational measures that failed to protect customer personal data during a cyber-attack, with the cyber-attacker accessing and downloading the personal data of 2.7 million UK customers, including names, email addresses and phone numbers, and taking the personal data of almost 82,000 drivers; and
- in October 2018, fining a global social media provider GBP500,000 for failing to comply with the data protection principles under the Data Protection Act 1998 when processing personal data and for failing to take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data.

On 11 April 2018, the UK government passed the UK Data Protection (Charges and Information) Regulations 2018, which require controllers to pay a fee to the ICO, subject to tiered criteria. Importantly, the ICO, in November 2018, started issuing fines against organisations in the finance, business, construction, health, childcare and manufacturing sectors for failing to pay the fee.

1.5 Significant Pending Changes, Hot Topics and Issues

The ICO, in its draft regulatory action policy, has set out the practical and policy approach the ICO is going to take towards discharging its role as the UK's data supervisory authority. In the draft policy, the Information Commissioner states the approach her office adopts is "always try to select the most suitable regulatory tool by assessing the nature and seriousness of a failure, the sensitivity of the subject matter, whether and how individuals are affected, the novelty and duration of the concerns, the public interest, and whether other regulatory authorities are already taking action on the matter." The draft policy is currently subject to consultation with the UK parliament and is not expected to be approved before spring 2019.

The ICO recognises that "privacy and innovation go hand in hand" and has established a 'regulatory sandbox' that will enable organisations to beta-test new initiatives, support innovative digital products and services, whilst ensuring the appropriate safeguards continue to remain in place. The ICO intends to open applications in April 2019.

2. Fundamental Laws

2.1 Omnibus Laws and General Requirements

Data Protection Officers

The appointment of a data protection officer (DPO) in the private sector is required where an organisation's core activities (ie, the primary business activities of an organisation) involve:

- *the regular and systematic monitoring of individuals on a large scale* – for example, where a large retail website uses algorithms to monitor the searches and purchases of its users and, based on this information, offers recommendations to them; or
- *the large-scale processing of special categories of personal data (eg, health data) or personal data relating to criminal convictions and offences* – for example, a health insurance company processes a wide range of personal data about a large number of individuals, including medical conditions and other health information.

The ICO states in its guidance on the appointment of DPOs that, regardless of whether the GDPR requires an organisation to appoint a DPO, the organisation must ensure that it has sufficient staff and resources to discharge its obligations under the GDPR, and that a DPO can be seen to play a key role in an organisation's data protection governance structure and help improve accountability. The guidance further advises that, should an organisation decide that it does not need to appoint a DPO, it is recommended that this decision be recorded in order to help demonstrate compliance with the accountability principle.

The GDPR requires an organisation to publish the contact details of the DPO and to communicate such details to the ICO. To notify the ICO, organisations should send an email to dataprotectionfee@ico.org.uk, with the subject line 'Add a DPO.' The email should include:

- the organisation's ICO registration number;
- whether the organisation is required to appoint a DPO or whether the organisation has appointed one voluntarily; and
- the name, address, phone number and/or email address of the DPO (if they are an individual, ie, a member of staff) or the external organisation that will be carrying out DPO duties on the organisation's behalf. Organisations must clearly state within the email whether they

wish to publish the name of their DPO if it is an individual.

Application of "Privacy by Design" or "by Default"
Data protection by design and by default requires controllers to put appropriate technical and organisational measures in place to implement the data protection principles and safeguard individual rights. Although not a new concept, it was historically viewed as 'good practice' under the previous Data Protection Act 1998. The GDPR has now made this a legal requirement, essentially requiring controllers to consider data protection and privacy issues at the outset, and by default process the minimum amount of personal data necessary to achieve the specific purpose (ie, data minimisation).

Data Protection by Design
In its guidance on data protection by design and by default, the ICO states that data protection by design is about adopting an organisation-wide approach to data protection, and 'baking in' privacy considerations into any processing activity undertaken. Indeed, in considering whether or not to impose a penalty, the ICO has advised that it will take into account the technical and organisational measures a controller has put in place in respect of data protection by design.

Data Protection by Default
Practically, the ICO recognises in its guidance that controllers will need to process personal data in order to achieve their purposes. However, 'privacy by default' requires the controller to inform individuals appropriately prior to processing and only process the personal data needed for the specified purposes. The ICO acknowledges that what actions are required to be taken will depend on the circumstances of the processing and the risks posed to individuals.

In its guidance, the ICO encourages controllers to develop a set of practical, actionable guidelines that can be used in its organisation, framed by the controller's assessment of the risks posed and the measures available to it. The ICO suggests that these guidelines could be based on the seven foundational principles of privacy by design, as developed by the Information Commissioner of Ontario.

Data Protection Impact Assessments (DPIAs)
Controllers are under an obligation to carry out a DPIA where the processing is likely to result in a high risk to individuals. Processors are required under Article 28 of the GDPR to provide assistance to the controller in carrying out a DPIA. Whilst the GDPR provides three specific examples where a DPIA should be carried out, the ICO in its updated guidance on DPIAs states that it is also good practice to perform a DPIA for any other major project that requires the processing of personal data. The ICO has also published a DPIA screening checklist, which sets out instances where a DPIA should always be carried out (eg, processing special categories of personal data or criminal offence data on a large scale, or processing personal data without providing a privacy notice directly to the individual) and instances where a DPIA should be considered (eg, processing on a large scale, or using innovative technological or organisational solutions). The updated guidance also recommends that, where a controller decides not to carry out a DPIA, the reasons for this decision are documented.

Privacy Policies and Notices
The implementation of internal privacy policies may assist organisations in meeting the principle of accountability as required under Article 5(2) of the GDPR, as well as the requirement under Article 24(2) of the GDPR to implement appropriate data protection policies where this is proportionate in relation to the processing activities.

Individuals have a right to be informed about the collection and use of their personal data. The information to be provided is set out in Articles 13 and 14 of the GDPR. Where personal data is collected directly from the individual, this transparency information must be provided at the time the personal data is collected. Where personal data is collected from another source, the transparency information must be provided within a reasonable period of time, no longer than one month. The ICO has published detailed guidance on the right to be informed, which requires the transparency information to be reviewed regularly and, where necessary, updated.

The DPA 2018 includes a number of exemptions from the requirement to provide information as required under Articles 13 and 14 of the GDPR, in addition to those provided for in the GDPR. These exemptions are set out in Schedule 2 of the DPA 2018 and include:

- *crime and taxation* – where the personal data are processed for the prevention or detection of crime, the apprehension or prosecution of offenders, or the assessment or collection of any tax or duty or any imposition of a similar nature, to the extent the provision of the transparency information would be likely to prejudice any such purposes;
- *disclosures required by law* – where the disclosure is required by law or is necessary for the purpose of or in connection with legal proceedings (including prospective legal proceedings), obtaining legal advice, and establishing, exercising or defending legal rights;
- *legal professional privilege* – where the personal data processed consists of information in respect of which a claim to legal professional privilege could be maintained in legal proceedings;
- *management forecasting and planning* – where the personal data are processed for the purposes of management forecasting or management planning in relation to a business or other activity;

- *negotiations* – where the personal data consists of records of the intentions of the controller in relation to any negotiations with the individual; and
- *confidential references* – where the personal data consists of a reference given or to be given in confidence for the purposes of, for example, employment (or prospective employment) of the individual.

Data Subject Rights
The GDPR affords individuals certain rights under the GDPR, in relation to their personal data, which include:

- the right to be informed (see above);
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- rights in relation to automated decision-making and profiling.

The ICO has published guidance on each of the rights.

Right of Access
Individuals have a right to receive confirmation of whether the controller is processing personal data concerning them, receive a copy of the personal data, and receive certain supplemental information.

Right to Rectification
Individuals have a right to obtain rectification of inaccurate personal data concerning themselves. An individual also has the right to have incomplete personal data completed, including by means of providing a supplementary statement. The DPA 2018 defines 'inaccurate' as "incorrect or misleading as to any manner of fact."

Right of Erasure
Individuals have a right to have their personal data erased without undue delay in certain circumstances (eg, where the personal data is no longer needed for the purpose for which it was collected or processed).

Right of Restriction
Individuals have the right to restrict the processing of their personal data in certain circumstances (eg, where the business no longer needs the personal data for the purposes of the processing but the individual requires it for the establishment, exercise or defence of legal claims).

Right to Data Portability
Where an individual has provided their personal data to the controller, the right to data portability allows an individual to receive that personal data in a structured, commonly used and machine readable format, and to cause the controller to transmit that data to another controller, when the controller is processing the personal data based on either consent or the legal ground of where the processing is necessary for the performance of a contract with the individual, and the processing is carried out by automated means (ie, performed by a computer).

Right to Object
Individuals have the right to object to:

- processing where the controller's legal basis for the processing of the personal data is not in the public interest, or not in the legitimate interest of the controller;
- processing for direct marketing purposes; and
- processing for scientific or historical research purposes or statistical purposes.

Exemptions
Although the DPA 2018 does not afford individuals additional rights over and above those in the GDPR, it does include a number of exemptions that disapply the data subject rights above, in certain circumstances. These include, for example:

- *crime and taxation* – where the personal data is processed for the prevention or detection of crime, the apprehension or prosecution of offenders, or the assessment or collection of any tax or duty or any imposition of a similar nature, to the extent the provision of the transparency information would be likely to prejudice any such purposes; and
- *disclosures required by law* – where the disclosure is required by law or is necessary for the purpose of or in connection with legal proceedings (including prospective legal proceedings), obtaining legal advice, and establishing, exercising or defending legal rights.

The DPA 2018 includes a further exemption from the requirement to comply with a subject access request (ie, Article 15 of the GDPR) where doing so would involve disclosing information relating to another individual who can be identified from that information. However, this exemption does not apply where the other party has consented to the disclosure, or if it is reasonable to disclose the personal data without the consent, having regard to all the relevant circumstances.

A controller is also exempt from requirements to comply with a subject access request in, for example:

- *legal professional privilege* – where the personal data processed consists of information in respect of which a claim to legal professional privilege could be maintained in legal proceedings;
- *management forecasting and planning* – where the personal data is processed for the purposes of management

forecasting or management planning in relation to a business or other activity;
- *negotiations* – where the personal data consists of records of the intentions of the controller in relation to any negotiations with the individual; and
- *confidential references* – where the personal data consists of a reference given or to be given in confidence for the purposes of, for example, employment (or prospective employment) of the individual.

The DPA 2018 makes it a criminal offence – in certain circumstances and in relation to certain information – to require an individual to make a subject access request.

The GDPR requires a controller to respond to a request without undue delay, and within one month. This time-period can be extended by a further two months if the request is complex or if the controller has received a number of requests from the individual. However, guidance published by the ICO states that, in its view, it is unlikely to be reasonable to extend the time-limit if the request is manifestly unfounded or excessive, if an exemption applies, or if the controller is requesting proof of ID.

Anonymisation, De-Identification, Pseudonymisation
The DPA 2018 does not apply to anonymous data (ie, information that does not relate to an identified or identifiable individual). When assessing whether an individual is identifiable, guidance published by the ICO states that the information processed together with all the means reasonably likely to be used by either the controller or any other person to identify that individual should be considered. The ICO also acknowledges that it is possible that the same information is personal data for one controller's purposes but is not personal data for the purposes of another controller.

The DPA 2018 does apply to pseudonymised data (ie, where the separation of personal data from direct identifiers has occurred so that the linkage of the identity is not possible without the use of additional information). The ICO acknowledges that pseudonymised data can help reduce privacy risks by making it more difficult to identify individuals.

2.2 Sectoral Issues

The GDPR distinguishes between personal data and a narrower special category of personal data (or sensitive data). Special categories of personal data include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning an individual's sex life or sexual orientation.

In order to process special categories of personal data lawfully, controllers must identify a legal ground under Article 6 of the GDPR and a condition under Article 9 of the GDPR. The DPA 2018 includes certain conditions in relation to employment, health and research, which are:

- employment, social security and social protection;
- health or social care purposes;
- public health; and
- research, etc.

Part 2 of Schedule 1 of the DPA 2018 includes 23 conditions in relation to processing that are necessary for reasons of substantial public interest, including inter alia:

- equality of opportunity or treatment;
- racial and ethnic diversity at senior levels of the organisation;
- regulatory requirements relating to unlawful acts and dishonesty, etc;
- preventing fraud;
- insurance; and
- occupational pensions.

Criminal records and offences data is not included within the scope of special categories of personal data. The DPA 2018 states that references in the GDPR to criminal records and offences data include personal data relating to the alleged commission of offences by the individual, or proceedings for an offence committed or alleged to have been committed by the individual.

In order to process criminal records and offences data lawfully, controllers must identify a legal ground under Article 6 of the GDPR, and carry out the processing under the control of the official authority or have legal authority for the processing under Article 10 of the GDPR. Where the processing of criminal records and offences data is not carried out under the control of the official authority, such processing is authorised by UK law for the purposes of Article 10 only if the processing meets a condition in Part 1, 2 or 3 of Schedule 1 of the DPA 2018.

Part 3 of Schedule 1 of the DPA 2018 sets out a number of conditions for the processing of criminal records and offences data, including, inter alia, those that relate to:

- consent;
- protecting an individual's vital interests;
- processing by not-for-profit bodies;
- personal data in the public domain;
- legal claims;
- judicial acts;
- administration of accounts used in the commission of indecency offences involving children; and
- extension of the insurance conditions in Part 2 of Schedule 1.

Part 3 also permits a controller to rely on a Part 2 condition, and the requirement that the processing be in the substantial public interest can be disapplied.

Where processing sensitive data in reliance on a condition under the DPA 2018, the controller will need to have an 'appropriate policy document' in place that explains the controller's procedures for securing compliance with the principles in Article 5 of the GDPR, and explains the controller's policies as regards the retention and erasure of personal data processed in reliance on the DPA 2018 condition.

Health Data

Data concerning health falls within the scope of sensitive data under Article 9 of the GDPR. The GDPR defines 'data concerning health' as "personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status."

Article 9(2)(j) of the GDPR sets out the legal ground where the processing is necessary for scientific research purposes. To rely on this legal ground, the processing must comply with Article 89(1) of the GDPR, which requires the processing be subject to appropriate safeguards, in particular to comply with the principle of data minimisation. The DPA 2018 states that the processing will not meet these requirements where it is likely to cause substantial damage or distress to an individual, or where the processing is carried out to support measures or decisions relating to a particular individual, unless this includes the purposes of approved medical research.

The DPA 2018 includes exemptions from data subject rights for data concerning health where:

- it is processed by a court, supplied in a report or other evidence given to a court, and under specified rules (ie, those relating to family and children's hearings in the courts) may be withheld from an individual; or
- the request is made by someone with parental responsibility for a person under the age of 18 (or 16 in Scotland) and the data subject has an expectation that the information would not be disclosed to the requestor or has expressly indicated that it should not be disclosed.

The DPA 2018 also includes an exemption from the subject access right to health data where the disclosure would likely cause serious harm to the physical or mental health of the individual or another person.

Children's Privacy

The DPA 2018 states that where a controller is relying on consent as the legal ground for processing personal data when offering an information society service directly to a child, only children aged 13 years or over are able to provide their own consent. Where a child is under 13 years, the processing will only be lawful where consent is given or authorised by a parent or guardian, unless the information society service is an online preventive or counselling service.

The DPA 2018 requires the ICO to prepare an age-appropriate design code for information society services that are likely to be accessed by children. The ICO has also published detailed guidance on children and the GDPR, which includes guidance on direct marketing to children, the profiling of children and the sharing of children's data.

2.3 Online Marketing

The DPA 2018 defines direct marketing as the communication (by whatever means) of advertising or marketing material directed to particular individuals. Where direct marketing involves the processing of personal data – for example, where the organisation knows the name of the individual it is contacting – the sender must comply with the GDPR and the DPA 2018 in its treatment of that personal data.

Individuals are given a right to object to their personal data being processed for direct marketing purposes. This is an absolute right and an individual can request an organisation to stop processing their personal data at any time. In its guidance on direct marketing, updated in March 2018 in the context of the GDPR, the ICO recommends that it is good practice to acknowledge the request and confirm that the marketing will stop. The ICO guidance expects that any communications should stop within 28 days of receiving the objection (and providing two months for postal communications). However, if an organisation can reasonably stop direct marketing communications sooner, then it should do so.

The ICO has also created a direct marketing checklist that enables organisations to check if their marketing messages comply with the law, and is currently developing a Direct Marketing Code of Practice as mandated by the DPA 2018, which will replace and update the current guidance.

In addition to compliance with the GDPR and the DPA 2018, organisations that conduct electronic direct marketing will also need to comply with the PECR. Although the PECR has not yet been updated following the coming into force of the GDPR, organisations will still be required, for example, to use the new standard of GDPR consent when complying with the PECR. Under the GDPR, consent must be freely given, specific, informed and an unambiguous indication of the individual's wishes, in order to be valid.

2.4 Workplace Privacy

Special Categories of Personal Data

The processing of special categories of personal data for employment law purposes is permitted under the DPA 2018

where the controller meets the condition as set out in Part 1 of Schedule 1 of the DPA 2018, which requires that:

- the processing is necessary for the purposes of performing or exercising obligations or rights that are imposed or conferred by law on the employer or employee in connection with employment, social security or social protection;
- the employer has an 'appropriate policy document' in place when the processing is carried out; and
- the additional safeguards as set out in Part 4 of Schedule 1 of the DPA 2018 are complied with – ie, the data processing record (as required under Article 30 of the GDPR) includes reference to the DPA 2018 condition relied upon, the Article 6 legal ground relied upon, and whether the personal data is retained and erased in accordance with the employer's policies and, if not, the reason for not following the policies.

Employee Monitoring

The DPA 2018 does not specifically address employee monitoring. However, the ICO's guidance on DPIAs states that a controller should carefully consider carrying out a DPIA for processing that involves monitoring of vulnerable individuals (ie, employee monitoring).

The ICO has also published its Employment Practices Code and Supplementary Guidance (the 'Code'), which addresses monitoring at work and covers employers' monitoring of employees' use of telephones, internet, email systems and vehicles. However, the Code was prepared under the previous Data Protection Act 1998 and has not yet been updated to reflect the position under the GDPR and DPA 2018.

Whistle-blower Hotlines and Anonymous Reporting

The DPA 2018 does not specifically address the use of whistle-blowing hotlines (ie, where employees and other individuals can report misconduct or wrongdoing via a hotline), nor does it offer specific legislative protection for whistle-blowing. However, controllers using whistle-blower hotlines in the UK will need to comply with the data protection principles under the GDPR and the DPA 2018.

The ICO has not published any general guidance on the use of whistle-blowing hotlines but has published guidance on protection for whistle-blowers who disclose information to the ICO about concerns that their employer may be contravening requirements of legislation relating to data protection and freedom of information.

Anonymous reporting is not strictly prohibited in the UK and there is no specific obligation under the DPA 2018 to keep the identity of the accused confidential.

2.5 Enforcement and Litigation

As referred to above, the DPA 2018 provides the ICO with various enforcement powers, including the ability to issue, in sequence, information notices, assessment notices, a notice of intent, enforcement notices and penalty notices to controllers or processors that it considers to have breached the data protection legislation.

As under the GDPR, the DPA 2018 provides two levels of financial penalties. The higher maximum amount is EUR20 million or 4% of the undertaking's total annual worldwide turnover in the preceding financial year, whichever is higher, and the standard maximum amount is EUR10 million or 2% of the undertaking's total annual worldwide turnover in the preceding financial year, whichever is higher. The level of penalty imposed will depend on the context of the breach, and the DPA 2018 provides a number of factors that must be taken into account by the ICO when determining the penalty level within the two bands.

The ICO is required to produce guidance on its enforcement powers under the DPA 2018.

The GDPR and the DPA 2018 also provide individuals with the right to lodge a complaint with the ICO if they consider that there has been an infringement of the GDPR, in connection with personal data relating to them.

Where the ICO receives a complaint, the DPA 2018 requires that the ICO:

- takes appropriate steps to respond to the complaint;
- informs the complainant of the outcome of the complaint;
- informs the complainant of the rights under section 166 of the DPA 2018 (ie, where the ICO fails to take appropriate steps to respond to the complainant, inter alia, the complainant may progress the complaint further to a tribunal); and
- provides the complainant with further information about how to pursue the complaint, if asked to do so by the complainant.

3. Law Enforcement and National Security Access and Surveillance

3.1 Laws and Standards for Access to Data for Serious Crimes

A number of laws relating to law enforcement access to data are applicable in the UK, but the following focuses on the application of the Law Enforcement Directive 2016/80.

Law Enforcement Directive and DPA 2018: Key Principles

The transposition of the Law Enforcement Directive into UK law, via the DPA 2018, introduced further requirements to comply with the data protection principles when processing personal data for law enforcement purposes.

Under the DPA 2018, processing for law enforcement purposes in the UK is only lawful if it is based on law and if either the data subject has given consent to the processing of his or her personal data for that purpose or if the processing of the personal data is necessary for the performance of a task carried out for law enforcement purposes by a competent authority. This includes the UK government, a UK police authority, the UK's revenue and customs, the director general of the national crime agency, the director of the serious fraud office, the financial conduct authority, a court or tribunal, or the ICO.

Additionally, the DPA 2018 requires controllers to comply with the principle of collecting personal data for specified, explicit and legitimate purposes when processing personal data for law enforcement purposes.

In accordance with the accuracy data protection principle, where personal data is being processed for law enforcement purposes in the UK, the controller must take every reasonable step to ensure that inaccurate personal data is erased or rectified without delay, having regard to the law enforcement purposes for which it is processed. When processing personal data for UK law enforcement purposes, controllers must also ensure:

- that personal data based on facts must, so far as possible, be distinguished from personal data based on personal assessments; and
- that there is a clear distinction, where relevant and as far as possible, between personal data relating to different categories of data subject, such as:
- persons suspected of having committed, or about to commit, a criminal offence;
- persons convicted of a criminal offence;
- persons who are or may be victims of a criminal offence; and
- witnesses or other persons with information about offences.

Moreover, controllers must ensure that all reasonable steps are taken to ensure that personal data that is inaccurate, incomplete or no longer kept up to date is not transmitted or made available for any law enforcement purposes.

The DPA 2018 also imposes a requirement for appropriate time-limits to be established for the periodic review of the need for the continued storage of personal data for law enforcement purposes.

Law Enforcement Directive and DPA 2018: transfers of data outside of the EEA

The DPA 2018 also introduces further derogations for the transfer of personal data from the UK to a country outside of the EEA, where the transfer:

- is necessary for law enforcement purposes; and
- is based on an adequacy decision; or
- if not based on an adequacy decision, is based on appropriate safeguards where a legal instrument containing appropriate safeguards for the protection of personal data binds the intended recipient of the personal data, or the data controller – having assessed all the circumstances surrounding the transfers of that type of personal data to that specific country or territory outside of the EEA – concludes that appropriate safeguards exist to protect the personal data. When relying on this particular derogation, the transfer must also be documented, and such documents must be provided to the ICO upon request, including the date and time of the transfer, the name or any other pertinent information about the recipient, the justification for the transfer of the personal data, and a description of the personal data transferred; or
- if not based on an adequacy decision or on there being appropriate safeguards, is based on special circumstances that allow for the transfer of personal data from the UK to a country or territory outside of the EEA, where the transfer is necessary:

  (a) to protect the vital interests of the data subject or another person;
  (b) to safeguard the legitimate interests of the data subject;
  (c) for protection against an immediate and serious threat to the public security of a member state or a third country (non-EEA member state);
  (d) in individual cases for any law enforcement purposes (provided that the controller has not determined that fundamental rights and freedoms of the data subject override the public interest in the transfer of personal data from the UK to a third country); or
  (e) in individual cases for a legal purpose (provided the controller has not determined that fundamental rights and freedoms of the data subject override the public interest in the transfer of personal data from the UK to a third country). When relying on this particular derogation, the transfer must also be documented, and such documents must be provided to the ICO upon request, including the date and time of the transfer, the name or any other pertinent information about the recipient, the justification for the transfer of the personal data, and a description of the personal data transferred.

4. International Considerations

4.1 Restrictions on International Data Issues

The GDPR prohibits the transfer of personal data outside of the EEA to third countries, unless:

- the recipient country is considered to offer an adequate level of data protection (such as Israel, Japan and New Zealand);
- a data protection safeguard has been applied (such as the EU's standard contractual clauses for transfers of personal data from the EU – also known as 'model contracts' – or the organisation has implemented binding corporate rules); or
- a derogation from the prohibition applies (such as the data subject having explicitly consented to the transfer).

Such safeguards and derogations are not considered in detail here, but a salient point from a UK perspective is that under the Data Protection Act 1998, controllers were allowed to determine for themselves that their transfers of personal data outside of the EEA were adequately protected. The DPA 2018 does not contain such a provision. However, the GDPR contains a more limited version of the Data Protection Act 1998 self-determination provision, and allows transfers:

- that are not repetitive, concern only a limited number of data subjects and are necessary for the purposes of compelling legitimate interests that are not overridden by the interests or rights and freedoms of the data subject; and
- where the controller has assessed all the circumstances surrounding the data transfer and has, as a result, implemented suitable data protection safeguards; and
- where the controller has notified the relevant data protection authority of the transfer.

The DPA 2018 also introduces a derogation where the transfer is a necessary and proportionate measure for the purposes of the controller's statutory function.

In addition, see **1.3 Multilateral and Subnational Issues** regarding the UK's proposals in relation to data transfers following Brexit.

4.2 Limitations and Considerations

In general, controllers may provide personal data in relation to non-EEA civil discovery requests, if:

- it is permitted under Article 48 of the GDPR;
- a data protection safeguard set out in Article 46 has been applied (such as model contracts or binding corporate rules); or
- a derogation from the prohibition set out in Article 49 applies.

Article 48 of the GDPR

Article 48 allows the transfer of personal data from the EU to a third country on the basis of a judgment of a court or tribunal or any decision of an administrative authority of the third country, where the transfer is based on (for example) a mutual legal assistance treaty (MLAT) between the requesting third country and the EU member state concerned. Importantly, Article 48 acknowledges that a transfer is also permissible if a safeguard or a derogation applies. As MLATs between EU Member States and third countries are not widespread, controllers can rely on the exemptions referred to above or the specific derogations below, as Article 48's applicability is without prejudice to other grounds of transfer.

Interestingly, the UK has sought an opt-out from the restrictions contained in Article 48 – that is, the UK does not want to be restricted in terms of foreign law data access rights by the restrictions contained in Article 48. In particular, the UK has sought to rely on Article 3 of Protocol 21 to the Treaty on the Functioning of the European Union to attempt to secure this opt-out. However, it is not clear whether the UK has successfully opted out of this protocol. In addition, it is not clear how this opt-out would work in practice; for example, could an organisation in Germany circumvent the requirements in Article 48 by first transferring the data to the UK before transferring it outside the EEA? In any event, as noted above, Article 48 itself acknowledges that transfers (that do not satisfy the requirements of Article 48) may nonetheless occur if another legal safeguard or derogation set out in the GDPR applies.

Data Protection Safeguards

The most commonly used safeguard is the European Commission-approved model contracts for data transfers, as these may be entered into with (for example) e-discovery vendors and document review-providers.

The most relevant derogations are that the transfer is:

- necessary for important reasons of public interest – for example, the transfer is needed to prevent money laundering or for purposes of public health;
- necessary for the establishment, exercise or defence of legal claims – this may be useful in civil proceedings (and even potentially in pre-trial discovery, though this is not clearly available if the discovery has not been ordered by a court);
- non-repetitive and relates only to a limited number of data subjects (see **4.1 Restrictions on International Data Issues**); or
- explicitly consented to by the relevant data subject – however, in practice, it may be challenging to obtain such consent in relation to foreign data access requests.

5. Emerging Digital and Technology Issues

5.1 Addressing Current Issues in Law

Big Data analytics

The ICO issued guidance regarding Big Data in July 2014, and revised this in 2017. This guidance covers a broad range of topics including anonymisation, privacy impact assessments, repurposing data, data minimisation, transparency and subject access.

Key points raised in the ICO's guidance include:

- the ICO recommends performing DPIAs. If particular issues are identified through such an assessment, the controller would then be able to identify and implement measures to address such issues and protect individuals' privacy;
- the ICO identified quality and reliability of data as a potential issue for Big Data analytics. These issues arise in particular because the frequency of data processing increases the risk of inaccuracies where the data has been partially de-identified or anonymised and cannot be easily reconnected with the original data subject. As a result of such inaccuracies, data subjects may be subjected to inaccurate profiling, discrimination, or other forms of prejudice;
- the ICO recommends conducting a compatibility analysis in order to determine whether the purpose limitation principle has been satisfied. In particular, the purpose limitation principle may be a barrier to the development of Big Data analytics, as many secondary uses may not have been considered when the data was first collected. Controllers may also wish to consider whether the 'research' exemption is also available;
- the ICO has identified the data minimisation principle as another key concern for Big Data analytics. It recommends that organisations identify at the outset why they need the particular data and what they expect to learn from its analysis, which, in turn, will limit the volume of personal data that is collected and processed. Similarly, with respect to data retention, controllers should justify why particular data should be retained, or alternatively seek to anonymise data that they retain; and
- the ICO acknowledges the potentially higher data security risks arising from Big Data, and suggests that appropriate data security measures be implemented.

6. Cybersecurity and Data Breaches

6.1 Key Laws and Regulators

The key data security obligations under UK law are provided in:

- the Communications Act 2003;
- the Computer Misuse Act 1990;
- the GDPR and DPA 2018;
- the Network and Information Systems Regulations 2018 (NIS Regulations);
- the Official Secrets Act 1989; and
- the Privacy and Electronic Communications (EC Directive) Regulations 2013.

Only the NIS Regulations are considered here, as they represent the most significant recent change in UK data security laws (outside of the GDPR and the DPA 2018).

NIS Regulations

Organisations Subject to the NIS Regulations

The UK government implemented the Network and Information Systems Directive (NIS Directive) into national law in the form of the NIS Regulations, which came into force on 10 May 2018. The NIS Regulations (like the NIS Directive) impose security incident obligations on operators of essential services (OESs) – ie, energy, transport, digital infrastructure, the health sector and drinking water supply and distribution services. While the UK was permitted (under the NIS Directive) to designate organisations as OESs within the banking and financial markets infrastructure sectors, the UK elected (in the NIS Regulations) not to do so. In order to be considered an OES, the organisation must provide an essential service of the kind identified in Schedule 2 of the NIS Regulation, and that service must rely on network and information systems, and meet specific threshold requirements.

The NIS Regulations also impose security obligations on relevant digital service providers (DSPs) – ie, online marketplace providers, online search engines and cloud computing service providers. An organisation may be a DSP if:

- it provides a digital service in the UK;
- it is not a small or micro business; and
- its head office is in the UK or the organisation has nominated a representative who is established in the UK.

Key Features of the NIS Regulations

The NIS Regulations:

- require the UK Government to publish strategic objectives and priorities on the security of the network and information systems in the UK;
- designate the UK's Government Communications Headquarters (GCHQ) as the Computer Security Incident Response Team (CSIRT) for certain relevant sectors and digital sectors. The CSIRT is required to provide incident support and assistance to OESs and DSPs;
- designate the GCHQ as a single point of contact (SPOC) intended to act as a liaison and to facilitate cross-border co-operation, including with the European Network and Information Systems Agency (ENISA); and

- designate one or more national competent authorities ('CAs'). The UK has determined that it wishes to designate CAs for particular sectors (rather than one single CA across sectors). CAs have a key role under the NIS Regulations, including:

  (a) preparing and publishing guidance for OESs and DSPs;
  (b) receiving incident reports;
  (c) conducting incident investigations; and
  (d) enforcing the NIS Regulations.

The NIS Regulations also impose a tiered system of fines in proportion to the impact of the security incident, with a maximum fine of GBP17 million, imposed where a competent authority decides the incident has caused or could cause an immediate threat to life or a significantly adverse impact on the UK economy. CAs are also vested with a number of enforcement-related powers under the NIS Regulation.

Security Obligations
In general, OESs and DSPs must take appropriate and proportionate technical and organisational measures to:

- manage the risks posed to the security of relevant network and information systems; and
- prevent and minimise the impact of incidents affecting the security of relevant network and information systems.

6.2 Data Breach Reporting and Notification

Data-breach notification obligations under the GDPR, the DPA 2018 and the NIS Regulations are considered below; there may be additional sector-specific data-breach notification obligations such as for organisations that are regulated by the UK Financial Conduct Authority (FCA).

GDPR and DPA
Controllers have an obligation to report personal data breaches to the ICO within 72 hours of the breach, unless the breach is unlikely to result in a risk to the rights and freedoms of the data subject. Controllers are also required to inform the data subject where such breach is likely to result in a high risk to their rights and freedoms.

Sidley Austin LLP

Woolgate Exchange
25 Basinghall Street
London
EC2V 5HA

Tel: +44 20 7360 2061
Email: wlong@sidley.com
Web: www.sidley.com

When a personal data breach is reported to the ICO, the GDPR requires to be provided:

- a description of the nature of the personal data breach, including, where possible:
- the categories and approximate number of data subjects concerned; and
- the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including where appropriate, the measures taken to mitigate any possible adverse effects.

Where controllers do not have all of the required information, the ICO requires them to notify the breach as soon as they become aware of it, and to note that submission of further information will follow as soon as possible. If full details cannot be provided within 72 hours, any such delay should be communicated to the ICO and when that further information will be expected.

The ICO provides an online personal data-breach reporting form for any personal data breach to be notified to the ICO online and has also published guidance on reporting a personal data breach.

NIS Regulation
An OES must notify its designated CA about any incident that has a significant impact on the continuity of the essential service provided by the OES. The NIS Regulations set thresholds in relation to determining whether notice must be provided by OESs. If such a notice must be given, it should be given 'without undue delay' and in any event within 72 hours.

A DSP must notify the ICO (its CA) about any security incident that has a substantial impact on the provision of specified digital services. The NIS Regulations set out thresholds in relation to determining whether notice must be provided by DSPs. If such a notice must be given, it should be given 'without undue delay' and in any event within 72 hours.

In certain circumstances, the relevant CA is required to share information regarding the incident with the CSIRT. The CA may also notify the public itself, or direct the relevant OES or DSP to do so.