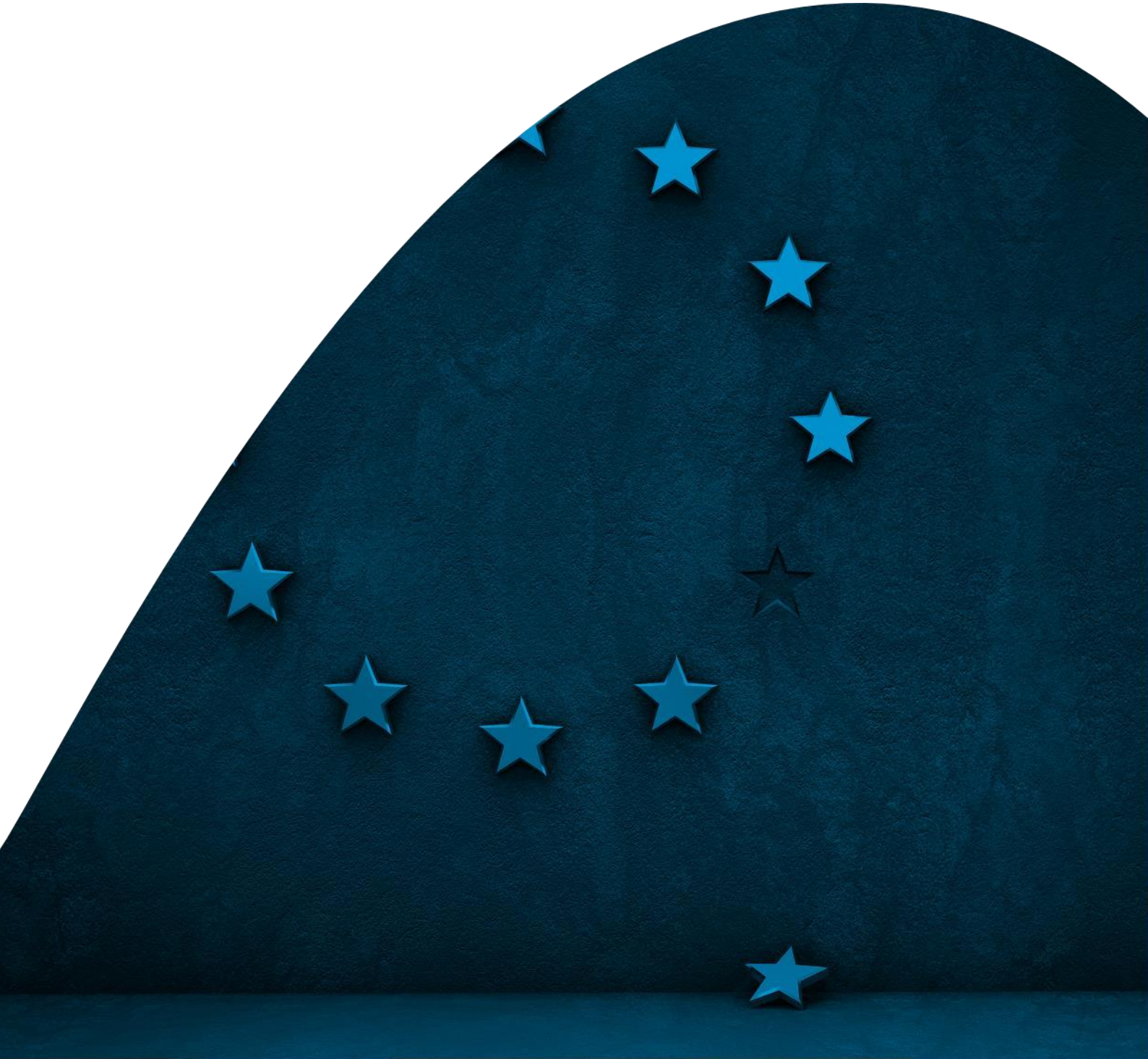
FT INNOVATIVE LAWYERS 2015
FINANCIAL TIMES
AWARD WINNER
The Most Innovative Law Firm in Europe

Pinsent Masons

Guide to the EU General Data Protection Regulation, post Brexit



Contents

This Guide contains information on the following areas:

1. Introduction

The General Data Protection Regulation (Regulation) is a data protection law which applies directly across the European Union (EU) as from **25 May 2018**. The Regulation establishes a modified framework of legal rights and duties designed to safeguard personal data and destined to replace the current EU Data Protection Directive and national implementing legislation under the Directive, with a view to modernisation and cross-EU harmonisation. A separate Directive deals with the processing of personal data for law enforcement and related purposes.

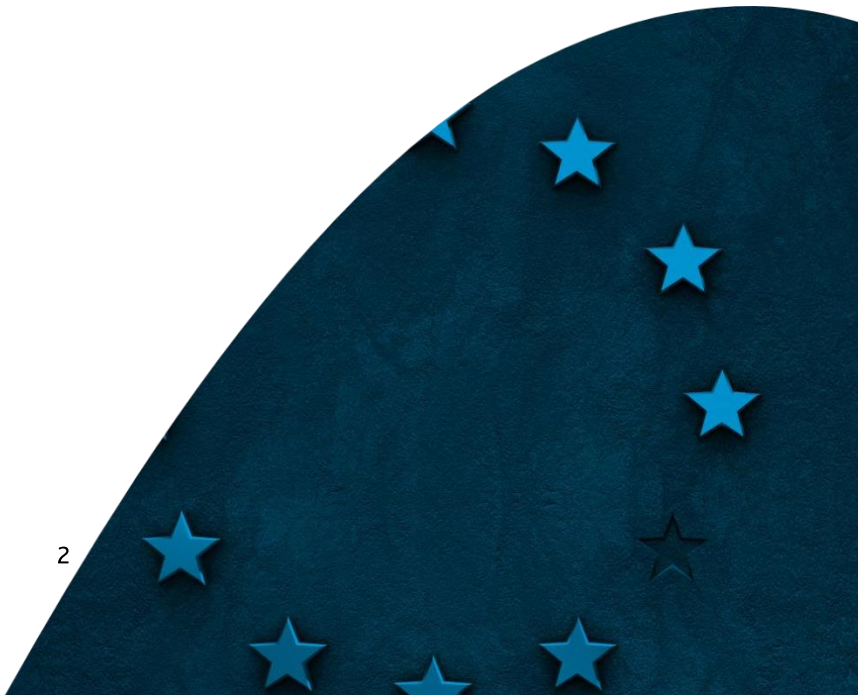
Brexit

Following the June 2016 UK referendum vote in favour of "Brexit", an issue at the forefront of many organisations' minds is: to what extent should they be concerned with complying with the Regulation?

While it is impossible to predict the final position at the time of publication (July 2016) given the political uncertainty, the most likely scenario is that the UK leaves the EU after 25 May 2018 and that, therefore, the Regulation will take effect before any Brexit occurs. It is possible however that after the UK's article 50 notification is made, the European Communities Act 1972 is repealed before 25 May 2018, in which event the position would be as follows:

- UK-based organisations that offer goods or services to EU-resident individuals or monitor their behaviour, or whose personal data processing activities are related to such offering/monitoring, will in any event be directly subject to the Regulation regardless of whether the Regulation is in force in the UK.

- UK-based data controllers would continue to be subject to the Data Protection Act 1998 until repealed and (presumably) replaced by a new, UK data protection law.



The Regulation

As UK organisations that offer goods or services to EU-resident individuals, or whose processing activities are related to such offering, will in any event be directly subject to the Regulation and will have to comply with it, we are producing this revised Guide to the Regulation for clients.

For those familiar with the Data Protection Act 1998 (the **Act**), there is a lot within the Regulation which will look familiar. The **broad structure** and data protection language are similar. However, many of the **definitions have been expanded**, for example the definition of personal data. There are also some **changes**, such as to territorial scope, and **important additional provisions** such as on direct obligations of data processors and the level of fines and compensation. **Other changes** include the introduction of a requirement in certain circumstances for data protection officers, profiling, data protection impact assessments and a data portability right.

The Regulation is made up of Articles containing the substantive obligations, and Recitals which influence the interpretation of the substantive provisions.

Note: The Regulation was formally adopted on 14 April 2016. It will enter force on 25 May 2018 and its provisions will be directly applicable then in all EU Member States. This Guide has been developed from the standpoint of compliance with the Regulation and NOT the Act, which remains in effect until 25 May 2018.

Note: Whilst this Guide considers the Regulation, the wording used is not always an exact copy of provisions from the Regulation and this should be borne in mind when using the Guide.

Note: This Guide relates to the United Kingdom only and therefore reference is made to the UK's supervisory authority, the Information Commissioner, throughout.

Note: This is a summary note only and does not constitute legal advice. Specific legal advice should be taken before acting on or refraining from acting on any of the issues covered in this Guide.

2. Key changes

Summary of key changes

- General focus on **accountability** measures – the Regulation requires not only compliance with its rules, but being able to *evidence* compliance, e.g. documented policies and procedures, records of consents etc. Registration with supervisory authorities such as the Information Commissioner will no longer be required but there will be internal **record-keeping obligations**, with the **supervisory authorities having expanded powers** e.g. to demand information, conduct audits, order remediation etc.
- **Territorial scope** (Article 3), extending to non-EU controllers and processors in some situations. There will also be a "one stop shop" so that organisations operating in multiple EU Member States may report to only one main supervisory authority, with a consistency mechanism to promote harmonisation across EU Member States and resolve cross-border issues.
- **Definitions** have been substantially **amended** (Article 4), for example, expanded definitions of "personal data" and "data subject" (catching more types of data and processing operations), and some **new definitions** have been added, for example on "pseudonymisation" and "profiling". **Consent will be more difficult** to use as a legal basis.
- **Direct statutory obligations** (Articles 28, 30, 44-49, 33(2)) and **liability** (Article 82) on **processors**, and additional requirements regarding the minimum terms that must be included in **personal data processing contracts** (Article 28).
- Generally **tighter rules on international transfers**, applicable to both controllers and processors.
- A requirement to carry out **data protection impact assessments** before initiating certain types of processing or other processing operations that are likely to result in a high risk to individuals, which must consider at least the issues specified by the Regulation (Article 35), and to **consult with the supervisory authority** in some circumstances (Article 36).
- A requirement on controllers and processors to appoint a **data protection officer** in certain circumstances (Articles 37-39).
- The introduction of mechanisms for the purposes of demonstrating compliance with the Regulation, involving **codes of conduct** (Articles 40-41) or **certifications** (Articles 42-43) approved under the Regulation for these purposes.
- Generally, information provided in response to a **subject access request** will have to be provided within a **tighter timescale** and free of charge (Article 12).
- **New data subject rights** – the "right to be forgotten" or right to erasure (Article 17), building on current rights confirmed in the *Costeja* case and "data portability" (Article 20).
- **Security breach notification** – mandatory **"personal data breach" notifications** to the supervisory authority without undue delay (within **72 hours** where feasible) (Article 33), and **personal data breach notifications to the data subject** without undue delay where there is a high risk to their privacy (Article 34).
- The introduction of the **Board** (Section 3 - Articles 68-76) to replace the Article 29 Working Party, with an enhanced role and powers.
- Harsher **sanctions** and a new framework for fines (in two tiers), which will be substantially higher than under the Act (Article 83). Under the Act, the maximum fine is £500,000, but under the Regulation, there will be two tiers of administrative fines which could be levied by supervisory authorities: up to 20 million EUR or 4% of total worldwide turnover if higher, and up to 10 million EUR or 2% of total worldwide turnover if higher.

For further detail on these key changes, please refer to the table at **Appendix 1**.

3. What the regulation means for you

There are a number of considerations for you in the wake of the Regulation, as the landscape of data protection will change substantially. Whilst it will not be in force until 25 May 2018, there is much to do to prepare in time, and organisations should be reviewing their practices and policies against the new requirements so that they will be ready in time. Clients should be looking at the following:

- consider **whether this Regulation will apply to you regardless of the result of any Brexit,** e.g. if you are providing good or services to data subjects in the EU or monitoring EU residents, then the Regulation will continue to be relevant after the UK leaves the EU;
- if the Regulation will apply to you, establish a **task force** to work on its implementation within your organisation, including developing resources to **train staff and raise their awareness** of the Regulation;
- consider whether a **data protection officer** will be required under the new rules and start the process of appointing one if necessary;
- **conduct an audit of your personal data processing operations**: what categories of personal data are being processed, for what purpose, how, and where, and to whom are personal data being disclosed, including whether any profiling is being conducted; and **develop a plan** to ensure relevant group entities will comply with their obligations under the Regulation. Develop **procedures** to record and maintain **evidence of compliance** on an on-going basis, including considering and recording for each personal data processing operation what its **legal basis** should be under the Regulation, such as legitimate interests. If relying on **consent** from data subjects, consider whether another basis is possible or else how to ensure that the consent process will be valid under the Regulation (particularly in relation to pre-ticked boxes online).
- **review and update as necessary** internal and customer-facing **data protection policies/fair processing notices** to comply with the new transparency obligations, and also review and update all data protection **practices** within the business, including to take account of new **record-keeping obligations** on controllers and processors;
- develop a template **data protection impact assessment** for use in any future high risk projects and consider carrying out such assessments sooner rather than later where relevant, for example where profiling is used;
- whether your organisation is a controller or processor, start reviewing **data protection clauses used (both for templates and live negotiations)** in **supplier agreements** to ensure they include the mandatory provisions under the Regulation and an appropriate change of law clause, and also **review existing contracts** with either controllers or processors, depending on the nature of the business, in particular to consider whether the contracts include the prescribed provisions under the Regulation and whether they maintain your risk position in light of the change in law; consider **future-proofing deals** being negotiated now by documenting the responsibilities of the parties and specifically taking into account the forthcoming changes;
- if your organisation is a supplier/vendor performing the **data processor role,** review the **scope of obligations** and **liability/indemnity provisions** in your personal data processing contracts, given your new exposure under the Regulation;
- consider if/how data is **transferred internationally**, whether within the same entity, to other group entities or to third parties, and what mechanisms may be used to regularise transfers under the Regulation;

- review existing processes and procedures for dealing with **subject access requests** including the development of template response forms and assessing whether the one-month response deadline can be met; also review IT systems and internal processes to ensure **data portability** (the ability to pass an electronic copy of data to the data subject or another controller), and to enable personal data to be **deleted** easily;
- review **security breach notification and management systems and procedures**, including draft notification forms for notifications to the Information Commissioner and affected individuals (or, where you are a data processor, to controllers). Also consider how to deal with security breach notifications from **third party suppliers/vendors** (if you are a data controller receiving a notification from your data processor);
- review how **children's data** is dealt with by your organisation, where relevant;
- keep a watching brief on areas such as **employee data protection,** where Member States have **national discretion** in relation to the rules, and also on **implementing acts and guidance** to be issued by the Commission and from the Board. This is an area where you should expect to see **UK developments**, as new legislation is developed or existing legislation adopted **post-Brexit**.

4. Key Differences between the Data Protection Act 1998 and the Regulation

This table lists the main topics in alphabetical order, showing the key differences between the Act and the Regulation.

Area	Data Protection Act 1998	General Data Protection Regulation	Why is the change important?
Accountability principle (see also **Certifications, Data protection by design, Data protection impact assessments, Data protection officers**)	The Act has no specific accountability requirement.	The controller is responsible for, and **must be able to demonstrate compliance** with, the fundamental data protection principles (see **Appendix 1**). Associated requirements aimed at evidencing compliance include **Record keeping obligations** (see below), and provisions regarding codes of conduct and certifications. The accountability requirements **replace obligations to register, notify or file** with supervisory authorities.	There will be **stricter rules** requiring controllers to put in place (and implement) policies and **documented procedures** which not only serve to ensure compliance with the Regulation but also to **evidence** that compliance. Full documentation, **records**, logging etc. will be important to help avoid or reduce sanctions, e.g. **proving that proper consents were obtained** where necessary. Adhering to **codes and certifications** approved under the Regulation (see below) will assist to evidence compliance.
Administrative fines	Section 55A – the Information Commissioner has the power to impose a monetary penalty. The fine for breach must not exceed those detailed in regulations made by the Secretary of State. Under The Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010, Regulation 2, the maximum	Article 83 – the Regulation introduces a two tier system of fines, depending on circumstances and which provisions of the Regulation are breached. The maximum amount of fine in the higher tier is **€20,000,000** or (in the case of an undertaking) up to **4%** of the **total worldwide annual turnover** of the preceding financial year, whichever is higher. The maximum amount of fine in the lower tier is **€10,000,000** or (in the case of an undertaking) up to **2%** of the **total worldwide annual turnover** of the preceding financial year, whichever is higher. Both data controllers and data processors may be subject to such	Unsurprisingly, this area has been hotly discussed and is subject to much commentary, with businesses large and small alike worrying about the impact of fines of such potential size. The Regulation has massively increased the **potential administrative fines** which can be imposed for breach of data protection requirements. Article 83 introduces a complex mechanism of sanctions, which are **much higher** than the fines currently available to the Information Commissioner, who until the introduction of the Regulation can fine controllers/processors a maximum of **£500,000 for serious contraventions**

	prescribed fine is £500,000.	sanctions. However, each supervisory authority must ensure that in each case the fine is **effective, proportionate and dissuasive**. Specific **factors** are listed which must be considered in deciding whether to impose a fine and, if so, how much, including the nature, gravity and duration of the infringement, types of personal data and number of data subjects affected and level of damage, intentional or negligent character of the infringement, any action taken to mitigate damage suffered by data subjects, degree of responsibility taking account of security and data protection by design/default measures, degree of cooperation with the supervisory authority, previous infringements or remediation ordered, adherence to approved codes/certifications, and other aggravating or mitigating factors. The Board is empowered to issue **guidelines** to supervisory authorities on their enforcement powers and on the setting of fines (Article 70(1)(k)).	**of the Act**. Organisations should bear in mind the **mitigating factors** to be taken into account should an infringement occur, because matters such as **cooperation** with the supervisory authority, having **documented procedures**, having implemented state of the art **security measures** and data protection by design/default, and/or having adhered to an **approved code/certification**, may help to reduce or even avoid a fine. Equally, organisations should seek to avoid the aggravating factors. Any guidance by the Board on the exercise of supervisory authorities' powers should also be monitored and considered.
Applicability, territorial scope	Section 5 – except as otherwise provided, this Act applies to a data controller in respect of any data only if— (a) the data controller is established in the United Kingdom and the data are processed in the context of that establishment, or (b) the data controller is established neither in the United Kingdom nor in any other EEA State but uses equipment in the United Kingdom for processing the data otherwise than for the purposes of transit through the United Kingdom.	Article 3 – The Regulation applies to the processing of personal data in the **context of the activities of an establishment** of a controller or processor in the EU, regardless of whether or not: (i) the processing takes place in the EU; or (ii) a controller or processor is established in the EU, where the **processing activities are related to**– (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the EU; or (b) the monitoring of their behaviour as far as their behaviour takes place within the EU. A non-EU-established controller or processor who is within scope as above must appoint in writing a **representative** in a relevant EU Member State, with some exceptions. The representative's contact details must be notified to data subjects. Supervisory authorities may liaise with the representative and even enforce against it, but the non-EU controller/processor remains responsible and liable under the Regulation.	The territorial scope has been **amended and largely extended** in comparison to the current legislative framework of the Act. The focus is no longer on the use of equipment located within an EU Member State; instead, the focus is on those who are targeting EU residents. This means that non-EU organisations that were not caught by the Act but which were targeting a UK market or UK individuals, despite lack of presence or use of equipment in the UK, will be caught by the Regulation. In the Brexit scenario, if UK organisations offer goods or services to individuals in the EU or monitor their behaviour in the EU (such as through tracking cookies on their computers), then the Regulation would apply to those organisations and they would have to appoint an EU representative. The Regulation's extraterritorial scope is broad. Non-EU controllers and processors will be caught where the processing activities are "related to" the offering of goods or services to data subjects in the EU, or the monitoring of their behaviour in the EU.

			For example, technically a non-EU web hosting provider would be considered a "processor" bound under the Regulation if its service is used by a non-EU controller to host an e-commerce website selling goods or services to EU individuals.
Automated decision-taking and profiling (See also **Objection**, **Marketing** and **Children**)	Section 12 – A natural person is entitled at any time, by notice in writing to any data controller, to require the data controller to ensure that no decision taken by or on behalf of the data controller which significantly affects that natural person is based solely on the processing by automatic means of personal data.	Article 22 – a similar right applies in the Regulation, i.e. data subjects will continue to have a right not to be subject to a decision based solely on automated processing which produces **legal effects** concerning them or similarly significantly affects them, unless **necessary for a contract** with the data subject and **suitable safeguards** for data subjects are implemented, or authorised by **EU or Member State law**. The Regulation specifically states that such automated processing includes "**profiling**", a new definition of which is introduced (see Definitions). It also adds a new basis for allowing such automated decision-making: **explicit consent**. However, automated decision-making based solely on **sensitive personal data** is prohibited unless **suitable safeguards** are in place, and the controller has obtained the **explicit consent** of the data subject or the processing is necessary for substantial reasons of **public interest** based on appropriate EU/Member State law. Finally, the **existence** of automated decision-making, **meaningful information** on the **logic** involved, its **significance** and **envisaged consequences** for data subjects may have to be **notified** to them for fair and transparent processing, and data subjects are also entitled to **access** such information. The Board may issue guidance on profiling (Recital 72).	The Regulation specifically defines "**profiling**", making it clear that profiling is considered to be a form of automated processing on which decisions affecting data subjects could be based, and to which data subjects could object. Accordingly, use of big data and other forms of **analytics** based on personal data could be considered "profiling", depending on what is analysed and why. Therefore, organisations that conduct automated decision-taking based on profiling, through **big data analytics** or otherwise, will need to ensure such use is compliant with the Regulation, implementing the necessary procedural and other safeguards and reviewing privacy notices' content and mechanisms/timing, including processes for obtaining explicit consent where appropriate. Infringement (such as not implementing suitable safeguards) is subject to a **higher-tier** fine.
Board	The Act imposes obligations on the Information Commissioner. The Data Protection Directive required the establishment of the Article 29 Working Party (comprising the supervisory authority of each Member State and the European Data Protection Supervisor).	The Regulation (Articles 68-76) establishes the **European Data Protection Board (Board)**, which will replace the Article 29 Working Party, and will have **binding powers** in various respects such as approving criteria for certifications (see below).	The Board will provide overall supervision and governance of data protection in the EU and facilitate **cooperation between Member States** and supervisory authorities, particularly in relation to the application of a "consistency mechanism" to promote cross-EU harmonisation of the Regulation's application. After the UK leaves the EU, the Information Commissioner would not be able to participate in the Board without agreement to this effect having

			been reached between the UK and the EU. The UK might have observer status with the Board if the UK joins the European Economic Area (of which Iceland, Liechtenstein and Norway are members although they are not EU Member States), and the EEA Joint Committee decides in relation to the Regulation that EEA members may have such observer status, as is currently the case with EEA members and the Article 29 Working Party under the Data Protection Directive. In any event, the UK would have no voting rights in relation to any Board decisions.
Certifications and codes of conduct	The Act does not include a certification mechanism.	The Regulation encourages the establishment and use of **codes of conduct** (Articles 40-41) and **certifications** (Articles 42-43), in each case as approved under the Regulation for data protection law purposes. The Regulation suggests particular, non-exhaustive, areas suitable to be covered by codes (e.g. fair and lawful processing, collection of personal data, dispute resolution procedures for data subjects). Approved codes/certifications will be publicised. Both controllers and processors may (but are not required by the Regulation to) adhere to an approved code/certification. This would not reduce responsibility for continued compliance and is no defence to infringement, but such adherence would be taken into account by the supervisory authority in deciding whether to impose a fine and if so how much. Although costs are involved, codes/certifications should bring some benefits to controllers and processors too, and not just in relation to possible fines. Adherence will enable competitive differentiation: an organisation which claims to have good data protection compliance can take steps to substantiate that claim. International transfers are also permitted to recipients adhering to an approved code/ certification – see below. Certifications will last for 3 years unless revoked, repealed or suspended sooner by the certification body or supervisory authority for non-compliance. The Regulation includes (differing) procedures for the approval of codes and accreditation of certification bodies that will award certificates under the Regulation. Certification criteria may be issued by the supervisory authority or the Board (in the latter case, resulting in a "European Data Protection Seal"), and the Commission may specify	The Regulation introduces a **new mechanism** for data controllers and data processors to adhere to **approved codes of conduct** or obtain **approved certifications**, as a way of demonstrating compliance with the Regulation's requirements – a visible "seal" for data subjects, to promote trust. Once more details are known regarding which codes or certifications will be approved under the Regulation (and the requirements of such codes or certifications), organisations should consider the costs/benefits of adhering to them (including for their group entities and/or business partners). Industry bodies have an opportunity to draft or put forward industry-standard, sector-appropriate codes or certifications for approval under the Regulation.

		requirements regarding certification mechanisms.	
Children	The Act contains no specific provisions relating to children, although the ICO has issued various publications relating to children e.g. subject access requests for information about children and examples of good/bad practice when collecting information about children.	Article 8 – requires that if "information society services" based on consent are offered directly to a "child" (i.e. under 16, or a lower age between **13 and 16 as the Member State may specify**), then parental consent or authorisation must be obtained and the controller must make reasonable efforts to verify such consent or authorisation in light of available technology. "Information society services" include online services provided at the user's request for remuneration (including services free to the user but where the provider is remunerated e.g. by advertisers). Note that "any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand" (Article 12(1), Recital 58), and the "right to be forgotten" (see Rectification below) is particularly relevant when consent was given as a child (Recital 65). Generally, the Regulation considers that specific protection should apply to the direct collection of children's personal data or the use of such data for marketing or creating profiles, and in applying the "legitimate interests" legal basis for processing (see below). A code of conduct (see Certifications above) is possible in this area.	Data controllers should be aware of the additional obligations imposed around consent when relying on consent to process the personal data of children to whom such services are directly offered. Strictly, these requirements do not apply when not offering such services directly at children, or when using some other legal basis for processing such as legitimate interests, but it is still good practice to take special care when processing the personal data of a child and to seek parental consent in such cases (particularly if the child is under 13).
Consent of the data subject (see **Rectification**)	Schedule 2 paragraph 1 – one of the conditions enabling the requirement of fair and lawful processing in Schedule 1 Part 1 paragraph 1 of the Act to be met is that the data subject has given his consent to the processing. Consent is not defined in the Act but under the Data Protection Directive "the data subject's consent" means "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement	Consent is "any freely given, specific, informed **and unambiguous** indication of the data subject's wishes by which he or she, **either by a statement or by a clear affirmative action**, signifies agreement to the processing of personal data relating to him or her". (Article 4(11)). As now, consent will not be the only legal basis for processing personal data. However, consent may not be considered to be "freely given" if: provision of a service is made **conditional** on consent to the processing of personal data not necessary for the performance of the contract; there is a **"clear imbalance"** between data subject and controller; **separate consent** is not permitted for **different processing operations** where appropriate; or the data subject has no genuine free choice or cannot refuse or **withdraw consent without detriment**. For consent to be "informed", the data subject must be notified at least of the controller's **identity** and **purposes** of intended processing. When relying on consent, consent needs to be obtained for all relevant **processing activities** (for whatever purpose) as well as all **intended**	Much more care will have to be taken if relying on consent as the legal basis for processing, as valid consent will be much more difficult to obtain and prove under the Regulation. Note that infringing the conditions for consent will carry a higher-tier fine. Thus organisations will need to review the legal bases for their different personal data processing operations, and consider whether for example legitimate interests or necessity for contract may be relied on instead of consent. The continued viability of services offered conditionally on consent to "unnecessary" personal data being processed will need evaluation in particular. Activities where consent is the best or only available legal ground should be identified. Organisations

	to personal data relating to him being processed".	**processing purposes**, and controllers must be able to prove consents were given for the relevant processing operations and purposes. The further processing of personal data for **incompatible purposes** is permitted on obtaining consent. Consent may be indicated by a written/electronic/oral statement, **ticking a box**, "choosing technical settings for information society services", or other statement/conduct **clearly indicating acceptance** of the proposed processing. But silence, **pre-ticked boxes** or inactivity cannot constitute consent. To be binding, the request for consent and declaration of consent (which may be pre-formulated by the controller) must be presented in a manner **clearly distinguishable** from any other matters, in intelligible and easily accessible form, using clear and plain language not containing "unfair terms", with safeguards to ensure data subjects are aware of the fact and extent of their consent. Electronic requests for consent must be "clear, concise and not unnecessarily disruptive to the use of the service". Their **right to withdraw consent** must be notified to data subjects, although withdrawal is not to affect the lawfulness of processing based on consent before the withdrawal. Note the data subject rights to erasure and data portability (see below) in cases where the processing is based on consent. See further the section on Marketing, below.	should consider how to implement appropriate processes for requesting and proving consent and dealing with any withdrawal of consent in compliance with with the Regulation, such as creating an online preferences dashboard or portal where data subjects could give or withdraw consents to specific processing operations and purposes. They should also review the content of their privacy notices (including specific purposes/processing operations, right to withdraw, plain English), and procedures including on the timing of notices and ensuring records of consents are kept for as long as consent-based processing is continuing. The Regulation allows continued processing of pre-existing "consented" data, but only where the consent was given "in line with" the Regulation's conditions. It is unclear what "in line with" means. Personal data currently being processed based on consent should therefore also be evaluated. Is the processing still necessary, could any such data be deleted? If not, ideally new consents should be obtained compliantly with the Regulation's requirements, or another legal basis found.
Data protection by design and default	No obligation.	Article 25 requires controllers, both when **determining the means** for processing and when **processing** personal data, to implement appropriate technical and organisational measures **designed to implement data-protection principles**, such as data minimisation, effectively, and to integrate **safeguards** into the processing to meet the Regulation's requirements and protect data subjects' rights. Data protection by design could include **pseudonymisation measures**. Controllers must also implement technical and organisational measures to ensure that, by default, only personal data which are **necessary for each specific processing purpose** are processed, and in particular ensure that by default personal data are not made accessible without the individual's intervention to "an indefinite number of natural persons". That obligation applies to the amount of personal data collected, the extent of processing, their storage period and their accessibility. An approved certification (see the Certification section)	Controllers will be obliged to implement **"data protection by design and default"**, including security by design and default, which is aimed at building in data protection from the outset. Failure to do so may be subject to a lower-tier fine, while implementing such measures may help to reduce or avoid fines if an infringement of the Regulation occurs. Processes should be reviewed to ensure data protection by design and default, particularly for new projects, services or products. DPIAs (see below) could consider specific data protection by design/default measures as measures to mitigate risks to data subjects.

		may be an element in demonstrating compliance.	
Data portability rights	The Act has no requirement for data portability.	Article 20 – introduces the right for a data subject, in certain circumstances, to receive data concerning him/her in a **structured, commonly-used and machine readable format,** and also requests that the personal data be **transferred directly to another controller, where technically feasible.** This right only applies to **data which the data subject has provided** to the controller, and where the processing is based either on the **data subject's consent** (explicit consent in the case of sensitive data) or on **necessity for a contract**, and not where the processing is based on another legal ground. It does **not** apply to processing in the exercise of **public duties** (processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller), and it must not adversely affect the rights or freedoms of others (such as other individuals, in the case of mixed data), or prejudice the right to erasure. The right to data portability may have to be **notified** to data subjects for fair and transparent processing.	This is a new right which entitles a data subject to obtain from the controller a copy of his data in a structured, commonly used and machine-readable format, but only in particular circumstances e.g. where processing is necessary for a contract. Broadly speaking, this Article brings data protection legislation in line with modern technological developments and the need for information to be provided in mediums other than physical hard copy and to allow for circumstances where data subjects wish to **direct transfers of personal data from one controller to another**, for example to switch bank accounts. Private organisations need to review their systems and procedures to facilitate data portability (and erasure) where appropriate, and also review their privacy notices/policies.
Data protection impact assessments (DPIAs)	No obligation to carry out impact assessments, although this is recommended as good practice by the Information Commissioner (see its privacy impact assessments code of practice).	Article 35 – obligation on controllers (with some Member State exceptions) to carry out **DPIAs**, taking advice from any DPO, where intended processing is likely to result in a "high risk" to data subjects and taking into account the nature, scope, context and purposes of the processing, particularly when using new technologies. Such assessments must be conducted in the case of a "systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person". They are also required if the intention is to process "on a large scale" special categories of data (sensitive data such as health data), or personal data relating to criminal convictions and offences; or in the case of "systematic monitoring of a publicly accessible area on a large scale" such as public CCTV. Supervisory authorities will be listing further types of processing operations where DPIAs are required and may specify types of processing where they are not required, applying the	Before commencing any processing likely to result in a high risk to individuals, such as profiling activities, controllers will have to carry out a review of that envisaged processing to assess the privacy risks to individuals, and identify measures to address these risks and demonstrate compliance with the Regulation. Where the DPIA indicates that the processing would be high risk, in the absence of measures by the controller to mitigate that risk, the controller will be required to consult with the Information Commissioner before being able to process that personal data under the Regulation. The Information Commissioner will be able to suspend or even ban the processing. Organisations should consider developing templates for DPIAs (bearing in mind they may need to be

		consistency mechanism e.g. where several Member States are involved. The Regulation specifies what DPIAs must cover at a minimum. DPIAs must take account of any approved code or certification (see separate section), and the controller must review whether processing is performed in accordance with the DPIA when necessary (at least where there is a change in the risk of processing). Where a DPIA indicates that the processing would result in a high risk in the absence of measures by the controller to mitigate the risk, it must consult the supervisory authority before commencing the processing and provide the DPIA and certain other information about the processing. The supervisory authority may require changes or even stop the processing to prevent infringement of the Regulation.	made available to the Information Commissioner), for use in upcoming potential high risk projects, and build in procedures for reviewing processing against compliance with DPIAs. Adherence by controllers/processors to an approved code (see Certifications section) is relevant when assessing the impact of their processing operations for DPIA purposes.
Data protection officer (DPO)	No requirement to appoint a data protection officer.	Articles 37-39 – introduces a requirement for a **data protection officer** in certain circumstances. This includes most public bodies, or where an organisation is processing data in such a way that its core activities involve conducting "regular and systemic monitoring" of data subjects "on a large scale", or processing "on a large scale" of sensitive personal data or data on criminal convictions. A group of undertakings may appoint a **single DPO** provided that a data protection officer is "easily accessible from each establishment". A single DPO officer may be designated for several public authorities or bodies, taking account of their organisational structure and size. A DPO may be a staff member of the controller or processor or fulfil tasks based on a service contract, but their contact details must be published and communicated to the supervisory authority. The qualifications, role and tasks of DPOs are set out in Articles 37-39. A DPO must operate independently and must not receive instructions from his or her employer on the exercise of the DPO's tasks.	This is the first time such a role has been mandated by data protection legislation in the UK. Note that having a DPO was already required in some jurisdictions e.g. Germany. **Public authorities** and private companies whose core activities involve **large-scale monitoring** or large-scale processing of sensitive data or data on criminal convictions must appoint a DPO. Processors for such organisations may also have to appoint DPOs. Organisations should therefore consider whether they will need to appoint a DPO and, if so, commence the recruitment process.
Definitions	Section 1 – small number of basic definitions	Article 4 – **extended/enhanced definitions** and new definitions, including definitions of "pseudonymisation", "profiling", "genetic data" and "biometric data", see below.	

Biometric data	Not specifically covered by the Act.	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 be considered sensitive "special category" data when processed for the purposes of uniquely identifying a natural person. Such processing will be prohibited unless an exception applies such as explicit consent for the purpose.
Data and manual records	Section 1(1) – "Data" means Information which— (a) is being processed by means of equipment operating automatically in response to instructions given for that purpose, (b) is recorded with the intention that it should be processed by means of such equipment, (c) is recorded as part of a relevant filing system *[structured manual filing systems]* or with the intention that it should form part of a relevant filing system; (d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68 *[health, educational or certain public records]*; or (e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d) *[essentially, semi-structured or unstructured manual records]*.	"Data" is not specifically defined. Rather, different categories of data are defined, such as personal data, genetic data, biometric data and data concerning health. However, the Regulation defines "**filing system**" as "any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis", similar to the Data Protection Directive's "structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis". In the UK, the Directive's definition was transposed into the Act as "**relevant filing system**": "any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible." Limb (e) of the Act's "data" definition (see left) was intended to cover semi-structured manual files held by public authorities, so that such files would come within the personal information exemption under Section 40 of the Freedom of Information Act 2000 (FOIA). However, it is now not clear whether such records will be exempt under FOIA. More pertinently, "accessible records" and also "recorded information" in manual files structured "according to specific criteria" (including criteria not relating to individuals) could be considered "personal data" under the Regulation.	Manual records may be brought into scope which are not considered "data" (and therefore cannot be "personal data") under the Act, and organisations, particularly public authorities, need to review their manual records and put in place systems and procedures to ensure compliance with the Regulation in relation to those which will be in scope under the Regulation.

Data concerning health	No definition in the Act.	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.	Arguably this broadens the scope of sensitive "special category" personal data, as much data could reveal information about a person's health status. "Wellbeing" data could therefore be caught by the rules regarding the processing of "special category" personal data.
Data subject	A natural person who is the subject of personal data.	An identifiable natural person, being one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.	See definition of "personal data".
Genetic data	Not specifically covered by the Act.	Personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.	Genetic data will be considered sensitive "special category" data, the processing of which, will be prohibited unless an exception applies, such as explicit consent for the purpose, or scientific research based on appropriate EU or Member State law.
Personal data	Data which relate to a living natural person who can be identified – (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the natural persons and any indication of the intentions of the data controller or any other person in respect of the natural persons.	Any information relating to an identified or identifiable natural person i.e. "data subject" (see above). Natural persons may be associated with **online identifiers** provided by their devices, applications, tools and protocols, such as Internet Protocol addresses, cookie identifiers or other identifiers such as Radio Frequency Identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them (Recital 30).	The definition of "personal data" will cover any information relating to identified or identifiable living individuals, whether identifiable by information in the possession of the controller **or any third party** (the Act only refers to identifiability by the controller, unlike the Data Protection Directive), and the Regulation clarifies that pseudonymous data remain personal data. More data, such as **IP addresses**, may therefore have to be treated as "personal data" subject to the requirements of the Regulation, and policies, systems and procedures will have to be adapted to accommodate the wider definition.

Profiling	Not defined	Any form of automated processing of personal data consisting of use of the personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.	See the section on Automated decision-taking and profiling.
Pseudonymisation	Not defined	The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. Pseudonymisation is one area where a code of conduct (see above) is possible.	The Regulation makes it clear that pseudonymous data must be treated as personal data. Pseudonymisation is considered to be a risk-reducing, data-protective measure or safeguard for personal data, rather than a way to anonymise personal data. The definition of pseudonymisation would encompass the process of **encryption**, so that encrypted personal data must be considered "personal data".
International transfers	Schedule 1 part 1 principle 8: "Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data." Schedule 1 Part II lists factors for determining an adequate level of protection, and sets out circumstances when transfers are permitted (e.g. Commission Decisions on the adequacy of particular countries, and Commission-adopted standard model clauses). Schedule 4 sets out derogations when the transfer prohibition	Articles 44-50 deal with international transfers, catching **processors** as well as controllers for the first time, "transfers" to **international organisations** as well as to "third countries" outside the EEA, and explicitly applying to **"onward transfers"** (to others in a different, and probably also the same, third country as the initial recipient). **Adequacy decisions** may be made only by the Commission (based on factors such as "essential equivalence") under a "comitology" procedure – and no longer by controllers assessing adequacy for themselves. Decisions must be reviewed at least every 4 years. "Adequate safeguards" are replaced by "appropriate safeguards", including **new model clauses** which the Commission or supervisory authorities may adopt; **binding corporate rules (BCRs)**, which once approved must, helpfully, be **recognised cross-EEA** without further authorisation; (new) legally-binding arrangements between **public authorities**; and (new) **approved codes/certifications** with legally-binding commitments to apply safeguards. Supervisory authorities may also individually authorise **contractual clauses**, or **provisions in administrative arrangements** between public authorities that include effective enforceable data subject rights. The Board may issue guidelines/further requirements regarding BCRs (Articles 70(1)(c),	Restrictions on transferring personal data outside the EEA (e.g. to third country data centres, or accessing remotely from outside the EEA) will generally be tightened up, including specifically restricting **"onward transfers"** also. The **higher tier** of fine will apply to breaches of the data export rules. Under the Regulation, the current safeguards (adequacy decisions "whitelisting" certain countries, existing model clauses and BCRs authorisations) **remain available until revoked or replaced** (or invalidated – the validity of model clauses decisions is to be referred to the Court of Justice of the EU). This also applies to the **Privacy Shield,** adopted in July 2016 to replace the Safe Harbour decision for transfers to certain US organisations (the Safe Harbour decision having been struck down by the Courts in October 2015). As and when **new forms of model clauses** are adopted by the Commission (or supervisory authorities) under the Regulation, organisations

	does not apply.	70(1)(i)). Derogations are largely similar to the current derogations, but the consent-based derogation will require relevant data subjects' **explicit consent**, **having been informed** of the possible risks for them due to the absence of an adequacy decision and appropriate safeguards. The Board is empowered to further specify criteria/requirements regarding derogations (Article 70(1)(j)). Transfers necessary on important public interest grounds will only allow for **public interests recognised by EU or Member State law**, although sometimes these may coincide with third countries' public interests, e.g. fighting terrorism. Article 48, the **"anti-FISA" provision** (as it has been termed), specifically prohibits transfer/disclosure under any third country judgment/decision unless based on international agreement, e.g. a mutual legal assistance treaty (MLAT). Even before the Brexit referendum, the UK had indicated its view that it is entitled *not* to opt in to "the parts of" this provision that trigger its opt-in under Protocol 21 to the Treaty on the Functioning of the EU, and that it will not be opting in. A new derogation allowing transfers for **"legitimate interests"** has been watered down so much that it is effectively unusable in practice except in rare cases. Note that for countries/territories/sectors where no Commission adequacy decision has been issued, EU or Member State law may, "for important reasons of **public interest**, expressly **set limits** to the transfer of **specific categories** of personal data", notifying them to the Commission. Member States may also require specific safeguards for transfers in the **employment context**, and must provide exemptions/derogations from the transfer restriction if necessary to balance data protection with **freedom of expression**. **Controller-processor contracts** will have to refer to transfers, and **records** must also include certain information on transfers. Mandatory **notifications to data subjects** must include information on proposed transfers, adequacy decisions or safeguards and the means to obtain a copy.	currently using model clauses should move to implement the new clauses, or put in place another transfer mechanism accepted under the Regulation (such as **approved codes or certifications**) before the revocation date for the "old" model clauses. Organisations wishing to implement **BCRs** should monitor for Board guidance/requirements on that front. **Self-assessment of adequacy** (based e.g. on encrypting data prior to transfer) will **no longer be a route to compliance** under the Regulation, so UK organisations relying on self-assessment for transfers that may continue beyond 25 May 2018 will need to implement another route before that date. However, as BCRs must now be recognised cross-EEA without further authorisation, the process for BCRs should be cheaper and quicker, so organisations may take the opportunity to consider whether to implement BCRs (bearing in mind they are only effective for intra-group transfers and other mechanisms must be used if third parties are involved). In the Brexit scenario, quite apart from some UK organisations being directly subject to the Regulation if they offer goods/services to EU individuals etc., there is also the issue of whether EU individuals' personal data may be allowed to flow to the UK. Unless a Commission decision is issued to rule the UK "adequate", organisations will have to use mechanisms such as model clauses or BCRs, or approved codes or certifications. If the UK adopts laws "essentially equivalent" to the Regulation (it voted in favour of the final version in the Council in April 2016), hopefully the Commission may be persuaded to adopt such a decision. A watching brief should be kept on any **national restrictions** promulgated by **relevant Member States**, including regarding employees, freedom of expression, and the UK's "non-opt-in".

			Contracts, procedures (e.g. record-keeping, see below) and **privacy notices** will also need updating in relation to transfers.
Joint controllers	Section 1(1) already envisages the concept of joint controllers, defining "data controller" as a person who, "alone or jointly or in common with other persons", determines the purposes for which and the manner in which any personal data are, or are to be, processed (reflecting the Data Protection Directive's definition).	The Regulation includes specific provisions on joint controllers who "jointly determine" the purposes and means of processing. They must "in a transparent manner" determine their respective obligations for compliance with the Regulation - particularly in relation to data subject rights and notifications to data subjects - "by means of an arrangement between them" that "duly reflects" their respective roles/relationships as regards data subjects. The "essence of the arrangement" must be made available to data subjects. Data subjects may nonetheless exercise their rights against any or all joint controllers. Certain information regarding any joint controllers must be included in controller records and given to the supervisory authority in any prior consultation required following a DPIA (see **Data protection impact assessments**). While not explicitly required, notifications to data subjects should ideally include information on joint controllers also.	Joint controllership is not uncommon in practice. The **contract** between joint controllers needs to allocate obligations appropriately, and consideration must be given as to **how to make the "essence" of the arrangement available** to data subjects, including reviewing **privacy notices**. Systems/procedures should also be reviewed to ensure information about joint controllers is properly recorded.
Legitimate interests (See also **Children, Marketing** and **Objection rights**)	Schedule 2 paragraph 6 – permits processing "necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject".	With one important difference, the legitimate interests of the controller or third party remains a permitted legal basis for processing personal data, except where overridden by data subjects' interests/rights/freedoms requiring data protection, particularly in the case of a child. The difference is that **public authorities cannot use legitimate interests** for processing personal data "in the performance of their tasks"; separate specific legal bases allow processing "necessary for the performance of a task carried out in the public interest or in the exercise of official authority" or "necessary for compliance with a legal obligation to which the controller is subject". (Disclosure to a third party is no longer mentioned, suggesting that processing necessary in the legitimate interests of a third party may be possible even when the data are not disclosed to it). **Relevant factors when considering relying on legitimate interests** are listed, including taking account of data subjects' **reasonable expectations** based on their relationship with the controller when their personal data are collected. Legitimate interests may allow processing to the extent "strictly necessary" for **fraud prevention** and **network and information security**, and may also allow **intra-group** administrative sharing (e.g. of client/employee data), "whistle-blowing"	Legitimate interests will be an increasingly important legal basis for processing personal data (along with necessity for contract), given the enhanced difficulties with obtaining and proving consent (see the Consent section above). However, they will need to be carefully assessed and documented as well as notified to data subjects, so procedures for considering legitimate interests and the content of privacy notices will require review, particularly if children are involved. Infringement of these provisions carries a **higher-tier fine**. (Note: some provisions of the Regulation refer to the legitimate interests of data subjects, but this note focuses on the legitimate interests of controllers as a legal basis for processing personal data.)

		and **direct marketing**. Data subjects must be **notified** of the controller or third party legitimate interests concerned, and any **DPIA** must also describe such interests. When processing is based on legitimate interests, data subjects will have **objection rights** (see Objection, below). Legitimate interests of controllers is one area where a code of conduct (see Certifications, above) is possible.	
Marketing (See also the sections on **Children, Consent**)	Section 11 – data subjects may require controllers to cease, or simply not to begin, processing of their personal data for direct marketing. PECR also contains provisions relating to direct marketing and consents, particularly electronic marketing.	**Marketing activities** will have to comply with both the Regulation and PECR (marketing rules under PECR are not affected by the Regulation, see **Appendix 3**). The Regulation notes that processing personal data for direct marketing may be considered a **legitimate interest**, but it is unclear how far this concept may be stretched across different brands/group entities. As now, data subjects are entitled to **stop the processing of their personal data for direct marketing** purposes (including any **profiling** related to direct marketing). Under the Regulation, this right must be **brought to their attention explicitly** by the time of first communication and presented clearly and separately from other information.	Organisations should review their marketing activities and, in particular, privacy notices/communications, for compliance.
National differences	Member States have implemented the Data Protection Directive into national laws differently, and the lack of harmonisation was one driver for the Regulation.	The Regulation explicitly allows Member States to enact their own legislation (if "necessary and proportionate in a democratic society") in numerous areas, from **restrictions** to exemptions/relaxations – too many to list here, but including regarding **data subject rights** and corresponding **principles**, **employee data**, etc. One very broad basis is **"other important objectives of general public interest"** of the EU/Member State, particularly economic/financial interests. Exemptions for **national security** will continue, and also (regulated by a separate Directive) for **law enforcement/public security purposes**.	Organisations should **monitor relevant national legislation** and national guidance for specific provisions in the areas affecting them.
Objection rights (see **Automated decision-taking, Marketing,**	Section 10 – with exceptions, individuals are entitled by notice to the data controller to require it to cease processing or not process their personal data (whether in full or only for a	Data subjects are entitled, "on grounds relating to his or her **particular situation**", to object at any time to the processing of their personal data based on **legitimate interests** or necessity for **public interest/official tasks**, including **profiling** conducted on that basis. The right to object also arises where personal data are processed for **historical or scientific research or statistical purposes**, unless the	Organisations should review their **systems and procedures for handling objections** from data subjects, including processes to cease processing and perhaps also delete the personal data concerned, as well as related **privacy notices**, particularly as infringements are subject to a

Rectification)	specified purpose or in a specified manner), on the basis that the processing is causing or likely to cause substantial unwarranted damage/distress to the individual or another.	processing is necessary for tasks conducted for public interest reasons. **No substantial unwarranted damage/distress need be involved**, and data subjects "may" exercise this right to object by "automated means using technical specifications" in the context of information society services (see Children). The controller must then cease the processing automatically (in the case of direct marketing) or (in other cases) unless it can demonstrate **"compelling legitimate grounds"** overriding the data subjects' interests "or for the establishment, exercise or defence of **legal claims**" (e.g. retention for litigation purposes). The right to object must be **brought to data subjects' attention explicitly** by the time of first communication, presented clearly and separately from other information.	**higher-tier fine**.
Processing contracts (see **Processors' obligations/liability**)	Schedule 1 part 2 paragraph 12 requires controllers to choose processors which provide sufficient guarantees in respect of the technical and organisational security measures governing processing and to take reasonable steps to ensure compliance with those measures. Paragraph 12 requires the processing to be under a written contract requiring the processor to act only on the controller's instructions and comply with obligations equivalent to the security requirements imposed on the controller.	The **pre-contractual due diligence** required of controllers will be expanded beyond the processor's ability to provide "sufficient guarantees" regarding security measures, to measures such that the processing will meet the Regulation's requirements and ensure protection of data subjects. The **minimum mandatory contractual provisions** that data processing clauses/contracts must contain are amended (e.g. "documented" instructions, including regarding international transfers, but with an explicit carve-out for processing required by EU/Member State law), and **expanded significantly** beyond instructions/security. Detailed contractual commitments must be imposed on processors, including to take "into account the nature of the processing", to "assist" with many of the obligations imposed on controllers by other provisions of the Regulation (such as controllers' obligations to respond to the exercise of data subject rights and their security and certain other obligations). The processing contract must be governed by **EU or Member State law**. Processing or sub-processing contracts may be based wholly or partly on **standard contractual clauses** which the European Commission or supervisory authorities are empowered to adopt (to meet the requirements for mandatory terms in processing and/or sub-processing agreements).	There will be **many prescriptive requirements regarding the terms of personal data processing clauses/agreements**, including flow-down of those obligations to sub-contractors. Both controllers and processors may be fined (lower-tier) if they do not implement compliant contracts. Therefore, for new processing contracts, or existing contracts that may expire after 25 May 2018, organisations should consider inserting change of law/change control clauses tailored for the Regulation, or alternatively inserting clauses attempting to comply with the Regulation with effect from 25 May 2018 (or sooner - although some processors may be reluctant to accept the Regulation's more onerous obligations before they are required to from 25 May 2018). Certain service providers (e.g. of infrastructure cloud services) may have difficulty agreeing to the expanded terms unless they control the whole supply chain so that they have no subcontractors, or unless they have the bargaining power to compel their subcontractors (e.g. data centre operators) to accept the required flow-down obligations. Processors are likely to want to include further

		Processors will also have a direct statutory "policing" obligation, to "immediately inform" the controller if, in the processor's opinion, an **instruction infringes the Regulation** or other EU or Member State data protection provisions (this will be a challenge for processors unfamiliar with other Member State laws). Reinforcing the importance placed on "instructions", the Regulation spells out that a processor who "infringes this Regulation by determining the purposes and means of processing" will be considered a controller (as is already the case under current laws), and thereby be subject to increased obligations and exposure to fines. **Subcontractors** cannot be engaged without the controller's **prior consent**, which may be general, but if general then proposed changes must be notified in advance to give controllers a chance to object. The contractual terms required in processing agreements must also be **"flowed down"** to subcontractors engaged to conduct "specific processing activities" for the controller. Adherence by processors or sub-processors to **approved codes/certifications** may help to demonstrate that they provide "sufficient guarantees".	terms in the contract for other reasons (see **Processors' obligations/liability**), so negotiations on processing contracts may well become more involved. Processors should also **review and update their systems/processes** as necessary to enable them to be in a position to comply with their direct obligations under the Regulation as well as their contractual obligations to controllers, by 25 May 2018. **Industry bodies/trade associations** have the opportunity to draft/put forward for adoption industry-appropriate and sector-specific standard contractual clauses and/or codes/certifications. Organisations should consider adhering to relevant **codes/certifications**, when approved.
Processors' obligations/liability (See **Processing contracts**)	No direct obligation on processors. However there are contractual obligations which must be imposed upon processors, as set out in Schedule 1, Part 2.	New **direct obligations are imposed on processors** in relation to **processing contracts, security measures, security breach notification, international transfers, data protection officers** and **record-keeping** (see the relevant sections in this table). **Administrative fines** may be imposed on processors, and other enhanced supervisory authority **powers such as audit** apply to processors also. In addition, processors may also be subject to claims for **compensation for the "entire damage"**, from "any person" who has suffered damage (including non-financial) resulting from infringement of the Regulation, although a processor is liable only if it did not comply with the controller's instructions or the obligations imposed by the Regulation on processors. It would be exempted from liability if it proves it is "not in any way responsible for the event giving rise to the damage". A processor who has paid full compensation for the "entire damage" is entitled to **claim back from controllers/processors involved** in the "same processing" compensation corresponding to "their part of the responsibility for the damage". However, proving exactly who is responsible for what, and to what degree, is not likely to be easy in	The Regulation will have a significant impact on service providers/vendors (i.e. data "processors") and organisations that engage them. Data processors will face direct obligations that are backed by sanctions for non-compliance. Processors may be exposed to **claims for financial damage or distress** by individuals affected by a security incident or indeed any other infringement of the Regulation, who may choose to sue (for the entire damage) whomever in the supply chain is perceived to have the deepest pockets. All this means that negotiations of controller-processor contracts are likely to be more protracted, as the parties will want a **clear, detailed allocation of responsibilities/obligations** and processors will want **cross-indemnities** in case they are sued first, as well as provisions on **conduct of litigation and proof**.

		practice, particularly with a complex supply chain.	Organisations should also consider whether taking out **insurance** would be appropriate.
Record-keeping	No specific obligations, but controllers must notify certain information ("registrable particulars") to the Information Commissioner under Section 16.	Both controllers and processors (and representatives where applicable) must maintain records of processing activities including certain prescribed information, to be made available to the supervisory authority on request. There is some overlap with the information that must be notified to data subjects (see **Transparency**). This obligation does not apply to organisations with fewer than 250 employees unless the processing is likely to result in "a risk" to data subjects (which low threshold would still catch many SMEs), is not occasional or includes special categories or criminal convictions/offences data.	Organisations should check that their systems/procedures enable the recording of the required information.
Rectification, erasure and restriction rights	Schedule 1 part 1 paragraph 4, principle 4 - requires personal data to be accurate and, where necessary, kept up to date. Section 14 – If a court is satisfied on the application of a data subject that personal data of which the applicant is the subject are inaccurate, the court may order the data controller to rectify, block, erase or destroy those data and any other personal data in respect of which it is the data controller and which contain an expression of opinion which appears to the court to be based on the inaccurate data. Under Section 40 the Information Commissioner may also serve an enforcement notice or order the rectification, blocking, erasure or destruction	For rectification, the Regulation does not require a court to be satisfied on the application of a data subject. Instead, there is an absolute right in Article 16 to obtain from the controller without undue delay the **rectification** of inaccurate personal data, including completing incomplete personal data. Article 17, the right to erasure, enshrines the **"right to be forgotten"** principle. The data subject is entitled to require the controller to erase personal data without undue delay in certain circumstances. Additionally, where the controller has **made that data public** and is obliged to erase the data, it must (taking account of available technology and implementation costs) take **reasonable steps to inform controllers** processing the data of the **request for erasure** of their links/copies of the data. This right applies only where: ○ the personal data are **no longer necessary in relation to the purposes** for which they were collected or otherwise processed; ○ the data subject **withdraws consent** on which the processing is based (see Consent) and there is no other legal ground for its processing; ○ the data subject exercises his or her **right to object** to the processing (see Objection rights) for direct marketing, or there are no overriding legitimate grounds for the processing; ○ the personal data have been unlawfully processed; ○ the data must be erased for compliance with a legal obligation	Building on the existing right to erasure, whereby individuals can request that a controller deletes personal data that has been or is being processed in contravention of data protection laws, under the Regulation an individual will be able to request that his personal data be deleted and, where the personal data has been made public, that other controllers processing the personal data also erase links to, or copy or replication of, such personal data. It is worth noting that this "right to be forgotten" has been significantly watered down from the 2012 draft of the Regulation. It was anticipated that the concept would almost allow someone to eradicate an online presence; whereas, it is now a right to have specific data removed only in particular situations. The **higher-tier** fine applies in relation to these provisions. Organisations will need to review their systems and procedures to enable compliance with the rights to rectification, erasure and restriction, including notifications to recipients (which will require recording of recipients). Privacy notices

	of inaccurate data.	in EU/Member State law to which the controller is subject; ○ the data were collected in relation to the offering of information society services to a child (see Children). The Board may issue **guidelines**, recommendations, and best practices on procedures for erasing links, copies or replications of personal data from publicly available communication services (Article 70(1)(d)). However, the controller is not obliged to erase the data or inform other controllers to the extent that processing is necessary for **freedom of expression/information**; compliance with applicable **EU/Member State law; public interest/official tasks**; public interest in public health; **archiving purposes in the public interest, scientific or historical research purposes or statistical purposes** insofar as the right to erasure is "likely to render impossible or seriously impair the achievement of the objectives of that processing"; or **legal claims**. Expanding significantly on "blocking" under current laws, data subjects will have the **right to require controllers to restrict processing** where: they contest the personal data's accuracy (pending the controller's verification of accuracy); they object to the processing (pending verification of whether the controller's "legitimate grounds" override the data subject's); the processing was unlawful but the data subject wishes restriction rather than erasure; or the personal data are no longer needed for the controller's purposes but the data subject requires them for legal claims. Such data can be **stored but not otherwise processed** except with the data subject's consent, for legal claims, to protect another person's rights or for important EU/Member State public interest reasons. The controller must **inform the data subject** before lifting the restriction. The rights of rectification, erasure and restriction must be **notified** to data subjects (see Transparency). Controllers must also notify any **rectification, erasure or restriction** to every recipient to whom the data concerned was disclosed (informing the data subject of those recipients if the data subject so requests), unless that is impossible or requires disproportionate effort,.	should also be updated. Organisations should also monitor for any guidance from the Board on the erasure of public links.
Security measures (see also **Security breach notification,**	Schedule 1 part 1 paragraph 7, principle 7 – requires data controllers to take "appropriate technical and organisational	The basic underlying risk-based approach is unchanged, so that **costs** and the **state of the art** remain factors to be taken into account. However, the Regulation's requirements apply to **processors,** not just	Organisations, particularly controllers, should review their policies and procedures as well as systems (and employee contracts) for compliance with the Regulation, instigating regular

Certifications)	measures" against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. Schedule 1 part 2 paragraph 11 requires the level of security to be appropriate to the harm that might result and the nature of the data, having regard to the state of technological development and implementation cost. Schedule 1 part 2 paragraph 10 obliges data controllers to take reasonable steps to ensure the reliability of employees with access to personal data (the UK's transposition of Article 16 of the Data Protection Directive, which requires that any person acting under the authority of the controller or processor (including the processor) who has access to personal data must not process them except on instructions from the controller, unless required to do so by law).	controllers. It specifically mentions the standard security objectives of **confidentiality, integrity and availability** and also requires measures to ensure **resilience and business continuity**, as well as **regular testing** and evaluation of the effectiveness of security measures. **Controllers are subject to a higher-tier fine** for infringement of the security requirements, but **processors only to a lower-tier fine**. Again, adherence to an **approved code/certification** may be used to help demonstrate compliance with the basic security requirements. Article 16 of the Data Protection Directive, requiring processing only in accordance with the controller's instructions, is largely replicated (twice) but explicitly mentions persons under the **processor's authority**. The Regulation spells out that only **EU or Member State law** may allow processing other than on the controller's instructions.	testing/evaluation if not already conducted. They should also consider whether to adhere to relevant approved codes/certifications once more information about them is known.
Security breach notification (see also **Security measures**)	The Act does not require notification of personal data breaches to the Information Commissioner (although the Information Commissioner encourages notification of serious breaches, and has produced guidance on security breach management and notification). However, Reg 5a, Privacy and	Articles 33 and 34 – introduce an obligation for the controller to notify the supervisory authority of certain minimum information (including the nature of breach, data subjects concerned, likely consequences and mitigation measures), **without undue delay** (but, where feasible, within **72 hours**) after becoming aware of a "**personal data breach**" (effectively, a security breach affecting confidentiality or integrity, but not availability). This is unless the data breach is unlikely to result in "a risk" to the rights and freedoms of natural persons. If notification is not made within 72 hours, reasons for the delay must be given. Notification may be phased, as more information becomes available. Any such breaches must be documented, including their effects and the remedial	The Regulation introduces a mandatory notification requirement in relation to any "personal data breach". Under the Act, organisations that suffer a serious personal data breach can potentially avoid enforcement by not notifying the Information Commissioner (on the assumption that the data breach does not come to the ICO's attention in another way). In contrast, under the Regulation there will be "nowhere to hide" as failure to notify a personal data breach could itself lead to a (lower-

	Electronic Communications (EC Directive) Regulations 2003 ("**PECR**"), does impose an obligation to report a "personal data breach" to the Information Commissioner, and also to data subjects if likely to adversely affect their personal data or privacy. Note that this obligation to notify only applies to organisations providing electronic communications services to the public, it does not apply to all data controllers. **NB:** PECR has not been repealed by the Regulation.	action taken. There is also an obligation (similarly to an obligation in PECR) for controllers to communicate a personal data breach to **data subjects without undue delay**, where the breach is likely to result in a "**high risk**" to the data subject, or if the supervisory authority requires it to do so on that basis. However, notification to data subjects is not needed where the breached data were rendered **unintelligible to unauthorised persons** through measures like encryption, or subsequent measures by the controller have made the high risk unlikely, and notification may be through public communication if it would otherwise involve disproportionate effort. **Processors** must notify their controllers of personal data breaches "without undue delay" in circumstances when breaches must be notified. The Board is also empowered to issue guidelines for "establishing" personal data breaches, determining "undue delay", and circumstances likely to result in a "high risk" (Articles 70(1)(g), 70(1)(h)). Security breach notification is one area where a code of conduct (see below) is possible.	tier) fine. Organisations will need to ensure **effective breach management/recording procedures**. The threshold in the Regulation of "unless unlikely to result in a risk" is very low, but arguably might not be reached where, for example, all breached data have been **securely encrypted** and the key has not been compromised. However, with many breaches it is difficult to know which data were accessed, so for caution's sake organisations may choose to notify in any event, particularly given the threat of a fine for not notifying relevant breaches. Organisations' **breach management measures** should be integrated with measures to meet the more prescriptive (although still risk-based) security obligations under the Regulation (see below). Thus, incident response/management plans should also be regularly tested. Organisations should also monitor for Board guidance.
Sensitive "special category" personal data; criminal convictions	Section 2 – defines "sensitive personal data" ("special categories" of data under the Data Protection Directive) to include information on racial or ethnic origin, physical or mental health or condition and certain information on criminal offences. Sensitive personal data cannot be processed unless a Schedule 3 condition is met (in addition to the conditions for fair and lawful processing), such as explicit consent, necessity for meeting the controller's national employment law	The "special categories" of personal data are expanded to include **biometric data** for the purpose of uniquely identifying a natural person, and **genetic data**, while "**data concerning health**" has been specifically defined (see Definitions, above). Reference to sexual orientation has also been added. The situations when processing of "special category" data is allowed are largely the same (with social security/social protection law added to employment law). Further exemptions are added: legal **claims**, necessity for **public interest reasons** under appropriate EU or Member State law, necessity for **archiving purposes in the public interest, scientific/historical research or statistical purposes** under appropriate EU/Member State law, and various public health/health systems/services-related provisions, which again must be under appropriate EU/Member State law. Member States are given a "margin of manoeuvre" regarding special categories data, e.g. they may introduce **further conditions/limitations** regarding genetic data, biometric data or data concerning health.	More types of personal data are included in the "special categories", so organisations should review their systems/processes to enable compliance by 25 May 2018 for the processing of data that would not be "sensitive" under the Act but would be classed as "special category" under the Regulation, considering the relevant exemptions as well as applicable national laws. Organisations that need to process criminal convictions data, such as driving offences data for motor insurance purposes, may wish to check appropriate national legislation.

	obligations, etc.	**Criminal convictions/offences data** can only be processed under official control or if authorised by appropriate EU/Member State law. In various areas, **further restrictions or requirements** apply in the case of special categories or criminal convictions/offences data, e.g. DPIAs.	
Subject access rights	Section 7 – data subjects are entitled to request certain information relating to their personal data being processed, including a right to access the underlying data, with certain exemptions. A data controller is not obliged to supply this information, unless the request is received in writing, the data controller has verified the data subject's identity and the relevant fee (not exceeding £10 – or £50 in certain circumstances e.g. health data and education information) has been paid.	The relevant information will have to be provided **free of charge** under the Regulation, except where shown to be "manifestly unfounded/excessive" or for further copies, and must be provided in **commonly used electronic form** when requested electronically. The time limit for responses is reduced – "without delay" and in any event within **one month** (extendible by **two further months** for complex/numerous requests, explaining the reasons to the data subject). If the controller processes large quantities of information on the data subject, it should be able to ask the data subject to **specify the information/processing activities** to which the request relates. The information to be provided is similar to that required currently, with the addition of **further prescribed information** e.g. regarding storage periods "where possible", and **international transfers and safeguards**. There seem to be no **exemptions**, other than a general exemption that the provision of the copy of the personal data shall not adversely affect the **rights and freedoms of others** – such as intellectual property rights or, presumably, where others' personal data is involved.	Organisations should review their systems and procedures to enable the provision of the required information within the shorter timescales (e.g. drafting/updating template responses), noting the elimination of a fee, relative lack of exemptions and the higher-tier fine for infringement of these provisions. Organisations could consider providing remote access to a secure self-service system where appropriate.
Transparency – privacy/fair processing notices, privacy policies etc.	Schedule 1 part 2 paragraph 2 – personal data are not treated as processed fairly unless certain information is provided to the data subject. The Information Commissioner has issued a privacy notices code of practice.	**More information must be notified** to data subjects, differing slightly in terms of content and timing of notification depending on whether the data were obtained directly from the data subject or not, and including where **further processing** for other purposes is intended. There is a significant overlap between the information that must be recorded (see **Record-keeping**, above), and the information that must be notified to data subjects. The information need not be notified where the data subject already has it, or an **exemption** applies (in relation only to data not obtained directly from the data subject) such as disproportionate effort for scientific research data where safeguards are implemented. The requirements for transparency are **expanded**, including regarding the form of the information (concise, intelligible, clear and plain language).	Organisations should update their privacy notices and similar notifications accordingly as well as related procedures, before further processing (beyond the original purpose) takes place. Infringement of these requirements is subject to a higher-tier fine.

5. References

Appendix 1 Where have the Data Protection Act 1998's principles gone?

Data Protection Act 1998 (now) (SCHEDULE 1)		General Data Protection Regulation (Article 5)
1. Personal data shall be processed **fairly and lawfully** and, in particular, shall not be processed unless: (a) at least one of the conditions in Schedule 2 is met, and (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.	→	1. Personal data must be: (a) processed **lawfully, fairly and in a transparent** manner in relation to the data subject ("lawfulness, fairness and transparency").
2 Personal data shall be obtained only for one or more **specified and lawful purposes**, and shall not be further processed in any manner incompatible with that purpose or those purposes.	→	(b) collected for **specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ("purpose limitation").
3. Personal data shall be **adequate, relevant and not excessive** in relation to the purpose or purposes for which they are processed.	→	(c) **adequate, relevant and limited** to what is necessary in relation to the purposes for which they are processed ("data minimisation").
4. Personal data shall be **accurate and, where necessary, kept up to date**.	→	(d) **accurate and, where necessary, kept up to date**; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are **erased or rectified without delay** ("accuracy").
5. Personal data processed for any purpose or purposes shall **not be kept for longer than is necessary** for that purpose or those purposes.	→	(e) 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ("storage limitation").
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.		
7. **Appropriate technical and organisational measures** shall betaken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.	→	(f) 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").
8. **Personal data shall not be transferred to a country or territory outside the European Economic Area** unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.	→	**No equivalent principle**, although the area of **transferring personal data** to a third country or international organisation is dealt with at length in the GDPR. 2. The **controller shall be responsible for and be able to demonstrate compliance** with paragraph 1 ("accountability").

Appendix 2

Key Topics – Articles/Recitals

Area	Article(s)	Recital(s)
Accountability principle	5(2), 24,, 83(4)(a), 83(5)(a)	74; 85
Administrative fines	58(2)(i), 83; 70(1)(k)	148, 150, 151, 152; 130
Applicability, territorial scope	3, 4(17), 27; 1(17), 13(1)(a), 14(1)(a), 30, 31, 58(1)(a), 83(4)(a), 83(5)(a)	22, 23, 24, 25, 80, 122
Automated decision-taking and profiling	4(4), 21, 22; 13(2)(f), 14(2)(g), 15(h); 35(3)(a); 47(2)(e); 70(1)(f), 70(1)(l), 83(4)(a), 83(5)(b)	70, 71, 72, 73, 75, 91; 24
Board	68, 69, 70, 71, 72, 73, 74, 75, 76; 51(3), 52(4), 57(1)(t), 60(7), 61(8), 61(9), 64, 65, 66, 67, 78(4); 35(4), 35(5), 40, 41(3), 42, 43, 59, 94(2)	139, 140, 141, 142, 143 and numerous others
Certifications and codes of conduct	24(3), 83(2)(j), 83(4)(b); 40, 41, 42, 43; 24(3), 25(3), 28(5), 28(6), 32(3), 35(8), 46(2)(e), 46(2)(f), 57(1)(m), 57(1)(n), 57(1)(o), 57(1)(p), 57(1)(q), 58(1)(c), 58(2)(h), 58(3)(d), 58(3)(e), 58(3)(f), 64(1)(b), 64(1)(c), 70(1)(n), 70(1)(o), 70(1)(p), 70(1)(q), 70(1)(x)	98, 99, 100, 148; 77, 81, 166, 168
Children	8, 4(25); 6(1)(f), 12(1), 17(1)(f), 40(2)(g), 83(4)(a)	38, 58, 65, 71, 75
Consent of the data subject	4(11), 7, 6(1)(a), 13(2)(c), 14(2)(d), 17(1)(b), 18(2), 20(1)(a), 22, 49(1)(a), 49(1)(f), 83(5)(a); 6(4)	32, 33, 38, 40, 42, 43, 50, 65, 68, 71, 111, 155, 171
Data protection by design and default	24, 25, 47(2)(d)	78, 108
Data portability rights	20, 13(2)(b), 14(2)(c), 83(5)(b)	68, 73, 156
Data protection impact assessments (DPIAs)	35, 36, 39(1)(c); 57(1)(k), 64(1)(a), 83(4)(a)	84, 89, 90, 91, 92, 93, 94, 95, 96, 97
Data protection officer (DPO)	37, 38, 39; 13(1)(b), 14(1)(b), 30(1)(a), 30(2)(a), 33(3)(b), 35(2), 36(3)(d), 47(2)(h), 57(3), 83(4)(a)	77, 97

Area	Article(s)	Recital(s)
Definitions		
Biometric data	4(14), 9 particularly 9(1), 9(4), 83(5)(a)	51, 53, 91
Data and manual records	2(1), 4(6)	15
Data concerning health	4(15) 9(1), 9(2)(h), 9(2)(i), 9(4), 17(3)(c), 23(1)(e), 36(5), 88; 4(4), 4(13), 83(5)(a)	(Public health issues also included) 35, 53, 54, 63, 65, 71, 73, 75, 91, 112, 155, 159
Data subject	4(1)	26, 27, 30
Genetic data	1(13), 4(1), 9 particularly 9(1), 9(4), 83(5)(a)	34, 35, 53, 71, 75
Personal data	4(1), 5(1)(e), 11, 83(4)(a), 87, 89; 4(14)	26, 27, 30, 51, 57, 64, 156
Profiling	4(4), 21, 22; 13(2)(f), 14(2)(g), 15(1)(h), 35(3)(a), 47(2)(e), 70(1)(f), 83(4)(a)	30, 38, 60, 63, 70, 71, 72, 73, 75, 91; 24
Pseudonymisation	4(5), 6(4)(e), 25(1), 32(1)(a), 40(2)(d), 89(1)	26, 28, 29, 75, 78, 85, 156,
International transfers	4(26), 40(3), 42(2), 44, 45, 46, 47, 48, 49, 50, 58(2)(j), 85(2), 83(5)(c), 83(5)(e); 13(1)(f), 14(1)(f), 15(2), 28(3)(a), 30(1)(e), 30(2)(c); 57(1)(j), 57(1)(r), 57(1)(s), 58(3)(g), 58(3)(h), 58(3)(i), 58(3)(j), 64(1)(d), 64(1)(e), 64(1)(f), 70(1)(c), 70(1)(i), 70(1)(j), 93(2); 85(2), 96, 97(1), 97(2)(a)	101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 168, 169, 170
Joint controllers	26, 4(7), 30(1)(a), 36(3)(a)	79
Legitimate interests (See also Objection)	6(1)(f) and last paragraph, 13(1)(d), 14(2)(b), 21(1), 35(7)(a); 40(2)(b); 49(1)(g), 49(2)	47, 48, 50, 69, 111, 113
Marketing	21(2), 21(3)	47, 70; 38
Objection rights	21, 4(25); 13(2)(b), 14(2)(c), 15(1)(e), 83(5)(b)	69, 70, 156
Processing contracts	26, 28, 82, 83(4)(a), 93(2), 63; 57(1)(j), 83(4)(a)	81, 168
Processors' obligations/liability (See also Applicability; Certifications; Data	27, 28, 29, 30, 31, 32, 33(2), 35(8), 36(2); 79, 81, 82, 83; 70(1)(c), 70(1)(g),	145, 146, 147, 148, 149; 164; 13, 18, 28, 77, 82, 95, 97, 98, 99, 153

Area	Article(s)	Recital(s)
protection officer; International transfers)	70(1)(i), 70(1)(o), 85(2), 90	
Record-keeping	30, 49(6), 83(4)(a)	82, 13
Rectification, erasure and restriction rights	4(3), 5(1)(d), 13(2)(b), 14(2)(c), 15(1)(e), 16, 17, 18, 19, 58(2)(g); 4(9), 70(1)(g), 83(5)(b)	39, 59, 65, 66, 67, 73, 156
Security breach notification	4(12), 33, 34, 58(2)(e); 40(2)(i), 70(1)(g), 70(1)(h), 83(4)(a)	85, 86, 87, 88; 73
Security measures (See also Data protection by design; Definition – pseudonymisation; Processing contract)	32, 29, 30(1)(g), 30(2)(d), 5(1)(f), 83(2)(d), 83(4)(a), 83(5)(a); 25	81, 83
Sensitive "special category" personal data; criminal convictions	9, 10, 6(4)(c), 13(2)(c), 14(2)(d), 17(1)(b), 20(1)(a), 22(4), 27(2)(a), 30(5), 35(3)(b), 37(1)(c), 47(2)(d), 83(5)(a), 83(5)(b)	10, 51, 52, 53, 54, 71, 75, 80, 91, 97, 161
Subject access rights	12, 15, 83(5)(b)	58, 59, 63, 64
Transparency – privacy/fair processing notices, privacy policies etc.	12, 13, 14, 15, 83(5)(b)	58, 59, 60, 61, 62

Appendix 3

Interaction with other legislation

Please note that, beyond the legislation cited below, there is other legislation which you may need to consider (in terms of how it interacts with the Regulation) depending upon your circumstances; this list identifies only a few key legislative instruments.

PECR is unaffected by the Regulation, but the European Commission intends to amend the underlying E-Privacy Directive 2002/58/EC – the public consultation closed on 5 July 2016, and no doubt it will take some months for the Commission to digest the results and decide on the next steps.

Data Protection Regulation (EC) 45/2001 on data protection by EU institutions is also to be updated in line with the Regulation, but the timing is not yet known.

The revised EU Directive on payment services, popularly known as **PSD2**, must be implemented nationally by Member States by **January 2018**, with some transitional provisions. As the UK is likely to still be an EU Member State then, it would have to implement PSD2. To monitor statements from the Payment Systems Regulator regarding PSD2, please see https://www.psr.org.uk/psr-publications/news-announcements/PSR-statement-european-union-referendum-result. The Directive would require payment services providers to access, process and retain personal data necessary to provide their payment services, only with the "**explicit consent**" of the payment service user, which is narrower than the Regulation, although processing is also to be permitted "when necessary to safeguard the prevention, investigation and detection of payment fraud". The Directive also introduces various specific requirements on payment services providers regarding the management of operational and security risks, including "strong customer authentication" in certain situations and incident reporting obligations. Further guidance and requirements are to follow, particularly on technical standards. The possible overlap between the Regulation and the Directive, and how any conflicts are to be resolved, needs to be kept under review.

The **Network and Information Systems Security Directive** was approved by the European Parliament in July 2016, having previously been approved by the Council and is expected to be published in the Official Journal in August 2016, with Member States being required to implement it 21 months later (i.e. probably by **May 2018**), with another 6 months after that (**November 2018**) to produce their lists of or objective criteria for determining, the operators of "essential services" (basically, critical infrastructure in specified sectors such as banking, transport, utilities, health etc.) in their countries. This means that, subject to a contrary outcome as a result of Brexit, the UK would need to implement the Directive by around **May 2018**. Also, UK organisations operating in the targeted sectors who have an "establishment" in the territory of an EU Member State, and who are listed by that Member State or fall within its criteria for designation as providing "essential services" in that Member State, would still be subject to its national laws implementing the Directive, regardless of Brexit.

Extending to all data (not just personal data) the Directive will require Member States to impose security requirements and incident notification requirements on operators of essential services and similar but lighter requirements on digital service providers (cloud services, online marketplaces and search engines). Affected organisations will need to navigate the differences in requirements between the Regulation and the Directive and implement systems/procedures to deal with both.

Appendix 4

Out-Law commentary

Please see http://www.out-law.com/en/topics/tmt--sourcing/eu-data-protection-regulation/ for Out-Law commentary on the Regulation, including our on-going commentary following the date of issue of this Guide.

6. Contacts

UK

Marc Dautlich
Partner, Head of Information Law
T: +44 20 7490 6533
M: +44 7984 405 672
E: marc.dautlich@pinsentmasons.com

Cerys Wyn Davies
Partner, IP & Data Protection
T: +44 121 625 3056
M: +44 7836 527 690
E: cerys.wyn-davies@pinsentmasons.com

France

Diane Mullenex
Partner, Head of International Telecoms
T: +44 20 7490 9250
M: +44 7979 477 965
E: diane.mullenex@pinsentmasons.com

Annabelle Richard
Partner, IT, Telecoms & Data Protection
T: +33 1 53 53 02 23
M: +33 6 21 17 64 05
E: annabelle.richard@pinsentmasons.com

Germany

Florian von Baum
Partner, Head of IT/IP & Outsourcing
T: +49 89 203043 537
M: +49 172 368 01 88
E: florian.vonbaum@pinsentmasons.com

Stephan Appt
Partner, Automotive, IT & Data Protection
T: +49 89 203043 561
M: +49 174 333 28 56
E: stephan.appt@pinsentmasons.com