Title of Policy: Data Protection Policy	Policy No: SCG0112
Approved Date: 01/04/2020	Approved By: Director of Operations
Review Date: 01/04/2021 1/4/22	Next Review Date: 01/04/2025

Summary

EU Regulation 2016/679, generally known as the General Data Protection Regulation (GDPR), can be found at eur-lex.europa.eu. As an EU Regulation, it had direct effect in the UK from the day it came into force (25 May 2018). The Data Protection Act 2018, according to the ICO, is meant to be read side by side with GDPR. The ICO notes that the GDPR gives Member States limited opportunities to make provisions for how it applies in their particular country. One element of the DPA 2018 is providing these details. Parts of the new Act cover the ICO and its duties, functions and powers plus the enforcement provisions required to implement the GDPR. It also transposes the provisions of the EU Law Enforcement Directive into national law setting out the requirements for the processing of personal data for criminal "law enforcement purposes".

GDPR controls how personal information is used by organisations, businesses or the Government and it is designed to make sure that people's personal information is protected — no matter where it is sent, processed or stored, even outside the EU.

The ICO noted that organisations in the UK which had complied with the requirements of the Data Protection Act 1998 (DPA) would be in a good position to meet their obligations under GDPR. However, as this topic makes clear, there are several new elements and significant enhancements which require a more coherent and focused approach to data protection.

In the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (SI 2019/419), the UK Government confirmed that, following the decision to

leave the EU, the "UK GDPR" means Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the General Data Protection Regulation), as amended by SI 2019/214.

From 31 July 2022, all regulated social care providers in England must comply with the national data opt-out policy. See National Data Opt-Out Policy.

In Practice

Data Protection Principles

Article 5 of UK GDPR lays down six data protection principles which set out the main responsibilities for organisations in this area. These are that personal data must be:

- processed lawfully, fairly and in a transparent manner in relation to individuals
- 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 not be considered to be incompatible with the initial purposes
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- 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
- 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 subject to implementation of the appropriate technical and organisational measures required by GDPR in order to safeguard the rights and freedoms of individuals
- 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.

There is stronger legal protection for more sensitive information, such as:

- race
- ethnic background
- political opinions
- religious beliefs
- trade union membership

- genetics
- biometrics (where used for identification)
- health
- sex life or orientation

These principles must be followed at all times when processing or using personal information. Therefore, through appropriate management and strict application of criteria and controls, a compliant organisation will:

- observe fully the conditions regarding the fair collection and use of information including the giving of consent
- meet its legal obligations to specify the purposes for which information is used
- collect and process appropriate information only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements
- ensure the quality of information used
- ensure that the information is held for no longer than is necessary
- ensure that the rights of people about whom information is held can be fully exercised under GDPR (including the right to be informed that processing is being undertaken, to access one's personal information; to prevent processing in certain circumstances, and to correct, rectify, block or erase information that is regarded as incorrect)
- take appropriate technical and organisational security measures to safeguard personal information
- publicise and abide by individuals' right to appeal or complain to the supervisory authority (the Information Commissioner's Office (ICO)) in the event that agreement cannot be reached in a dispute regarding data protection
- ensure that personal information is not transferred abroad without suitable safeguards.

Data Protection by Design

Under UK GDPR, employers have a general obligation to implement technical and organisational measures to show that they have considered and integrated data protection into all data processing activities. In other words, safeguards must be built into products and services from the earliest stage of development and privacy-friendly default settings must be the norm. Keeping records of how and why decisions regarding data protection have been taken should become standard practice.

The ICO recommends that controllers should put appropriate technical and organisational measures in place that not only ensure that the necessary safeguards are in place but clearly

demonstrate compliance. Larger employers (more than 250 staff) will have to maintain internal records of their processing activities and smaller firms will have to do so for “higher risk” processing, such as DBS (Disclosure and Barring Service) checks. To embed these practices in the organisation, data protection policies could, for example, become part of staff training courses. It is sensible for organisations to carry out audits of their processing activities to make certain that everyone is aware of the new rules and that internal procedures and processes such as contracts, website design, publicity material and HR policies are all in line with UK GDPR’s requirements.

Personal Data

Personal data means any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. The EU defines personal data as: "...any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a photo, an email address, employee bank account details, posts made on social networking websites, medical information, or computer’s IP addresses". UK GDPR definition of personal data is broader than under the DPA as it includes IP addresses, device IDs, location data and genetic and biometric data.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way that businesses collect information about people. UK GDPR applies to both automated personal data and to manual filing systems where personal data is accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data. Personal data that has been key-coded can fall within the scope of UK GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

Sensitive Personal Data

Article 9 of UK GDPR covers sensitive personal data. It states: "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited." However, the Article goes on to list a series of exceptions to this ban which include:

- where the data subject has given explicit consent to the processing of those personal data for one or more specified purposes
- where processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by EU or national law
- processing is necessary to protect the vital interests of the data subject or of another

natural person where the data subject is physically or legally incapable of giving consent

- processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices; or
- processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects.

Personal data relating to criminal convictions and offences are not included in this prohibition, but similar extra safeguards apply to its processing under Article 10 of UK GDPR. Processing of such data or related security measures must be carried out only under the control of official authority or when the processing is authorised by EU or domestic law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions must only be kept under the control of official authority.

Employers' Duties

Employers must involve the organisation's Data Protection Officer (DPO), in a timely manner, in all issues relating to the protection of personal data. They must take account of the DPO's advice and the information they provide on the organisation's data protection obligations. Employers must ensure that any other tasks or duties they assign to their DPO do not result in a conflict of interests with their role as a DPO. They must never penalise the DPO for performing their duties.

Employers will need to collect permission from employees to store and process their data. However, they should avoid the temptation to refer to this process as "employee consent". While this concept worked well under the DPA, the requirements for valid consent have been made much stricter under UK GDPR and the ICO has frequently stressed that consent per se is not the "silver bullet" for UK GDPR compliance. This is because it is recognised that an imbalance exists between employer and employee which makes it difficult to show valid freely-given consent.

Under UK GDPR, consent is one lawful basis for processing, but there are alternatives and it is important to note that consent is not inherently better or more important than these alternatives. The difficulties of relying on consent include that it must be unambiguous and involve a clear affirmative action (an opt-in, but UK GDPR specifically bans pre-ticked opt-in boxes). It also requires individual (granular, to use the jargon) consent options for distinct processing operations. Consent should also be separate from other terms and conditions. Finally, it must be noted that employees will have the right to withdraw their consent at any time so any system based on consent would have to make this clear and be able to adjust to meet such a

change.

The options are as follows.

- "Legal obligations" is a lawful basis if an employer needs to process the personal data to comply with a common law or statutory obligation. This could, for example, relate to disclosing employee salary details to HM Revenue & Customs (HMRC) or to the processing of employees' bank account data for payroll purposes. The ICO makes clear that "you cannot rely on this lawful basis if you have discretion over whether to process the personal data, or if there is another reasonable way to comply".

- "Vital interests" is unlikely to feature in most employers' routine plans as it covers the need to process the personal data to protect someone's life. If the person's vital interests can reasonably be protected in another less intrusive way, however, this basis will not apply.

- "Public task" is mainly relevant to public authorities or to organisations that exercise official authority or carry out tasks in the public interest. Again, to quote the ICO: "If you could reasonably perform your tasks or exercise your powers in a less intrusive way, this lawful basis does not apply."

- "Legitimate interests" is the legal basis most likely to be favoured by employers. It is the most flexible, and likely to be most appropriate where they are using people's data in ways the employees would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing. The legitimate interests can be those of the employer or of third parties: they can include commercial interests, individual interests or broader societal benefits.

With regard to using legitimate interests as the legal basis, the ICO has stated: "You must balance your interests against the individual's. If they would not reasonably expect the processing, or if it would cause unjustified harm, their interests are likely to override your legitimate interests." It advises a three-step approach to verify this basis:

1. Identify a legitimate interest.

2. Show that the processing is necessary to achieve it.

3. Balance it against the individual's interests, rights and freedoms.

While it is not mandatory, employers would be well advised to draw up a comprehensive policy and workable procedures covering data protection rules and the right of access, taking the opportunity to consult trade union or other representatives. The policy should be made available to all members of staff, customers, contractors and volunteers and should form part of any induction course. They should also carry out a privacy impact assessment (PIA) to ensure that privacy risks have been properly considered and addressed. In the interests of transparency, the results should be publicised on the organisation's website.

Legitimate interests form

4. Seva Care Group has decided that "legitimate interests" as defined in the General Data Protection Regulation (UK GDPR) is the most appropriate basis for processing employee

data.

5. We have reached this decision having carried out a legitimate interests assessment (LIA) which is available for consultation and which ensures that we can justify this decision. Recognising our responsibility to protect your interests, we have ensured that the processing we will carry out is necessary and that there is no less intrusive way to achieve the same result.

   We will keep the LIA under review and repeat it if circumstances change.

6. In using this basis for processing data, we will make sure that your interests, as protected by UK GDPR, are not undermined by our legitimate interests. We also commit to only using your data in ways that you could reasonably expect as part of your employment with this organisation.

7. If there are any exceptions to this, should we be legally compelled to provide certain information to a statutory body, for example, then we will so far as is possible keep you informed of the change and explain our reasons.

8. Any processing carried out will be necessary. If it is possible reasonably to achieve the same result in another less intrusive way, legitimate interests will not apply.

9. We have considered and applied safeguards to reduce the impact of data processing where possible.

Legitimate interests assessment

There is no obligation in UK GDPR to do an LIA, but it is best practice to conduct one and it is difficult to meet obligations under the accountability principle without it. The ICO recommends using the following three-part test as the basis for an LIA.

10. Purpose test: this involves answering questions such as why the organisation wants to process the data; what benefit does it expect to get from the processing; what would the impact be if it was not possible to go ahead with the processing; is the organisation complying with industry guidelines or codes of practice?

11. Necessity test: questions under this part of the test will include how the processing will help the organisation to achieve its purpose; to what extent is the processing proportionate to that purpose; is it possible to achieve the same purpose without the processing; and is it possible to achieve the same purpose by processing less data, or by processing the data in another more obvious or less intrusive way?

12. Balancing test: this involves considering the impact on individuals' interests and rights and freedoms and assessing whether this overrides the organisation's legitimate interests. Question will include: is this special category data or criminal offence data; does it involve data which people are likely to consider particularly "private"; and does it involve processing children's data or data relating to other vulnerable people.

The ICO states: "If you have conducted your LIA and decided to rely on legitimate interests as

your lawful basis, you should not assume that this is where your responsibilities end." The LIA must be kept under regular review. If anything significant changes — such as the purpose, nature or context of the processing — that may affect the balance between the organisation and the individual, the LIA should be revisited and refreshed as appropriate.

UK GDPR does not define what factors to take into account when deciding if a purpose is a legitimate interest. It could be as simple as it being legitimate to start up a new business activity, or to develop a business. It is not enough, however, simply to say: "We have a legitimate interest in processing customer data", as this does not clarify the purpose or intended outcome. Being more specific about the purpose, could involve saying: "We have a legitimate interest in marketing our goods to existing customers to increase sales."

It hardly needs saying that, whilst any purpose could potentially be relevant, that purpose must be legitimate. Anything unethical or unlawful is not a legitimate interest. For example, although marketing may in general be a legitimate purpose, sending spam emails in breach of electronic marketing rules is most definitely not. Although GDPR does not have an exhaustive list of what purposes are likely to constitute a legitimate interest, its recitals do suggest that the following purposes are valid.

- Fraud prevention.
- Ensuring network and information security.
- Indicating possible criminal acts or threats to public security.

The recitals also say that the following activities may indicate a legitimate interest.

- Processing employee or client data.
- Direct marketing.
- Administrative transfers within a group of companies.

The ICO goes into considerable detail at ico.org.uk about why and how to use an LIA, giving several useful case studies.

Employees' Rights and Duties

Workers, employees, volunteers, job applicants and ex-employees (for convenience, referred to in this section as "employees") have the right to be informed of, and to see, records kept about them, which must be accurate, kept up to date and retained no longer than is necessary. Furthermore, any information must be processed securely, be lawful, fair and transparent. Employees have a right to know the source of any information relating to them personally and how it will be used, including whether it will go to third parties, such as a payroll bureau. They also have the "right to be forgotten" and may request the deletion or removal of personal data where there is no compelling reason for its continued processing. Finally, they have the right to "data portability" which applies to personal data an individual has provided to a data controller,

where the processing is based on the individual's consent or for the performance of a contract; and when processing is carried out by automated means. Employers must provide the data in a structured, commonly used and machine-readable form.

In return, employees must:

- act in accordance with their employer's policy and procedure in handling personal data about others; and
- be aware that serious breaches of data protection rules are a disciplinary offence.

In the event that a dispute over data protection cannot be resolved within the organisation, employees have a right to raise the matter with the data protection supervisory authority (the ICO).

Example of an Employee Data Policy

This organisation aims to fulfil its obligations under UK GDPR to the fullest extent. It has therefore adopted the following policy.

13. Under UK GDPR, employees have the right to access their personal data and supplementary information. They are also allowed to be aware of and to verify the lawfulness of any data processing. Information will be provided without delay and at the latest within one month of receipt of a request.

14. Details of an employee's personal data are available upon request in accordance with the principles of UK GDPR (see paragraph 1, above).

15. Personal data will only be kept for a legitimate purpose. It must also be relevant and limited to what is necessary and must be accurate and kept up to date. Furthermore, it will be processed securely, be lawful, fair and transparent and will only be stored for as long as is necessary.

16. Employees are required to read this information carefully and inform HR@sevacaregroup.com at the earliest opportunity if they believe that any of their personal data are inaccurate or untrue, or if they are dissatisfied with the information in any way.

17. UK GDPR gives data subjects the right to have access to their personal data on request at reasonable intervals. The organisation believes that complying with a request for a copy of the data annually will satisfy this requirement. Should employees wish to request access to their personal data, the request must be addressed to HR@sevacaregroup.com. The request will be judged in the light of the nature of the personal data and the frequency with which they are updated. The employee will then be informed whether or not the request is to be granted. If it is, the information will be provided within one month of the date of the request.

18. In the event of a disagreement between an employee and the organisation regarding personal data, the matter should be taken up under the organisation's formal grievance procedure. This does not negate the individual's right under UK GDPR to complain to the

supervisory authority (the ICO, Information Commissioner's Office).

Additional Clause(s)

19. Where employees make requests for their personal data which are manifestly unfounded or excessive, particularly when these are repetitive. a fee of £tbcwill be charged which must be paid to _____ before a copy of the personal data will be given. This fee is based on the administrative cost of providing the information.

20. In the interests of openness and fairness, the organisation will provide copies of personal records held manually to employees on _____ each year. The procedure which applies to computerised data will apply to such manual files as well as to information held on mobile phones, websites and social media or captured via CCTV.

Note:

In the context of this organisation, personal data may include:

- Names and addresses (with postcodes)*
- Gender*
- Marital status*
- NHS numbers*
- Email addresses*
- Dates of birth*
- Payroll numbers*
- National Insurance numbers*
- Tax, benefit or pensions records*
- Confirmation of Citizenship*
- Languages spoken*
- Trade union membership*
- Biometrics*
- Bank details*
- Disclosure and Barring Service (DBS) information*
- Family contact details*

*delete as appropriate

Controllers and Processors

Under UK GDPR, a controller determines the purposes and means of processing personal data while a processor is responsible for processing personal data on behalf of a controller. Generally speaking, UK GDPR treats the data controller as the principal party for responsibilities such as collecting consent, managing consent-revoking and enabling right to access. Therefore, a data subject who wishes to revoke consent for personal data will contact the data controller to initiate the request, even if such data is stored on servers belonging to the data processor.

UK GDPR places specific legal obligations on processors, including a requirement to maintain records of personal data and processing activities. They must process personal data only on instructions from the controller and must inform the controller if those instructions appear to contravene the regulation. They also have legal liability if they are responsible for a breach. As for the controllers, they must ensure that their contracts with processors comply with UK GDPR. Article 28(1) states: "Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this regulation and ensure the protection of the rights of the data subject."

Data Protection Officers

UK GDPR sets out three circumstances in which it is mandatory to appoint a DPO, specifically if an organisation is:

- a public authority or body (but not a court acting in its judicial capacity); or
- the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects "on a large scale"; or
- the core activities of the controller or processor consist of the processing on a large scale of sensitive data (defined in Article 9 of UK GDPR) or data relating to criminal convictions/offences (defined in Article 10).

An organisation may still decide to appoint a DPO, even if it considers that it does not meet the above criteria. If it is decided that an appointment is unnecessary then it is advisable that the reasoning behind that decision should be documented and retained. It is possible for a group of undertakings to appoint a single DPO provided that that person is easily accessible from each establishment. A single DPO may be designated for several local authorities or other public bodies, taking account of their organisational structure and size.

While the DPO may be an existing employee or externally appointed, they must be independent, an expert in data protection, adequately resourced and report to the highest management level. Their main role is to assist the data processor to monitor internal compliance, inform and advise on their data protection obligations, provide advice regarding data protection impact

assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority (the ICO). The DPO must be easily accessible as a point of contact for employees, individuals and the ICO with contact details readily accessible on the organisation's website and in any relevant publications.

Data Protection Impact Assessments

A DPIA is a process to help data processors and DPOs to identify and minimise the data protection risks of a project. They must be prepared for certain listed types of processing, or any other processing that is likely to result in a high risk to individuals' interests. The main indicators that a DPIA is required are when an organisation intends to:

- use new technologies
- carry out profiling on a large scale
- process personal data in a way which involves tracking individuals' online or offline location or behaviour
- process biometric or genetic data
- systematically monitor publicly accessible places on a large scale
- use systematic and extensive profiling or automated decision-making to make significant decisions about people
- process special category data or criminal offence data on a large scale
- process personal data without providing a privacy notice directly to the individua
- process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them
- combine, compare or match data from multiple sources.

A DPIA should describe the nature, scope, context and purposes of the processing and assess necessity and proportionality. In particular, it must identify and assess risks to individuals and identify any measures to mitigate those risks and protect the data. If the assessment identifies a high risk which the organisation cannot mitigate, the ICO must be consulted. It has stated: "It's important to embed DPIAs into your organisational processes and ensure the outcome can influence your plans. A DPIA is not a one-off exercise and should be seen as an ongoing process, kept under regular review." Even if there is no specific indication of likely high risk, it is, the ICO argues, good practice to do a DPIA for any major new project involving the use of personal data. "You should also think carefully about doing a DPIA for any other processing which is large scale, involves profiling or monitoring, decides on access to services or opportunities, or involves sensitive data or vulnerable individuals," it recommends.

Data Subject Rights

UK GDPR provides eight specific rights for individuals, as follows.

21. The right to be informed.
22. The right of access.
23. The right to rectification.
24. The right to erasure.
25. The right to restrict processing.
26. The right to data portability.
27. The right to object.
28. Rights in relation to automated decision-making and profiling.

Right to be informed

One of the key transparency requirements under UK GDPR is the right of individuals to be informed about the collection and use of their personal data. Data controllers must provide privacy information to individuals at the time they collect the personal data from them. At this point they must tell them: the purposes for processing the personal data; the retention periods for that personal data; and with whom it will be shared. The ICO refers to this collectively as "privacy information". This must be provided within a reasonable period of obtaining the data and no later than one month after doing so. This requirement also applies to personal data collected from other sources as well as directly from the individual concerned.

While the provision of such information may not be necessary if the individual already has it or if its provision would involve a disproportionate effort, where information is provided it must be concise, transparent, intelligible, easily accessible and presented in clear and plain language. Organisations must regularly review, and where necessary, update their privacy information, bringing any new uses of an individual's personal data to their attention before processing starts. As the ICO makes clear, getting this stage done correctly will be the basis for compliance with UK GDPR: getting it wrong can leave an organisation open to fines and lead to reputational damage.

Checklist

The following information should be the basis of any privacy notice.

- The name and contact details of the organisation.
- The name and contact details of its representative (if applicable).
- The contact details of its data protection officer (if applicable).

- The purposes of the processing.
- The lawful basis for the processing.
- The legitimate interests for the processing (if applicable).
- The categories of personal data obtained (if the personal data is not obtained from the individual to whom it relates).
- The recipients or categories of recipients of the personal data.
- The details of transfers of the personal data to any third (non-EU) countries or international organisations (if applicable).
- The retention periods for the personal data.
- The rights available to individuals in respect of the processing.
- The right to withdraw consent (if applicable).
- The right to lodge a complaint with the ICO.
- The source of the personal data (if the personal data is not obtained from the individual to whom it relates).
- The details of whether individuals are under a statutory or contractual obligation to provide the personal data (if applicable, and if the personal data is collected from the individual to whom it relates).
- The details of the existence of automated decision-making, including profiling (if applicable).

Right of access

This right allows individuals to be aware of and verify the lawfulness of the processing by giving them the right to access their personal data and supplementary information. After receiving such a request, the controller must provide a copy of the information free of charge. They may however charge a "reasonable fee" when a request is manifestly unfounded or excessive, particularly if it is repetitive. They may also charge a reasonable fee to comply with requests for further copies of the same information although this does not mean that they can charge for all subsequent access requests. Any fee must be based on the administrative cost of providing the information.

Information must be provided without delay and at the latest within one month of receipt of the request. This compliance period may be extended by a further two months where requests are complex or numerous, provided the individual is notified within one month of the receipt of the request with an explanation of why the time extension is necessary. The same time period (one month) applies if the controller decides not to comply with the request on the ground that it is

"manifestly unfounded or excessive". In such cases, the individual making the request must be informed of their right to complain to the supervisory authority (the ICO) seeking a judicial remedy. If the organisation holds a large quantity of information about an individual, UK GDPR allows it to ask the individual to specify the information to which the request relates.

If the information request is made electronically, the information should be provided in a commonly used electronic format. UK GDPR includes a best practice recommendation that, where possible, organisations should be able to provide remote access to a secure self-service system which would provide the individual with direct access to their information. The ICO recognises that this will not be appropriate for all organisations, but suggests that there are some sectors where it may work well.

Right to rectification

Individuals have the right to ask for inaccurate personal data to be rectified, or to be completed if it is partial. Such a request may be made verbally or in writing and, as with other rights under UK GDPR, controllers have one calendar month to respond. It can be made to any part of the organisation, not specifically to the DPO or other named person. Given that such requests may be made to a range of people within the organisation, it is a point to be borne in mind when arranging training for staff who regularly interact with individuals. The ICO reminds controllers: "Although you may have already taken steps to ensure that the personal data was accurate when you obtained it, this right imposes a specific obligation to reconsider the accuracy upon request." Taking into account the arguments and evidence provided by the data subject, it is the controller's responsibility to take "reasonable steps" to satisfy themselves that the data is accurate and to rectify it if necessary.

With regards to the question of what is reasonable in this context, the ICO suggests that controllers should make a greater effort to rectify inaccurate personal data if it is used to make significant decisions that will affect an individual or others, rather than trivial ones. Determining whether personal data is inaccurate can be more complex if the data refers to a mistake that has subsequently been resolved. It may be possible to argue, the ICO concedes, that the record of the mistake is, in itself, accurate and should be kept. In such circumstances the fact that a mistake was made and the correct information should also be included in the individual's data.

It is also complex if the data in question records an opinion, given that opinions are, by their very nature, subjective, and it can be difficult to conclude that the record of an opinion is inaccurate. As long as the record shows clearly that the information is an opinion and, where appropriate, whose opinion it is, it may be difficult to say that it is inaccurate and needs to be rectified. If the controller is satisfied that the data is accurate, the individual making the request must be informed that the data will not be amended. At the same time, they must be made aware of their right to make a complaint to the ICO or another supervisory authority; and their ability to seek to enforce their rights through a judicial remedy. It is also good practice (the ICO suggests) to place a note on the system indicating that the individual challenges the accuracy of the data

and their reasons for doing so.

If the personal data in question has been disclosed to others, each recipient must be contacted and informed of the rectification or completion of the personal data — unless this proves impossible or involves disproportionate effort. If asked, the controller must also inform the individual about these recipients. UK GDPR defines a recipient as a natural or legal person, public authority, agency or other body to which the personal data are disclosed. The definition includes controllers, processors and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

As with the other rights mentioned above, it is possible for the controller to refuse to comply with a request for rectification if the request is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature. The controller may in such circumstances refuse to deal with the request or may ask for a "reasonable fee" to deal with it. They do not then need to comply with the request until they have received the fee, but must then do so within the usual one month period. (Note, for example, if the organisation receives a request on 30 March, the time limit starts from the next day (31 March) and it has until 30 April to comply with the request. If 30 April falls on a weekend, or is a public holiday, the organisation has until the end of the next working day to comply.)

Right to erasure

This is also known as the right to be forgotten. Individuals may make a request for erasure verbally or in writing and the organisation then has the usual one-month period to respond. It is important to note that the right is not absolute and only applies in the following circumstances.

- The personal data is no longer necessary for the purpose for which it was originally collected or processed.
- The organisation is relying on consent as its lawful basis for holding the data, and the individual withdraws that consent.
- The organisation is relying on legitimate interests as its basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing.
- The organisation is processing the personal data for direct marketing purposes and the individual objects to that processing.
- The personal data has been processed unlawfully.
- It has been processed to offer information society services (ISS) to a child.

On that last point, there is an emphasis on the right to have personal data erased if the request relates to data collected from children. This reflects the enhanced protection of children's information, especially in online environments, under UK GDPR. Therefore, any organisation processing data collected from children must give particular weight to any request for erasure if

the processing of the data is based upon consent given by a child — especially any processing of their personal data on the internet. This is still the case when the data subject is no longer a child, because they may not have been fully aware of the risks involved in the processing at the time of consent.

The right to erasure does not apply if processing is necessary for one of the following reasons.

- To exercise the right of freedom of expression and information.
- To comply with a legal obligation.
- For the performance of a task carried out in the public interest or in the exercise of official authority.
- For archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing.
- For the establishment, exercise or defence of legal claims.

UK GDPR also specifies two circumstances where the right to erasure will not apply to special category data.

29. If the processing is necessary for public health purposes in the public interest (for example, protecting against serious cross-border threats to health, or ensuring high standards of quality and safety of health care and of medicinal products or medical devices).
30. If the processing is necessary for the purposes of preventative or occupational medicine (for example, where the processing is necessary for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or for the management of health or social care systems or services). This only applies where the data is being processed by or under the responsibility of a professional subject to a legal obligation of professional secrecy (eg a health professional).

Checklist (children)

If an organisation is relying on consent as its lawful basis for processing personal data, when offering an online service directly to a child, only those aged 13 or over are able provide their own consent. For children under this age — unless the online service on offer is a preventive or counselling service — the data controller needs to get consent from whoever holds parental responsibility for the child. Children have the same rights as adults over their personal data including: the rights to access their personal data; request rectification; object to processing; and have their personal data erased. In this context, organisations should ensure that they comply with the following points.

- This organisation complies with all the requirements of UK GDPR, not just those specifically relating to children and included in this checklist.
- It designs its processing with children in mind from the outset, and uses a data protection

by design and by default approach.

- It makes sure that processing is fair and complies with the data protection principles.
- As a matter of good practice, it uses DPIAs to help to assess and to mitigate the risks to children.
- If processing is likely to result in a high risk to the rights and freedom of children then a DPIA is considered mandatory.
- As a matter of good practice, this organisation consults with children (where appropriate) when designing its processing.
- When relying on consent, this organisation ensures that the child understands what they are consenting to, and it does not exploit any imbalance in power in the relationship between it and the child.
- When the legal basis is "necessary for the performance of a contract", it considers the child's competence to understand what they are agreeing to, and to enter into a contract.
- When relying upon "legitimate interests", this organisation takes responsibility for identifying the risks and consequences of the processing, and puts age appropriate safeguards in place.
- When offering ISS to UK children on the basis of consent, it makes reasonable efforts (taking into account the available technology and the risks inherent in the processing) to ensure that anyone who provides their own consent is at least 13 years old.
- When targeting wider European markets, it complies with the age limits applicable in each Member State.

Right to restrict processing

Individuals have the right to request the restriction or suppression of their personal data, although this is not an absolute right and only applies in certain circumstances. When processing is restricted, controllers are permitted to store the personal data, but not use it. An alternative to individuals requesting the erasure of their data, restriction may be because the person concerned contests the accuracy of their personal data and the data controller needs to verify its accuracy. In most cases, the ICO suggests, controllers will not be required to restrict an individual's personal data indefinitely, but will need to have the restriction in place for a certain period of time. In certain circumstances, the individual may have objected to their data being processed and the controller will have to consider whether its legitimate grounds override those of the person concerned.

In any event, controllers will need to have processes in place that enable them to restrict personal data if required. It is important to note that the definition of processing includes a broad range of operations including collection, structuring, dissemination and erasure of data. Therefore, organisations need to use methods of restriction that are appropriate for the type of

processing they are carrying out. This could involve: temporarily moving the data to another processing system; making the data unavailable to users; or temporarily removing published data from a website. According to the ICO: "If you are using an automated filing system, you need to use technical measures to ensure that any further processing cannot take place and that the data cannot be changed whilst the restriction is in place. You should also note on your system that the processing of this data has been restricted."

Checklist

With regard to requests for restriction, the organisation should ensure that it can comply with the following points.

- This organisation knows how to recognise a request for restriction and understands when the right applies.
- It has a policy in place for how to record requests received verbally.
- It understands when a request may be refused and is aware of the information to be provided to individuals in such circumstances.
- This organisation has processes in place to ensure that it responds to a request for restriction without undue delay and within one month of receipt. It is aware of the circumstances when this time limit can be extended.
- It has appropriate methods in place to restrict the processing of personal data on its systems and to indicate on those systems that further processing has been restricted.
- It understands the circumstances when it is possible to process personal data that has been restricted and is aware that it must tell individuals before such a restriction on processing is lifted.
- This organisation will not process restricted data in any way except to store it unless: it has the individual's consent; it is for the establishment, exercise or defence of legal claims; it is for the protection of the rights of another person; or is for reasons of important public interest.

Right to data portability

The right to data portability only applies:

- to personal data an individual has provided to a controller
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

Under this right, individuals must be able to move, copy or transfer personal data easily from

one IT environment to another in a safe and secure way, without hindrance to usability. The aim is to allow them to obtain and reuse their personal data for their own purposes across different services. The ICO notes that some organisations in the UK already offer data portability through the midata and similar initiatives which allow individuals to view, access and use their personal consumption and transaction data in a way that is portable and safe.

The requested information must be provided free of charge in a structured, commonly used and machine-readable form. Open formats include CSV files. Machine-readable means that the information is structured so that software can extract specific elements of the data enabling other organisations to use the data. Requests must be satisfied within the usual one-month time limit although this may be extended by two months where the request is complex or a number of requests are received. The individual must in any event be informed within one month of the receipt of the request and told why the extension is necessary.

As with previous rights, if a request is rejected, the individual must receive and explanation, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month. If the individual requests it, an organisation be required to transmit the data directly to another organisation if this is technically feasible. However, there is no compulsion on data controllers to adopt or maintain processing systems that are technically compatible with other organisations. Finally, if the personal data concerns more than one individual, consideration must be given to whether providing the information will prejudice the rights of any other person.

Right to object

According to UK GDPR, this right must be "explicitly brought to the attention of the data subject and be presented clearly and separately from any other information." Individuals must therefore be informed of their right to object "at the point of first communication" and in an organisation's privacy notice. They have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling)
- direct marketing (including profiling)
- processing for purposes of scientific/historical research and statistics.

However, individuals must object on "grounds relating to their particular situation". The data controller must then stop processing the personal data unless they can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual. Alternatively, they must be able to show that the processing is for the establishment, exercise or defence of legal claims. They must stop processing personal data for direct marketing purposes as soon as an objection is received: there are no exemptions or grounds to refuse such a request. If processing activities are carried out online, the organisation concerned must offer a way for individuals to object online.

Rights in relation to automated decision-making and profiling

Making a decision solely by automated means without any human involvement is covered by UK GDPR as is profiling (automated processing of personal data to evaluate certain things about an individual). Article 22 introduces additional rules to protect individuals if an organisation is carrying out solely automated decision-making that has legal or similarly significant effects on them. Organisations can only carry out this type of decision-making where the decision is:

- necessary for the entry into or performance of a contract
- authorised by EU or Member State law applicable to the controller
- based on the individual's explicit consent.

It is for the data controller to identify whether any of its processing falls under Article 22 and, if so, must ensure that it:

- gives individuals information about the processing
- introduces simple ways for them to request human intervention or challenge a decision
- must carry out regular checks to make sure that the systems are working as intended.

Checklists

With regard to all automated individual decision-making and profiling, a compliant organisation must:

- have a lawful basis to carry out profiling and/or automated decision-making and document this in its data protection policy
- send individuals a link to its privacy statement when it has obtained their personal data indirectly
- explain how people can access details of the information used to create their profile
- tell people who provide it with their personal data how they can object to profiling, including profiling for marketing purposes.
- put in place procedures for customers to access the personal data input into the profiles so they can review and edit for any accuracy issues
- have additional checks in place for profiling/automated decision-making systems to protect any vulnerable groups (including children)
- only collect the minimum amount of data needed and have a clear retention policy for the profiles it creates.

With regard to solely automated individual decision-making, including profiling with legal or similarly significant effects (Article 22), a compliant organisation must:

- carry out a DPIA to identify the risks to individuals, show how it is going to deal with them and what measures it has in place to meet UK GDPR requirements
- carry out processing under Article 22(1) for contractual purposes and can demonstrate why it is necessary

or

- carry out processing under Article 22(1) because it has the individual's explicit consent recorded. The organisation can show when and how it obtained consent and tells individuals how they can withdraw consent with have a simple way for them to do so

or

- carry out processing under Article 22(1) because the organisation is authorised or required to do so. This is the most appropriate way to achieve its aims
- show that it does not use special category data in its automated decision-making systems unless it has a lawful basis to do so, and can demonstrate what that basis is. Any special category data accidentally created is deleted
- explain that it uses automated decision-making processes, including profiling, and explain what information is used, why it is used and what the effects might be
- show that there is a simple way for people to ask the organisation to reconsider an automated decision
- identify staff in the organisation who are authorised to carry out reviews and change decisions
- show that its systems are regularly checked for accuracy and bias and that any changes are fed back into the design process.

Article 22(1) states: "The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."

Disaster prevention and recovery

One of the six data protection principles mentioned above states that processing must take place in a way 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. The ICO states: "You can consider the state of the art and costs of implementation when deciding what measures to take — but they must be appropriate both to your circumstances and the risk your processing poses." These measures must also enable the organisation to restore access and availability to personal data in a timely manner in the event of a physical or technical incident. Remember that while information security is sometimes considered as cybersecurity (the protection of your networks and information systems from attack), it also covers other things like physical and organisational

security measures.

In the event of a data breach or other problem that is likely to result in a risk to the rights and freedoms of individuals, the people affected must be informed as soon as possible and the ICO must be notified within 72 hours. It requires organisations to have the ability to restore the availability and access to personal data in the event of a physical or technical incident in a "timely manner". While UK GDPR does not define a "timely manner", the ICO argues that it depends on: what systems the organisation has and the risk that may be posed to individuals if the personal data it processes is unavailable for a period of time.

Checklist

To ensure compliance in this area, an organisation should:

- undertake an analysis of the risks presented by its processing, and use this to assess the appropriate level of security which it needs to put in place
- when deciding what measures to implement, take account of the state of the art and costs of implementation
- have an information security policy (or equivalent) and take steps to make sure the policy is implemented
- where necessary, have additional policies and ensure that controls are in place to enforce them
- ensure that it regularly reviews its information security policies and measures and, where necessary, improve them
- have in place basic technical controls such as those specified by established frameworks such as Cyber Essentials
- accept that it may also need to put other technical measures in place depending on its circumstances and the type of personal data it processes
- use encryption and/or pseudonymisation where it is appropriate to do so
- understand the requirements of confidentiality, integrity and availability for the personal data it processes
- ensure that it can restore access to personal data in the event of any incidents, such as by establishing an appropriate backup process
- conduct regular testing and reviews of its security measures to ensure they remain effective, and act on the results of those tests where they highlight areas for improvement
- where appropriate, implement measures that adhere to an approved code of conduct or certification mechanism

- ensure that any data processor it uses also implements appropriate technical and organisational measures.

Subject access requests

The ICO has recognised that there is a lack of clarity with regard to subject access requests (SARs) that has left employers confused as to what, for example, constitutes a manifestly excessive request and what is a reasonable fee. Having consulted on these questions, and received over 350 responses from organisations of all sizes and sectors, the ICO produced detailed guidance on the right of access and SARs. As well as the two points detailed above, this examines a problem raised by a number of respondents — what happens if it is not possible to satisfy a request within the stated time limits? The full guidance can be found at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/right-of-access: the main points are summarised below.

Manifestly excessive SARs

Before refusing a request on this ground, it is necessary to consider whether the request is proportionate when balanced with the burden or costs involved in dealing with it. The ICO emphasises that a request is not necessarily excessive just because the individual requests a large amount of information. Employers must take into account:

- the nature of the requested information
- the context of the request, and the relationship with the individual
- whether a refusal to provide the information or even acknowledge that it is held may cause substantive damage to the individual
- the available resources
- whether the request largely repeats previous requests without a reasonable interval having elapsed
- whether it overlaps with other requests (although if it relates to a completely separate set of information it is unlikely to be excessive).

This section of the guidance goes on to look at specific exemptions from having to comply with SARs and how they work as well as general considerations to be taken into account. For example, each request must be considered individually: it is not possible to have a blanket policy.

Manifestly unfounded SARs

A request may be manifestly unfounded if:

- the individual clearly has no intention to exercise their right of access. For example, they make a request, but then offer to withdraw it in return for some form of benefit from the organisation
- the request is malicious in intent and is being used to harass an organisation with no real

purpose other than to cause disruption

- it targets a particular employee against whom the requester has some personal grudge
- it makes unsubstantiated accusations against the organisation or specific employees which are clearly prompted by malice.

Note that the ICO states: "Whilst aggressive or abusive language is not acceptable, the use of such language does not necessarily make a request manifestly unfounded."

Stopping the clock

Having been asked about complicated requests that potentially cannot be answered within the 30-day time limit, the ICO has clarified that its position now is that, in certain circumstances, the clock can be stopped whilst organisations are waiting for the requester to clarify their request.

Reasonable fee

In most cases, the ICO makes clear, no fee should be charged when complying with a SAR. However, exceptions to this rule are possible if the request is manifestly unfounded or excessive, or an individual requests further copies of their data following a request.

A "reasonable fee" may include the costs of:

- photocopying, printing, postage and any other costs involved in transferring the information to the individual (eg the costs of making the information available remotely on an online platform)
- equipment and supplies (eg discs, envelopes or USB devices)
- staff time.

The costs of staff time should be based on the estimated time it will take staff to comply with the specific request, charged at a reasonable hourly rate.

As fees should be calculated in a reasonable, proportionate and consistent manner, the ICO suggests that it would be good practice to establish an unbiased set of criteria for charging fees which explains:

- the circumstances in which a fee is charged
- the standard charges (including a costs breakdown where possible eg the costs per A4 photocopy)
- how the fee is calculated — explaining the costs taken into account including the costs of staff time.

Data Protection Fees

Available at www.legislation.gov.uk, the Data Protection (Charges and Information) Regulations 2018 (SI 2018 No. 480) replaces the previous regime set out under the Data Protection

(Notification and Notification Fees) Regulations 2000. The new regulations set out the circumstances in which data controllers are required to pay a charge, and provide information, to the Information Commissioner from 25 May 2018. In short, data controllers will have to pay an annual charge to the Commissioner unless all their processing of personal data is exempt. Exemptions may be allowed, among other reasons, if: the processing is non-automated; or it is undertaken for the purposes of personal, family or household affairs; or it is for the purpose of the maintenance of a public register; or it is for the purposes of advertising, marketing and public relations in respect of the data controller's own activities.

Within the first 21 days of each charge period data controllers must provide their staff total (10 or fewer, 11 to 250 or 251+) to the Information Commissioner. They must also give turnover details (less than or equal to £632,000, greater than £632,000 but less than or equal to £36 million, or above £36 million). According to criteria relating to a data controller's turnover and number of members of staff (or only members of staff, for a public authority), three tiers of charge are laid down: £40, £60 and £2900. the ICO has produced *The Data Protection Fee: A Guide for Controllers* which is available at ico.org.uk. This makes clear that a data controller is breaking the law if they process personal data, or is responsible for the processing of personal data, for any of the non-exempt purposes and has either not paid a fee, or not paid the correct amount. The maximum penalty is a £4350 fine (150% of the top tier fee).

Data Protection after the Transition Period

The UK formally left the EU at the end of January 2020 but remained subject to European law during a transition period which ended on 31 December 2020. During this period there were no changes to the UK's data protection standards. EU data protection laws, including the GDPR, have continued to apply, alongside the Data Protection Act 2018, and the Information Commissioner remains the UK's independent supervisory authority on data protection.

Moreover, after the end of the transition period, the UK GDPR as introduced by way of retained EU law and continues to be read alongside the Data Protection Act 2018, with technical amendments (by way of Schedule 1 of the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019) to ensure it can function in UK law. The Government has stressed that the UK remains committed to high data protection standards.

Since 1 January 2021, organisations have needed to have Standard Contractual Clauses (SCCs) in place with EU counterparts in order to legally receive personal data from the EU. The European Commission has been carrying out a data adequacy assessment of the UK which would allow for the free flow of personal data from the EU/EEA to the UK to continue without any further action by organisations (the European Economic Area (EEA) includes Iceland, Liechtenstein and Norway).

As the EU had not made adequacy decisions in respect of the UK before the end of the transition

period, however, organisations have needed to ensure that they can continue to lawfully receive personal data from EU/EEA businesses (and other organisations) in the future. They have had to put in place alternative transfer mechanisms to ensure that data can continue to legally flow from the EU/EEA to the UK. For most organisations, the most relevant of these have been SCCs as mentioned above. Further details on this possibility, including an interactive tool that allows an organisation to build SCCs, can be found at https://ico.org.uk/for-organisations/data-protection-at-the-end-of-the-transition-period. Some UK data controllers and processors have had to appoint EU-based representatives from 1 January 2021. Further information is available from the ICO helpline on 0303 123 1113 or at https://ico.org.uk/for-organisations/data-protection-at-the-end-of-the-transition-period/data-protection-at-the-end-of-the-transition-period/the-gdpr/european-representatives.

It should be noted that the European Commission has published, in June 2021, the final version of new Standard Contractual Clauses (New SCCs) (see https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en for more details). These will be required for transfers of European personal data to any "non-adequate" countries outside the EU / EEA, such as the United States or India. The ICO has announced that it will publish its own UK SCCs for international data transfers of UK personal data. It may also recognise the validity of the EU's New SCCs for such transfers.

EU data adequacy decision

As mentioned above, the European Commission has been carrying out a data adequacy assessment of the UK which is now regarded by the EU as a "third country" which must demonstrate that its data protection rules comply with EU standards. As the UK has essentially adopted the GDPR in full, this would seem to be a relatively easy exercise but it has still taken several months to complete.

On 2 June, the European Parliament asked the Commission to modify its draft decisions on whether or not UK data protection is adequate to bring them into line with the latest EU court rulings and to respond to concerns raised by the European Data Protection Board (EDPB) in its recent opinions. The EDPB considers that UK bulk access practices, onward transfers and its international agreements need to be clarified further. The European Parliament resolution states that, if the Commission's implementing decisions are adopted without changes, national data protection authorities should suspend transfers of personal data to the UK when indiscriminate access to personal data is possible.

MEPs said that they accepted that the UK's basic data protection framework is similar to that of the EU, but raised concerns about the way it had been implemented. In particular, the UK regime contains exemptions in the fields of national security and immigration, which now also apply to EU citizens wishing to stay or settle in the UK. Current UK legislation also allows for bulk data to

be accessed and retained without a person being under suspicion for perpetrating a crime, and the EU court has found indiscriminate access to be inconsistent with the GDPR.

The European Parliament also expressed concerns about onward data transfers. The UK's data-sharing agreements with the United States mean EU citizens' data could be shared with the US, despite recent rulings of the EU's Court of Justice (CJEU) that found US practices of bulk data access and retention were incompatible with the GDPR.

However, on 18 June 2021, the European Council passed the Data Adequacy agreement approving the UK as having adequate data protection for the transfer of personal data. This means that the European Commission is likely to finalise its adequacy decisions in July.

Legacy data

The Withdrawal Agreement signed by the EU and the UK Government contains provisions that apply EU data protection law (in its end of the transition period state) to certain "legacy" personal data if the UK has not been granted full adequacy decisions by the end of the transition period. "Legacy data" includes personal data of individuals outside the UK processed in the UK prior to the end of the transition period, or subsequently on the basis of the Withdrawal Agreement. See https://ico.org.uk/for-organisations/data-protection-at-the-end-of-the-transition-period/information-rights-at-the-end-of-the-transition-period-frequently-asked-questions.

International Transfers

GDPR imposes restrictions on the transfer of personal data to what the EU calls third countries (those outside the Union) or to international organisations. Personal data may only be transferred outside of the EU in compliance with the conditions for transfer set out in Chapter V of GDPR. This states:

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this regulation is not undermined.

GDPR limits an organisation's ability to transfer personal data outside the EU where this is based only on its own assessment of the adequacy of the protection afforded to the personal data. Data controllers should look to rely on one of the following.

- Standard data protection clauses in the form of template transfer clauses adopted by the European Commission.
- Binding corporate rules (agreements governing transfers made between organisations within a corporate group).
- Compliance with an approved code of conduct approved by a supervisory authority.

- Certification under an approved certification mechanism.
- Provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority.

GDPR does, however, provide derogations from the general prohibition on transfers of personal data outside the EU for certain specific situations. These include where the transfer is:

- made with the individual's informed consent
- necessary for the performance of a contract between the individual and the organisation or for pre-contractual steps taken at the individual's request
- necessary for the performance of a contract made in the interests of the individual between the controller and another person
- necessary for important reasons of public interest
- necessary to protect the vital interests of the data subject or other persons, where the data subject is physically or legally incapable of giving consent
- made from a register which under UK or EU law is intended to provide information to the public (and which is open to consultation by either the public in general or those able to show a legitimate interest in inspecting the register).

The European Commission, which has the power to determine whether a country outside the EU offers an adequate level of data protection, has so far recognised Andorra, Argentina, Canada (commercial organisations only), the Faroe Islands, Guernsey, Israel, the Isle of Man, Japan (private-sector organisations only), Jersey, New Zealand, Switzerland and Uruguay in this regard. Most agreed to maintain unrestricted personal data flows with the UK after 31 December 2020 (for more details, see https://ico.org.uk/for-organisations/data-protection-at-the-end-of-the-transition-period/data-protection-at-the-end-of-the-transition-period/the-gdpr/international-data-transfers).

Privacy Shield

On 16 July 2020 the Court of Justice of the European Union (CJEU) invalidated the EU-US Privacy Shield adequacy decision with immediate effect in the Schrems II case, meaning this framework can no longer be relied upon for personal data transfers to businesses and organisations in the United States. The judgment upheld that EU standard contractual clauses (SCCs) remain a valid tool for the international transfer of personal data but only where they (together with any additional measures) provide for "essentially equivalent" protection as in the EU.

During the transition period, EU data protection law applies to the UK, and the Schrems II judgment and EU adequacy decisions are therefore binding on transfers of data leaving the UK. Further information on this issue can be found at https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/07/updated-ico-statement-on-the-judgment-of-the-european-court-of-justice-in-the-schrems-ii-case.

Codes of Conduct and Certification

As there is still little indication of how the ICO will police the requirements of UK GDPR, it is only possible to offer general compliance advice. For example, it seems certain that any investigation of a potential breach will involve examining an organisation's records so it clearly makes sense to document each step of the data gathering and processing undertaken by an organisation in order to be able to demonstrate clear evidence of good practice.

Similarly, it should be noted that the ICO has said: "The GDPR endorses the use of approved codes of conduct and certification mechanisms to demonstrate that you comply." While signing up to a code of conduct or certification scheme is not obligatory, therefore, where such codes or schemes are created, and assuming they cover the processing activity carried out by an organisation, there would seem to be a strong argument for considering membership as a way of demonstrating general compliance. Codes must be approved by the relevant supervisory authority. Joining will also be a serious matter: an infringement could lead to a member being excluded and the supervisory authority being informed. There will also be the risk of a fine of up to €10 million or 2% of the organisation's global turnover.

A certification mechanism is another way of demonstrating compliance, in particular showing that an organisation is implementing technical and organisational measures. A certification mechanism may also be established to demonstrate the existence of appropriate safeguards related to the adequacy of data transfers. They are intended to allow individuals to quickly assess the level of data protection of a particular product or service. Any certification will be valid for a maximum of three years and can be withdrawn if a member no longer meets the requirements of the certification. As with codes, the supervisory authority will be notified in such cases and the organisation involved risks a fine of up to €10 million or 2% of its global turnover.

Failure to Comply

The fact about UK GDPR which first caught the headlines was the new power of the ICO to fine non-compliant organisations a maximum of €20 million (c£17 million) or 4% of global turnover. However, Information Commissioner Elizabeth Denham has stressed: "It's scaremongering to suggest that we'll be making early examples of organisations for minor infringements or that maximum fines will become the norm." Pointing out that her organisation has always preferred the carrot to the stick, she said that its commitment to guiding, advising and educating organisations about how to comply with the law would not change under UK GDPR.

Ms Denham also highlighted that, in 2016/17, the ICO concluded 17,300 cases with only 16 of them resulting in fines for the organisations concerned. While heavy fines for serious breaches reflect the importance of personal data, she concluded that predictions of massive fines under GDPR were nonsense and this seems to have been borne out thus far. Just as with the DPA, the new rules provide a suite of sanctions to help organisations comply, including warnings,

reprimands, imposing a temporary or permanent ban on data processing and corrective orders. However while these may not hit organisations in the pocket, the extent of reputational damage must not be underestimated.

It should also be noted that, in October 2020, the ICO fined British Airways (BA) £20 million for failing to protect the personal and financial details of more than 400,000 of its customers. An ICO investigation found the airline was processing a significant amount of personal data without adequate security measures in place. This failure broke data protection law and, subsequently, BA was the subject of a cyber-attack during 2018, which it did not detect for more than two months.

National Data Opt-Out Policy

From 31 July 2022, all regulated social care providers in England must comply with the national data opt-out policy. This enables service users to stop use of their data for anything other than individual care, for example research or planning purposes, in line with the recommendations from the National Data Guardian in her *Review of Data Security, Consent and Opt-Outs* (2018).

National data opt-out applies to adult care homes/adult social care services including care arranged or provided by local authorities and adult social care providers, where regulated by the Care Quality Commission (CQC), and domiciliary services and private providers, funded or arranged by a public body, usually local authority. It does not apply to data from the devolved nations: Scotland, Wales, Northern Ireland, the Republic of Ireland or private patients treated in independent hospitals.

If a service user has opted out of sharing their data and the care organisation does use confidential patient information for planning or research purposes, it must comply. When organisations complete the Data Security and Protection Toolkit, they should include how national data opt-out information has been shared with service users and applied in practice.

Service users should be informed of how they can opt out. As national data opt-outs are set or changed by individuals themselves, this must be done by the service user or someone legally able to act on their behalf. They or their advocate can be directed to www.nhs.uk/your-nhs-data-matters/ or call 0300 303567.

There are some exceptions to data opt-out where there is a legal mandate/direction or overriding public interest such as pandemic situations. Data submitted to the Capacity Tracker as outlined in DHSC *Admission and Care of Residents in a Care Home During COVID-19* are not in scope of the national data opt-out.

Requirements to apply national data opt-out have been waived by the Secretary of State for Health and Care for invoice validation purposes and any payment flows not reliant on Regulation 5 support are not presently included in national data opt-out.

For more information, see NHS Digital.

Data Protection Law and Coronavirus Testing

Data protection law when carrying out tests

As employers will process information that relates to an identified or identifiable individual, they need to ensure compliance with UK GDPR and the Data Protection Act 2018. Any personal data that relates to health is classed as "special category data".

While the law does not prevent employers from taking steps to keep both their staff and public safe during the coronavirus crisis they still need to be responsible with personal data.

Lawful basis for testing employees

Provided there is a good reason for taking this action, employers are able to process health data that concerns Covid-19. The lawful basis of "legitimate interests" is likely to be appropriate but all employers should make their own assessment for their own company. For more information for determining a lawful basis for processing HR data, refer to our "How to" guide.

As health data has the protected status of "special category data" (see above), employers must also identify an Article 9 condition for processing it. This condition covers the majority of what employers need to do in this situation, provided they are not collecting or sharing any data that is unnecessary.

Ensuring compliance with data protection law

Employers will need to use the accountability principle when processing test data. In effect, this means they are responsible for UK GDPR compliance and must be able to demonstrate their compliance, which can involve additional record-keeping requirements.

One way of demonstrating this accountability is conducting a data protection impact assessment. This should establish:

- activity proposed
- data protection risks
- whether the proposed activity is necessary and proportionate
- the mitigating actions that can be put in place to counter the risks
- a plan or confirmation that mitigation has been effective.

An initial assessment should be regularly reviewed and updated.

Collecting appropriate amounts of data

It is important that employers only collect and retain the minimum amount of information needed in order to fulfil the purpose. All data collected should:

- be enough to fulfil the purpose

- have a rational link to that purpose
- not be more than needed for that purpose.

For example, employers will probably only require test results, rather than any other details considering underlying conditions.

It is important to note the date of test results as the health status of individuals change over time.

Keeping lists of staff who have symptoms or have been tested as positive

While employers can keep lists of this information, they need to make sure the data is necessary and relevant for the stated purpose. Data processing should be secure and consider any duty of confidentiality owed to their staff.

These lists must not result in any unfair or harmful treatment of employees. Information on staff who have reported symptoms should not be retained for purposes that staff would not reasonably expect.

Informing staff of data processing

It is important to be clear, open and honest with staff and clearly communicate why the company wishes to use their personal data. It should also be made clear what decisions will be made with information on positive test results, or testing for those with symptoms.

Before any tests are carried out, staff should be informed what personal data is required, what it will be used for and with whom it will be shared. The period the data will be kept should also be made clear. It is advisable to discuss the collection of this data with employees to provide them with the opportunity to bring forward any concerns they may have.

Disclosing positive test results to third parties

Staff should be informed of positive test results, but, if possible, employers should avoid identifying individuals.

Data protection law does not prevent employers from ensuring the health and safety of its employees and employers should consider routes available to share data as outlined in the law. It should also be considered that there may be risks to the wider public by not sharing test information.

Ensuring staff are able to exercise their information rights

In order for staff to exercise their rights, they need to fully understand what personal data is held by the company and what it is being used for. Employers should therefore consider if they need to put processes or systems in place.

An example given by the ICO is in relation to the right of access, which is also known as Subject Access. Employers could consider setting up portals or self-service systems which allow staff to

manage and update their personal data where appropriate.

If this is not possible, employers should still ensure that basic policies and procedures are in place to allow employee data to be available when required.

Data protection considerations when staff disclose test results

Employers should have due regard to the security of this data and consider any duty of confidentiality owed to individuals who voluntarily disclose test results.

Using temperature checks or thermal cameras on site

As taking this action is technically considered using intrusive technologies, especially for capturing health information, employers must give specific thought to the purpose and context of its use. All staff monitoring needs to be necessary and proportionate and it is essential to remain transparent.

It should also be considered whether the same results could still be achieved through less intrusive needs. If so, the monitoring may not be considered proportionate.

Useful Contacts

Information Commissioner's Office (ICO)

European Commission (data protection)

Article 29 Working Party

Representatives of the national data protection authorities (DPAs) in the EU Member States co-operate through the Article 29 Working Party (WP29) to produce guidance in this area. It has been publishing Opinions, reports and guidance since 1997, some of which relate to GDPR.

European Data Protection Board

European Data Protection Supervisor

List of Relevant Legislation

- Data Protection Act 2018
- Data Protection (Charges and Information) Regulations 2018
- General Data Protection Regulation (GDPR)
- Law Enforcement Directive
- Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019