Guide to Data Subject Rights, including Subject Access Requests and the Right to be Forgotten

1. Data protection laws

1.1 The Data Protection Act 1998 ("**DPA**") applies to any personal data that you process, and from 25th May 2018 this will be replaced by the General Data Protection Regulation (**GDPR**) and the Data Protection Act 2018 ("**DPA 2018**") (together "**data protection laws**") and then after Brexit the UK will adopt laws equivalent to these data protection laws.

1.2 This Guide is written as though GDPR and the DPA 2018 are both in force, i.e. it states the position as from 25th May 2018.

1.3 The data protection laws give individuals rights to access, correct and control how you use their personal data.

2. Key words in relation to data protection

2.1 The following are key terms that are commonly used in relation to data protection:

2.1.1 **Personal data** is data that relates to a living individual who can be identified from that data (or from that data and other information in or likely to come into our possession). That living individual might be an employee, member, coach, athlete, supplier, contractor or contact, and that personal data might be written, oral or visual (e.g. CCTV or photos).

2.1.2 **Identifiable** means that the individual can be distinguished from a group of individuals (although the name of that individual need not be ascertainable). The data might identify an individual on its own (e.g. a name or video footage) or might do if taken together with other information available to or obtainable by you (e.g. a job title and company name might give away the name of the individual if there is only one person in that business with that job title.).

2.1.3 **Data subject** is the living individual to whom the relevant personal data relates.

2.1.4 **Processing** is widely defined under the data protection laws and generally any action taken by you in respect of personal data will fall under the definition, including for example collection, modification, transfer, viewing, deleting, holding, backing up, archiving, retention, disclosure or destruction of personal data, including CCTV images.

2.1.5 **Data controller** is the person who decides how personal data is used, for example your organisation will always be a data controller in respect of personal data relating to your employees.

2.1.6 **Data processor** is a person who processes personal data on behalf of a data controller and only processes that personal data in accordance with instructions from the data controller, for example an outsourced payroll provider will be a data processor. An external assessor or examiner may also be a data processor

3. Data subject rights

3.1 Individuals have certain rights under the data protection laws (**Rights**). These are:

3.1.1 the right of access (also known as a data subject access request) (***see paragraph 7)***;

3.1.2 the right to erasure (also known as the right to be forgotten) (***see paragraph 0)***;

3.1.3 the right to rectification ***(see paragraph 9);***

3.1.4 the right to restrict processing ***(see paragraph 10);***

3.1.5 the right to data portability ***(see paragraph 11);***

3.1.6 the right to object ***(see paragraph 12);*** and

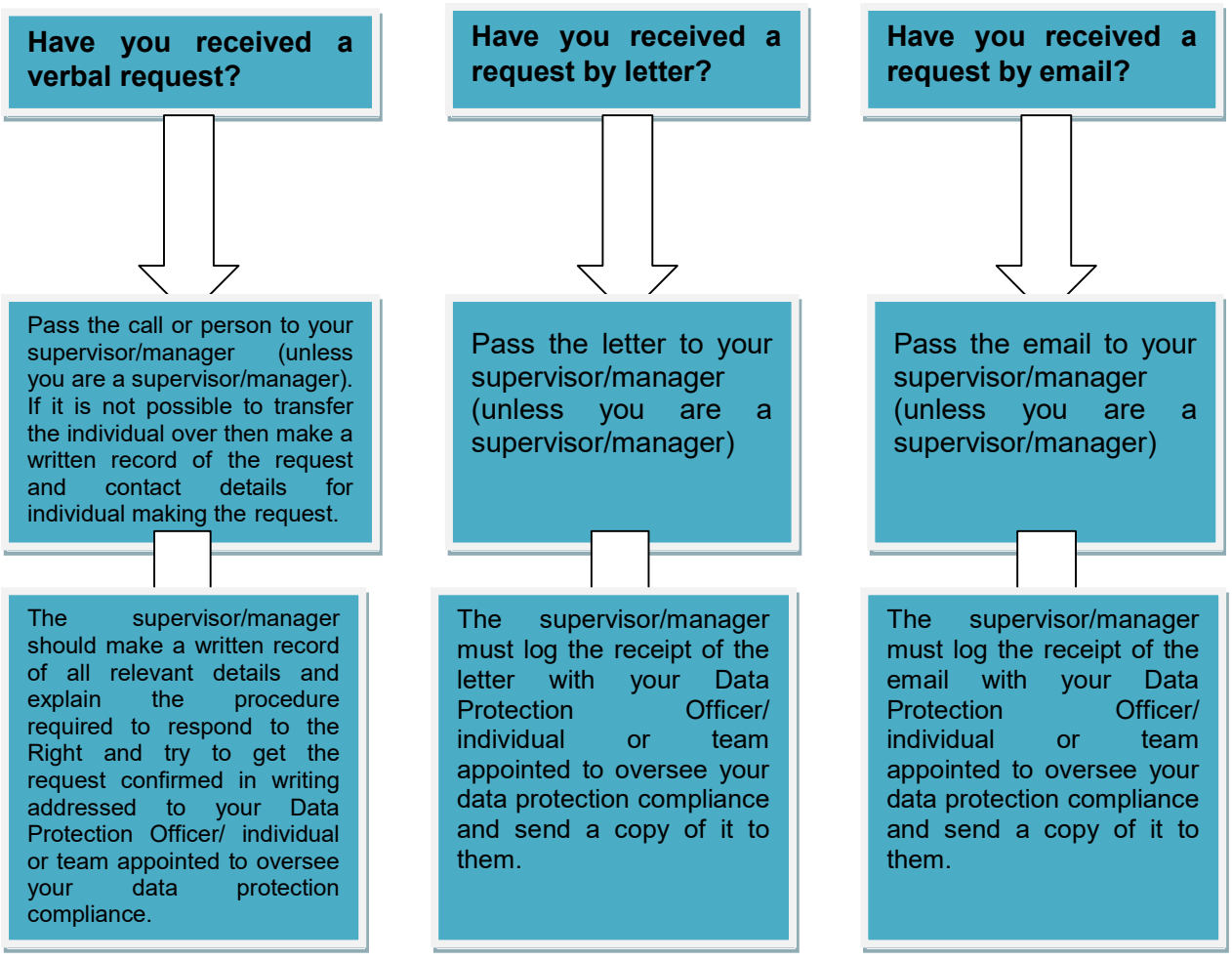
3.1.7 rights in relation to automated decision making and profiling ***(see paragraph 13).***

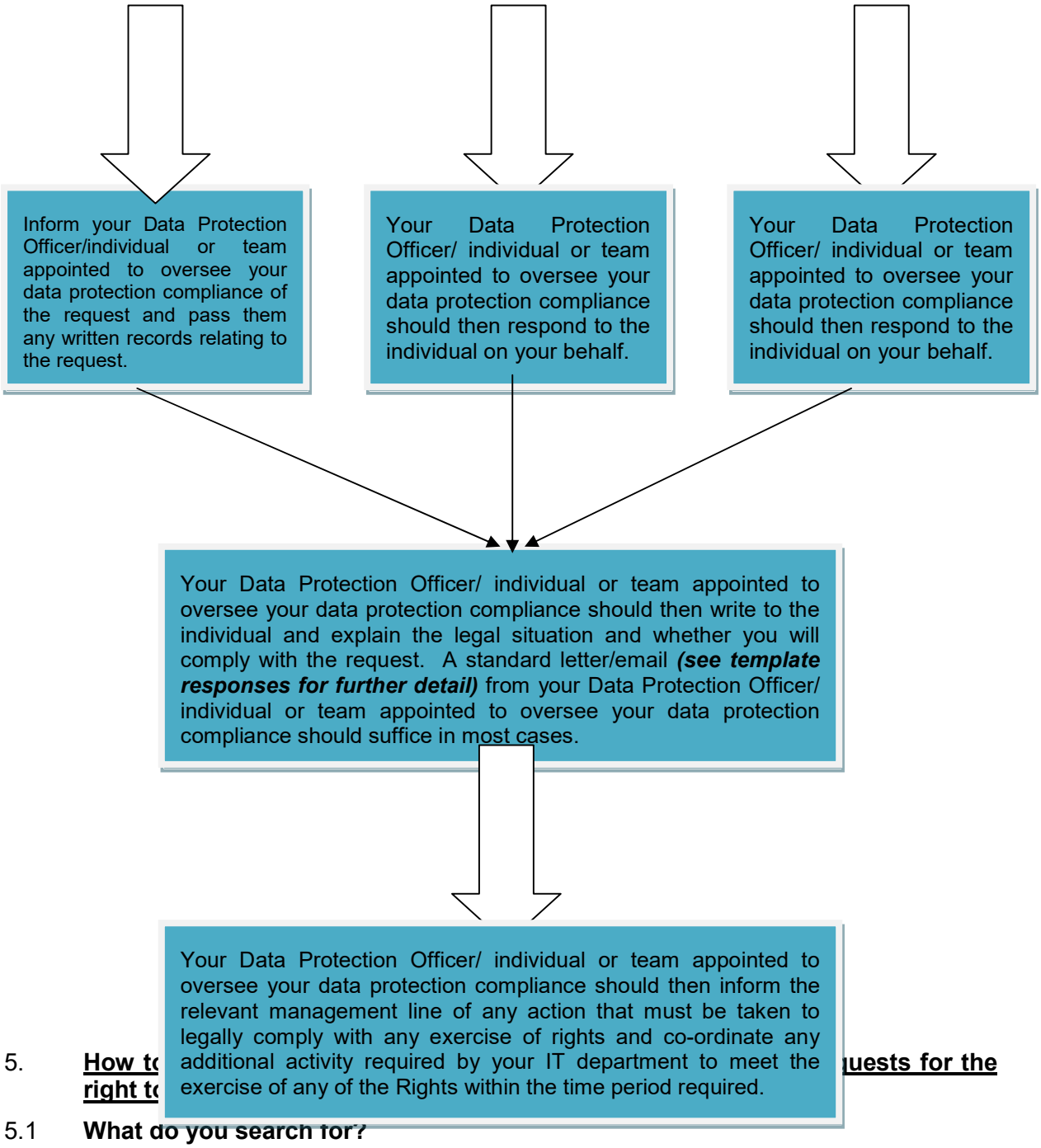
3.2 The exercise of these Rights may be made in writing, including email, and also verbally and should be responded to in writing by you (if you are the relevant data controller) without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. You must inform the individual of any such extension within one month of receipt of the request, together with the reasons for the delay.

3.3 Where the data subject makes the request by electronic means, any information is to be provided by electronic means where possible, unless otherwise requested by the individual.

3.4 If you receive the request from a third party (e.g. a legal advisor), you must take steps to verify that the request was, in fact, instigated by the individual and that the third party is properly authorised to make the request. This will usually mean contacting the relevant individual directly to verify that the third party is properly authorised to make the request.

4. **Notification and response procedure**





5. **How to ... quests for the right to**

5.1 **What do you search for?**

5.1.1 You should conduct a reasonable search of the relevant systems using the individual's name, employee or membership number, address, national insurance number, telephone number, email address or other information specific to that individual. In each case the scope of the search may be different, and you should check with your Data Protection Officer/ individual or team appointed to oversee your data protection compliance before commencing any search.

5.2 **Where do you have to search?**

5.2.1 Depending on the type of information requested, you may need to search all or some of the following:

5.2.1.1 electronic systems (e.g. databases, networked and non-networked computers, servers, customer records, human resources records system, email data, CCTV);

5.2.1.2 manual/paper filing systems (but only if they are '***structured filing systems'***, on which see below); and

5.2.1.3 any data systems held externally by your data processors.

5.3 If you are not authorised to access the relevant system or files that need to be searched, you will need to delegate those aspects of the search to a person who is authorised to access the relevant system or files.

5.4 You should liaise with your Data Protection Officer/ individual or team appointed to oversee your data protection compliance in relation to the searches to be carried out and they should then liaise with your IT department in relation to searches of your IT systems. Usually you will be required to carry out searches of any physical files or records.

6. What is a structured filing system?

6.1 In respect of personal data that is not processed by automated means (i.e. not on a computer) the GDPR only applies to the processing of personal data if the information forms part, or is intended to form part of a structured filing system. Therefore if the information is not part of a structured filing system, you will not be processing personal data for the purposes of the GDPR and the information will fall outside the scope of personal data under the data protection laws, and therefore will not be caught by the rights of data subjects. That being said, a 'clean desk' policy is advised and where you do store paper records, you should, as a matter of best practice, maintain a good filing system to avoid the loss of any personal data that may have not been filed correctly or promptly.

6.2 For the purposes of any manual/paper records, a 'structured filing system' must:

6.2.1 contain information relating in some way to individuals. Usually, there would be more than one file in the system or a group of information referenced by a common theme (e.g. an absence spread sheet). The files need not be located in the same geographical location, but could be dispersed over different locations;

6.2.2 be structured by reference to individuals (e.g. by name or employee or membership account number) or by reference to information relating to individuals (e.g. type of job or location, address), so it is clear at the outset whether the system might contain information capable of amounting to personal data and, if so, in which file(s) it is held; and

6.2.3 be structured so that specific information relating to a particular individual is readily accessible. This means that the system must be indexed or referenced so as to easily indicate whether and where in the file data about the individual is located. Examples would include any hard copy member or volunteer records or photo libraries.

6.3 It might help to apply the 'temp test' to determine if a system is a relevant filing system. Ask yourself if a temp with no specialist knowledge of your internal processes and procedures could, if asked to retrieve information about a specified individual, identify that the system might hold such information and where in that system the information would be. If so it will be a structured filling system.

7. Subject Access Requests

7.1 This paragraph 7 contains the specific procedure to be followed where an individual exercises their right of access (also known as a data subject access request). The

request need not refer to the Right, for instance, it might simply request ‘a copy of all the information that you have about me'.

7.2 There are limited timescales within which you must respond to a request and any delay could result in you failing to meet those timescales, which could lead to enforcement action by the ICO and/or legal action by the affected individual.

7.3 The data protection laws gives individuals the right to obtain:

7.3.1 confirmation that their personal data is being processed;

7.3.2 access to their personal data; and

7.3.3 access to other supplementary information.

7.4 The individual is entitled to receive a description of the following:

7.4.1 the purposes for which you process the data;

7.4.2 the categories of personal data you process about them;

7.4.3 the recipients to whom you may disclose the data;

7.4.4 the duration for which the personal data may be stored;

7.4.5 the rights of the data subject under the data protection laws;

7.4.6 any information available regarding the source of the data where it is not collected from the data subject direct;

7.4.7 the right of the data subject to make a complaint to the supervisory authority for data protection;

7.4.8 the logic behind any automated decision you have taken about him or her (see below), the significance and consequences of this automated processing.

7.5 Plus you must also provide the information constituting the individual’s personal data which is within the scope of their request. You must provide this information in an intelligible form and technical terms, abbreviations and codes must be explained, and where the request was made electronically you can, unless the data subject specifies otherwise, also provide the information in electronic form.

7.6 If the individual requests details on automatic decisions made about him, you must provide appropriate information, but in a format that does not compromise any trade secrets.

7.7 You may:

7.7.1 ask for additional information to confirm the identity of the individual making the request;

7.7.2 request that the scope of the request is narrowed in order to ease the searches to be undertaken (but the individual does not have to agree to such a request); and

7.7.3 where requests are manifestly unfounded or excessive, because they are repetitive: (a) charge a reasonable fee considering the administrative costs of providing the information (and the amount can be subject to limits); or (b) or refuse to respond. Where you refuse to respond to a request, you must explain why to the individual, 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.

7.8 Where you process a large quantity of information about an individual, the data protection laws permit you to ask the individual to specify the information the request

relates to. The legislation does not introduce an exemption for requests that relate to large amounts of data, but you may be able to consider whether the request is manifestly unfounded or excessive.

7.9 You should verify the identity of the person making the request, using "reasonable means" if you are not sure about their identity.

Redactions

7.10 Where you are providing information to an individual where they have made a subject access request, they are only entitled to their personal data. They are not entitled to see information which relates to other individuals or to other people, e.g. to a company.

7.11 In these cases you would redact, i.e. blank out in a permanent way, any information which is not the personal data of the individual making the subject access request.

Disclosing personal data relating to other individuals

7.12 Sometimes information that is determined to be personal data about one individual might include information identifying or personal data about another person (e.g. an email between two people might contain personal information relating to both the sender and the recipient) and in some cases it is not possible to redact the information about the other person. There are additional steps to consider in relation to whether you disclose this information.

7.13 You must consider whether the other person has consented to the disclosure of their information or whether it would be reasonable to comply with the request without the other person's consent.

7.14 Where the other person has consented, their information can be disclosed.

7.15 Where the other person has not consented, whether it would be reasonable to disclose that person's information will depend upon all the circumstances and you must assess these on a case by case basis.

7.16 You would consider whether:

7.16.1 The other person has refused their consent;

7.16.2 The other person's consent cannot be obtained (e.g. because they are incapable of giving it due to illness or incapacity);

7.16.3 Asking for consent might reveal the identity of the individual making the request;

7.16.4 You owe the other person a duty of confidentiality;

7.16.5 You have taken any steps to obtain the consent of the other person;

7.16.6 The other person is a recipient or one of a class of recipients who might act on the data to the individual's disadvantage;

7.16.7 The other person is the source of the information;

7.16.8 The information is generally known by the individual; and

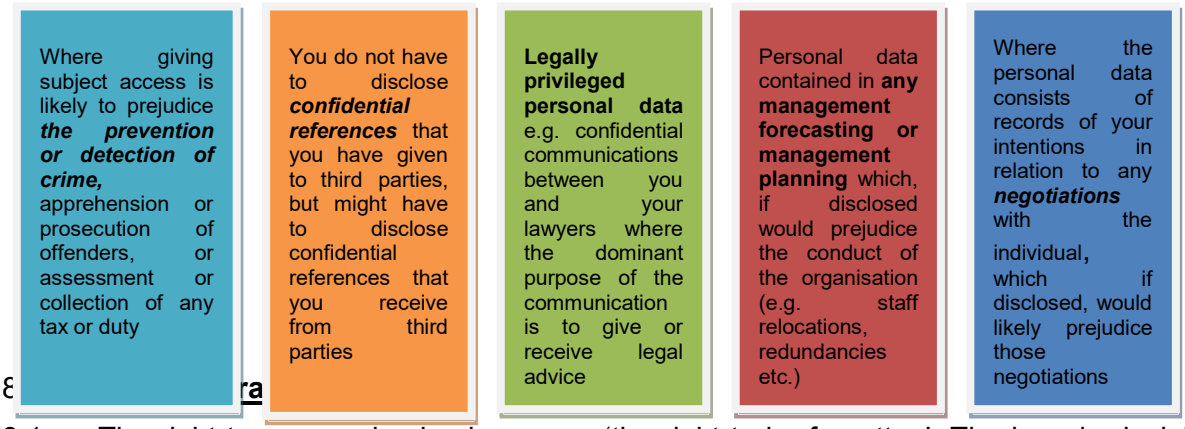
7.16.9 The individual has a legitimate interest in the disclosure of the other person's information which they have made known to us.

7.17 If you decide that the other person's information should be withheld (usually it should be), you still have to provide as much of the information requested as you can. Therefore, you should protect the other person's identity by redacting as much of this information and other identifiable particulars.

7.18 Always keep a record of what you have decided to do and your reasons for doing it.

Exemptions to the right of subject access

In certain circumstances you might be exempt from providing personal data in response to a subject access request. These exemptions are described below and should only be applied on a case by case basis after a careful consideration of all the facts.



8 Right to erasure

8.1 The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of their personal data where there is no compelling reason for its continued processing.

8.2 The right to erasure does not provide an absolute 'right to be forgotten'. Unless one of the exemptions applies below, individuals have a right to have their personal data erased and to prevent processing in specific circumstances:

8.2.1 where their personal data is no longer necessary in relation to the purpose for which it was originally collected/processed;

8.2.2 when the individual withdraws consent (but only to the extent that consent is the only basis for processing their personal data);

8.2.3 when the individual objects to the processing of their personal data and there is no overriding legitimate interest for continuing the processing;

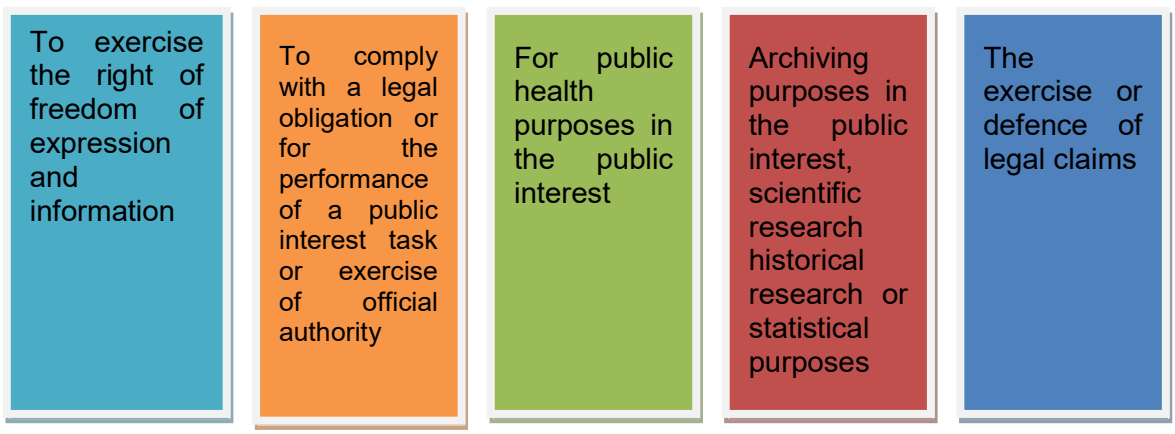
8.2.4 where their personal data was unlawfully processed;

8.2.5 where their personal data has to be erased in order to comply with a legal obligation; and

8.2.6 where their personal data is processed in relation to the offer of information society services (online service) to a child.

Exemptions to the right to erasure

There are some specific circumstances where the right to erasure does not apply and you can refuse to deal with a request:



8.3 If you have made the personal data public you are also obliged to inform the controllers which are processing such personal data to erase any links to, or copies or replications of those personal data, unless it is impossible or involves a disproportionate effort to do so.

9. **Right to rectification**

9.1 An individual has the right to ask you to:

9.1.1 correct inaccurate personal data;

9.1.2 complete information if it is incomplete; and

9.1.3 delete personal data which is irrelevant or no long required for our purposes.

9.2 If you have disclosed the personal data in question to third parties, you must inform them of the rectification request where possible. You must also inform the individuals about the third parties to whom the data has been disclosed where appropriate.

9.3 If data is factually correct and you are justified in keeping it, i.e. it is relevant to the lawful purpose you are holding it for then you do not have to change or delete it, but the individual may make a request for erasure, i.e. the right to be forgotten, and in that case you would have to analyse the personal data and whether you can retain it based on that Right.

9.4 Where you are not taking any action in response to a request for rectification, you must explain why to the individual, informing them of their right to complain to the supervisory authority (usually the ICO) and to seek a remedy from the Courts.

10. **Right to Restrict Processing**

10.1 An individual is entitled to require you to stop or not begin processing their personal data. When processing is restricted, you are permitted to store their personal data, but not further process it except in the exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest. You can retain just enough information about the individual to ensure that the restriction is respected in future.

10.2 You will be required to restrict the processing of personal data in the following circumstances:

10.2.1 where an individual contests the accuracy of the personal data, you should restrict the processing until you have verified the accuracy of the personal data;

10.2.2 where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and you are considering whether your legitimate grounds override those of the individual;

10.2.3 when processing is unlawful and the individual opposes erasure and requests restriction instead; and

10.2.4 if you no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.

10.3 Previously given consent for processing can be revoked at any time by the individual, therefore you cannot justify continued processing of data as a result of a previous consent.

10.4 The individual does not have this right if the individual has entered into a contract with you and the processing is necessary for the fulfilment of that contract.

10.5 You must inform individuals when you decide to lift a restriction on processing (for example, if an individual contested your right to process their personal data on legitimate interest grounds and you subsequently found that your processing was justified on these grounds).

10.6 If you have disclosed the restricted personal data to third parties, you must inform them about the erasure of the personal data, unless it is impossible or involves a disproportionate effort to do so.

11. The Right to Data Portability

11.1 The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. If the individual requests it, you may be required to transmit the data directly to another organisation if this is technically feasible. However, you are not required to adopt or maintain processing systems that are technically compatible with other organisations.

11.2 The right to data portability only applies:

11.2.1 to personal data an individual has provided to a data controller;

11.2.2 where the processing is based on the individual's consent or for the performance of a contract; and

11.2.3 when processing is carried out by automated means.

11.3 You must provide the personal data 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. This enables other organisations to use the data. The information must be provided free of charge.

11.4 If the personal data concerns more than one individual, you must consider whether providing the information would prejudice the rights of any other individual.

12. Right to Object

12.1 Individuals have the right to object to:

12.1.1 processing based on legitimate interests;

12.1.2 the performance of a task in the public interest/exercise of official authority (including profiling);

12.1.3 direct marketing (including profiling); and

12.1.4 processing for purposes of scientific/historical research and statistics.

12.2 If you process personal data on the basis of your legitimate interests or the performance of a task in the public interest/exercise of official authority:

12.2.1 individuals must have an objection on "grounds relating to his or her particular situation" i.e. the reasons for any objection must relate to their own personal situation; and

12.2.2 you must stop processing the personal data unless you can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or the processing is for the establishment, exercise or defence of legal claims.

12.3 If you process personal data for direct marketing purposes:

12.3.1 you must stop processing personal data for direct marketing purposes as soon as you receive an objection. There are no exemptions or grounds to refuse;

12.3.2 you must deal with an objection to processing for direct marketing at any time and free of charge; and

12.3.3 you must nevertheless comply with the terms of the Privacy and Electronic Communication Regulations and the e-Privacy Regulation which replaces it.

12.4 If you process personal data for research purposes:

12.4.1 individuals must have "grounds relating to his or her particular situation" in order to exercise their right to object to processing for research purposes; and

12.4.2 If you are conducting research where the processing of personal data is necessary for the performance of a public interest task, you are not required to comply with an objection to the processing.

12.5 If your processing activities fall into any of the above categories and are carried out online, you must offer a way for individuals to object online.

12.6 You must inform individuals of their right to object "*at the point of first communication*" and in your privacy notices. This right must be *"explicitly brought to the attention of the data subject and is to be presented clearly and separately from any other information".*

13. **Automated decision making and profiling**

(e.g. where a player has been automatically rejected for a place on a competition based solely on the automated processing of their personal data through the use of a sports algorithm or other wearable technology that monitors their performance)

13.1 The data protection laws provide safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention.

13.2 Individuals have the right not to be subject to a decision when:

13.2.1 it is based on automated processing; and

13.2.2 it produces a legal effect or a similarly significant effect on the individual.

13.3 You must ensure that individuals are able to:

13.3.1 obtain human intervention;

13.3.2 express their point of view; and

13.3.3 obtain an explanation of the decision and challenge it.

13.4 The right to obtain human intervention does not apply if the automated decision is:

13.4.1 necessary for entering into or performance of a contract between you and the individual;

13.4.2 authorised by law (e.g. for the purposes of fraud or tax evasion prevention); or

13.4.3 based on explicit consent (but bear in mind that any consent can be withdrawn).

13.5 The data protection laws define profiling as any form of automated processing intended to evaluate certain personal aspects of an individual, in particular to analyse or predict their:

13.5.1 performance at work;

13.5.2 economic situation;

13.5.3 health;

13.5.4 personal preferences;

13.5.5 reliability;

13.5.6 behaviour;

13.5.7 location; or

13.5.8 movements.

13.6 When processing personal data for profiling purposes, you must ensure that appropriate safeguards are in place. You must:

13.6.1 ensure processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the envisaged consequences;

13.6.2 use appropriate mathematical or statistical procedures for the profiling;

13.6.3 implement appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors; and

13.6.4 secure personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

13.7 Automated decisions taken for the purposes must not concern a child. Automated decisions must not involve or be based on the processing of special categories of data or criminal history records (previously sensitive personal data) unless:

13.7.1 you have the explicit consent of the individual; or

13.7.2 the processing is necessary for reasons of substantial public interest on the basis of EU / Member State law. This must be proportionate to the aim pursued, respect the essence of the right to data protection and provide suitable and specific measures to safeguard fundamental rights and the interests of the individual; and

13.7.3 (in each case) suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

14. Enforcement

14.1 If an individual disagrees that you have properly complied with a Right or you fail to respond they may apply to a Court for an order or complain to the ICO in each case requiring you to properly perform the Right.

14.2 If the Court or the ICO agrees with the individual it can:

14.2.1 order you to properly carry out the Right and what steps are needed to do this; and

14.2.2 order you to notify third parties who you have passed the data onto of the Right;

14.3 A court can also award compensation to the individual for any damage they have suffered as a result of our non-compliance. The ICO can also impose a civil fine upon you. These fines can be very substantial.

15. Deleting personal data in the normal course

15.1 You are only required to supply information in response to an exercise of Rights that was processed at the date of that request. However, you are allowed to carry out regular housekeeping activities even if this means deleting or amending personal data after the receipt of request in relation to a Right.

15.2 What you cannot do is amend or delete data because you do not want to supply it or because of the exercise of a Right.