

**GDPR TEMPLATE:**

**GUIDE TO HANDLING INDIVIDUALS’ REQUESTS TO EXERCISE DATA PROTECTION RIGHTS**

**Points to note**

* Before using this template Guide to Handling Individuals’ Requests to Exercise Data Protection Rights, it is essential that you read these ‘Points to note’, together with the separate document, ‘Make UK Essential GDPR Templates for HR – Points to note’, which provides important information applicable to all of the template documents, including this Guide.
* This Guide is effectively a template internal process for dealing with individual rights requests. It is intended to provide senior managers/HR with an explanation of how to identify and respond to individuals’ requests to exercise their data protection rights. It also provides those responsible for handling such requests with common examples of exemptions that might apply, enabling them to refuse to act upon requests, where appropriate.
* The Guide is not intended to be distributed to all staff. Taking into account factors such as the complexity, cost and administration of processing individuals’ data protection requests along with the potential impact on employee/public relations, our recommendation would be that only senior managers/HR (in collaboration with the Data Protection Officer/Data Protection Team/Data Protection Lead) are responsible for overseeing the response to individuals’ requests.
* Although the Guide is not designed to be distributed throughout the workforce, it is very important that all staff are trained to be able to identify an individual rights request and refer it to the correct internal bodies as soon as possible. This is because the time limits for processing these requests start to run from when the request was received by the organisation (irrespective of whether the request was made to a junior member of staff or an employee who is completely unfamiliar with data protection). While the Information Commissioner’s Office (ICO) recommends that employers have a designated email address to which individuals can send SARs, there is no requirement for individuals’ requests to be made in writing (they can be verbal or even made via social media). They do not have to be labelled with their common name (e.g. subject access request or SAR) and there is no need to make any reference to data protection legislation. As a result, requests are not always easy to identify and all staff need regular training and guidance to ensure that requests are recognised and dealt with correctly.
* We recommend that employers also have in place an organisation-wide data protection policy, such as our GDPR Template: Data Protection Policy, which (among other things) explains and emphasises the responsibility of all employees to recognise individual rights requests and alert the correct internal bodies. Such a policy should also emphasise the importance of not deleting, amending or hiding personal data with the intention of avoiding compliance with a request, as this can result in criminal liability.
* There is no express statutory obligation to have a written process, such as this Guide, for handling individuals’ rights requests. However, it is recommended as good practice in guidance produced by the ICO.
* The definition of ‘special category data’ which has been used in the Guide includes data relating to individuals’ criminal convictions or offences. While the GDPR definition of ‘special category data’ does not include this type of data, many of the same safeguards apply and, therefore, for practical purposes we have included this type of data in the Guide’s definition of ‘special category data’. The Guide assists in satisfying broader obligations under the GDPR to *demonstrate* compliance with data protection law (referred to as the ‘accountability’ principle). It can also be described as an organisational measure intended to ensure data protection compliance *by design and by default*.
* The Guide is divided into four parts: Part A provides a summary of the different individual rights requests that can be made under the GDPR. It does not expressly refer to the ‘Right to Information’ (i.e. the right to receive a privacy notice); this is technically an individual right under the GDPR but we have not included it in this Guide as it is usually treated as a standing obligation rather than one which is triggered by a particular request. (For further information about privacy notices and what they must contain, please refer to our GDPR Templates: Employee and Job Applicant Privacy Notices and their respective “Points to note”.) Part B of the Guide covers the general requirements which apply to the handling of all individual rights requests (e.g. general timing and communication provisions). Part C focuses on the requirements which are specific to each of the individual rights. Part D sets out the consequences of failing to deal properly with an individual rights request.
* The content of this Guide draws significantly on ICO guidance (in force as at October 2023). Much of the Guide is self-explanatory. However, where there are particular tricky issues, or the current ICO guidance lacks clarity, we have highlighted this and explained our recommended approach in the points set out below.
* **Subject access requests:** Note that locating the personal data required to respond to a subject access request is likely to involve searching the email inboxes and computer files of your staff, e.g. because they have corresponded by email with or about the requester. You should address this possibility in your electronic communications policy and/or your privacy notices. This is because, under the GDPR, individuals have the right to know that their personal data may be processed in this way. Our template Employee Privacy Notice includes appropriate wording to cover this.

* **Right to erasure – back-up data:** Regarding the reference to back-up data in the ‘Do you have to erase personal data from back-up data?’ section, we have included a reference to ICO guidance on deleting personal data that was produced before the DPA 2018 came into force:

(<https://ico.org.uk/media/fororganisations/documents/1475/deleting_personal_data.pdf>).

The ICO has stated that it will update this guidance in due course, but acknowledges that the old guidance remains useful in the meantime. The approach to back-up data set out in this Guide will therefore need to be reviewed (and possibly amended) once the ICO has published updated guidance on deleting personal data.

* **Automated decision-making and profiling:** In the ‘Assistance with requests to restrict automated decision-making and profiling’ section in Part C, there are two alternative drafting options depending on whether your organisation ever uses automated decision-making/profiling. Both options note that automated decision-making/profiling is a specialist area of processing which is subject to a highly regulated set of data protection rules; this Guide therefore does not include detailed guidance on handling requests to restrict such processing. If this type of processing is used, we would recommend that requests to restrict such processing are referred to your Data Protection Officer/Data Protection Team/Data Protection Lead to be dealt with on a case by case basis.
* **Data portability:**  We have included only minimal information about the right to data portability, because it is unlikely to apply to most manufacturing companies. Since it is such a highly regulated and technical area of individual’s data protection rights, any requests would need to be handled on a case by case basis. However, if you regularly receive requests to exercise this right, you may wish to amend this Guide to provide more detailed information about the right so that Employees within your organisation who are tasked with responding to such requests know how to handle them.

**Guide to Handling Individuals’ Requests to Exercise Data Protection Rights**

Data protection laws provide individuals with a number of rights in relation to their personal data. [COMPANY] is legally obliged to deal with individuals’ requests to exercise their rights appropriately and within applicable time limits.

[COMPANY’S] Data Protection Policy [, *which is available from/LINK*,] sets out a summary of individuals’ rights in relation to their personal data. It also specifies what [COMPANY] expects of its Employees (including current and former employees, workers, contractors, agency workers, consultants, interns, volunteers, partners and directors) in relation to alerting [COMPANY] if they receive a request from an individual seeking to exercise their rights.

This **Guide to Handling Individuals’ Requests to Exercise Data Protection Rights** (the Guide) explains the necessary procedures that senior managers/HR (in collaboration with the [Data Protection Officer/Data Protection Team/Data Protection Lead]) must follow as soon as they have been alerted to a request from an Employee or any other individual.

**PART A: SUMMARY OF INDIVIDUALS’ RIGHTS IN RELATION TO THEIR PERSONAL DATA**

Under data protection law, individuals have certain rights when it comes to how [COMPANY] handles their personal data including, for example:

* **The right to make a ‘subject access request’ (SAR).** This entitles an individual to receive a copy of the personal data [COMPANY] holds about them, together with information about how and why we process it and other rights that they have (as outlined below).
* **The right to object to our processing of an individual’s personal data** for direct marketing purposes, or where we are relying on our legitimate interests (or those of a third party) as our legal ground to process the data and we cannot show a compelling reason to continue the processing.
* **The right to request that we erase, delete or remove personal data** that we hold about an individual (also known as the ‘right to erasure’ or the ‘right to be forgotten’).
* **The right to request that we restrict our processing** of an individual’s personal data. This requires us to suspend the processing of personal data about an individual, for example, if they want us to establish its accuracy or the reason for processing it.
* **The right to request that we rectify or correct inaccurate personal data** **(or complete incomplete personal data)** that we hold about an individual (also known as the ‘right to rectification’).
* **Rights in relation to solely automated decision-making (including profiling),** including the right for the individual to voice their opinion, to obtain human intervention in the decision-making, and to contest the decision. Automated decision-making involves making a decision solely by automated means without any human involvement. Profiling involves the automated processing of personal data to evaluate certain things about an individual, such as work performance, and it may be part of an automated decision-making process.
* **The right to request that we transfer to an individual or another party, in a structured format, their personal data** which they have provided to us (also known as the ‘right to data portability’).

Most of the above rights are not absolute. Various conditions must be satisfied before individuals can exercise these rights. Equally, there may be circumstances where [COMPANY] can rely upon an exemption from complying with individuals’ requests, either partly or in full.

Regardless of the nature of an individual’s data protection request, there are some standard rules and procedures which must be adhered to whenever [COMPANY] is responding to a request. Part B sets out the general provisions that you must check and comply with whenever you are handling an individual’s data protection request. For rules and procedures that apply to specific individual data protection rights, see Part C.

**PART B: RESPONDING TO INDIVIDUALS’ DATA PROTECTION REQUESTS- GENERAL**

**Can you identify a data protection request?**

Provided that it is clear an individual is asking for action to be taken in relation to their personal data (or to gain access to it), a data protection request does not need to make reference to specific legislation or terminology.

A data protection request can be made verbally or in writing (e.g. letter, telephone, text message, email, or even via social media) to any part of the organisation. It does not have to be set out in a particular format and it does not have to be addressed to a specific person or contact point. You should record the details of requests that you receive, particularly those that are made verbally.

If you are uncertain whether an individual has made a data protection request, it is important to check the details with them to ensure that they have been understood correctly. This will help to avoid disputes over interpretation at a later stage.

**What is personal data?**

Personal data means any information relating to a living individual (also known as a ‘data subject’) who can be identified (directly or indirectly), in particular by reference to an identifier (e.g. name, NI number, employee number, email address, physical features). Relevant individuals can include colleagues, consumers, members of the public, business contacts, etc. Personal data can be factual (e.g. contact details or date of birth), an opinion about a person's actions or behaviour, or information that may otherwise impact on that individual. It can be personal or business-related.

Personal data may be held in an automated format (e.g. electronic records such as computer files or in emails) or in manual records which are part of a filing system (e.g. structured paper files and archives). Information that is stored in another way (such as in an unstructured file or in handwritten notes) can also be personal data if it is created with the intention that it will be stored electronically or in a filing system.

*Special category data*

Some categories of personal data are ‘special’ because they are particularly sensitive. Special category data is personal data about an individual’s:

* racial or ethnic origin;
* political opinions;
* religious or philosophical beliefs;
* trade union membership;
* physical or mental health;
* sex life or sexual orientation;
* biometrics (if used for identification purposes) or genetics; and/or
* criminal offences or convictions.

**Does the request relate to the individual’s personal data?**

An individual is only entitled to make a request in relation to their own personal data, and not in relation to other people’s personal data (unless the information is also about them, or they are acting on behalf of someone).Therefore, it is important to establish early on whether a request does relate to the individual’s own personal data or, if the request is made on someone else’s behalf, whether that person is entitled to make it (see **Do you need to check the entitlement of a third party making a data protection request on behalf of somebody else?** below).

**Have you recorded the data protection request and assigned responsibility?**

All data protection requests (whether verbal or in writing and whether made by the data subject or by a third party on their behalf) should be logged and recorded by the [Data Protection Officer/Data Protection Team/Data Protection Lead]. A specific [member of the team/HR/senior manager] must also be assigned responsibility for administering and tracking the progress of the request within the applicable time limits.

**Do you need to check an individual’s identity?**

You should only ask for proof of an individual’s identity if you have any reasonable doubts about their identity (e.g. because they are previously unknown to [COMPANY], they made the request via a personal email address that doesn’t match their name, etc.).

You should not request more information if the requester’s identity is obvious to you. This is particularly the case when you have an ongoing relationship with the individual.

If you are going to ask for proof of identity, you should do so as soon as possible after receiving the data protection request. Where the individual does not provide appropriate evidence to confirm identity where requested, you do not have to comply with their request. However, once they have provided the information necessary to confirm their identity, the time limit for responding to their request will begin to run.

When [COMPANY] is responding to a data protection request, it is sensible to record how you sought proof of identity. For accountability purposes, you should also document your reasoning for needing the proof of identity (i.e. the basis for any reasonable doubts over identity).

**Do you need to check the entitlement of a third party making a data protection request on behalf of somebody else?**

You must be satisfied that a third party making a data protection request on behalf of another individual is entitled to do so (e.g. a solicitor who has been instructed to act on their client’s behalf, or a third party who holds a genuine power of attorney for the individual).

It is the third party’s responsibility to provide [COMPANY] with evidence of this entitlement to make a data protection request on behalf of another individual. Keep a record of any evidence of entitlement to act.

If there is no evidence that a third party is authorised to act on behalf of the individual, you are not required to comply with the data protection request. However, you should still respond to the third party explaining this.

**Do you need to respond to a request which relates to personal data processed by a third party (e.g. payroll service provider) on behalf of [COMPANY]?**

Yes. As a controller of the individual’s personal data, we determine how that data is processed and we are therefore responsible for dealing with any request that we receive, even if it relates to data which is being processed by a third party processor on behalf of [COMPANY] (e.g. payroll providers, or confidential waste and shredding services).

**What is the time limit for responding to a data protection request?**

You must respond to a request without undue delay and, at the latest, within one month of receipt.

In cases where you have asked an individual to provide proof of identity (see **Do you need to check an individual’s identity?**), you have asked a third party to provide proof that they are entitled to make the request on another person’s behalf (see **Do you need to check the entitlement of a third party making a data protection request on behalf of somebody else?**),or where you have asked an individual to clarify a SAR (see in Part C **Can you ask an individual to clarify their SAR?**), the one month time limit starts to run once they have provided the additional information.

*Calculating the time limit*

Calculate the time limit from the day you receive the request (whether that day is a working day or not) until the corresponding calendar date in the next month.

For example, if [COMPANY] receives a request on 3 September, the time limit will start that day. This gives [COMPANY] until 3 October to comply with the request.

If this is not possible because the following month is shorter (and there is no corresponding calendar date), the date for response is the last day of the following month. If the corresponding date falls on a weekend or a public holiday, you have until the next working day to respond.

For example, if [COMPANY] receives a request on 31 March, as there is no corresponding date in April, [COMPANY] has until 30 April to comply with the request. If 30 April falls on a weekend, or is a public holiday, [COMPANY] has until the end of the next working day to comply.

[*Note – if the above is too complicated, you may prefer to adopt a ‘28 day rule’, to ensure compliance is always within a calendar month. If you take this approach, use the following wording in place of the ‘Calculating the time limit’ section, above:* In order to ensure that we always meet the one month deadline for responding to individual rights requests, [COMPANY] practice is to respond within 28 days, counted from the day after we receive the request.]

**Can the time limit be extended?**

The time for responding to a data protection request can be extended for a further two months, but only in very limited circumstances. This is where it is necessary because:

* the request is complex; and/or
* multiple requests have been made by the same individual.

Whether a request is complex depends on the specific circumstances of each case and you should not seek to extend the one month deadline on a routine basis.

With regard to SARs, for example, the need to search through a large volume of information may add to the complexity of a request, but a request will not be considered complex solely because the individual has requested a large amount of information. Other factors that may contribute towards the complexity of a SAR include technical difficulties in retrieving the information; applying an exemption that involves large volumes of particularly sensitive information; and needing to obtain specialist legal advice [*IF YOU ROUTINELY OBTAIN LEGAL ADVICE ON SARS:* (although since we routinely obtain legal advice on SARs, this is unlikely to be applicable to [COMPANY])].

[COMPANY] must let the individual know within one month of receiving the request that it intends to rely upon an extension and explain why an extension is necessary.

For accountability purposes, if you decide to rely upon a time extension you must carefully document your reasons for doing so.

**Can you refuse to comply with a data protection request?**

[COMPANY] may be able to avoid complying with a request if it is ‘manifestly unfounded or excessive’ or if another specific exemption applies (see below for further details of specific exemptions).

If a request is ‘manifestly unfounded or excessive’, you have the option of:

* charging a reasonable fee, taking into account the administrative costs of responding to the request; or
* refusing to act on the request.

*What is meant by ‘manifestly unfounded’?*

Guidance from the UK supervisory authority, the Information Commissioner’s Office (ICO), indicates that a request may be ‘manifestly unfounded’ if:

* the individual clearly has no intention to exercise their data protection rights (e.g. if example an individual makes a request, but then offers to withdraw it in return for some form of benefit from [COMPANY]); or
* the request is malicious in intent and is being used to harass [COMPANY] with no real purposes other than to cause disruption. For example:
  + the individual explicitly states, in the request itself or elsewhere, that they intend to cause disruption);
  + the request makes unsubstantiated accusations against [COMPANY] or specific employees;
  + the individual is targeting a particular [COMPANY] employee against whom they have a personal grudge; or
  + the individual systematically sends different requests to you as part of a campaign (e.g. once a week, with the intention of causing disruption).

However, the fact that one of these circumstances applies does not automatically mean that a request is manifestly unfounded. You must consider a request in the context in which it is made, and you are responsible for demonstrating that it is manifestly unfounded.

Also, you should not presume that a request is manifestly unfounded simply because the individual has previously submitted requests which *have* been manifestly unfounded or excessive or because the request includes aggressive or abusive language.

The ICO guidance emphasises that the word ‘manifestly’ means there must be an obvious or clear quality to the request being unfounded. You should consider the specific situation and whether the individual genuinely wants to exercise their rights. If this is the case, it is unlikely that the request will be manifestly unfounded.

*What is meant by ‘manifestly excessive’?*

In respect of subject access requests (SARs), the ICO guidance indicates that a request may be manifestly excessive if it is clearly or obviously unreasonable. In this regard, you should consider whether the request is proportionate when balanced with the burden or costs involved in dealing with the request. This will mean taking into account all the circumstances of the request, including:

* the nature of the requested information (e.g. how specific is it? is it limited by time or by topic?);
* the context of the request, and the relationship between you and the individual;
* whether a refusal to provide the information or even acknowledge if you hold it may cause substantive damage to the individual;
* your available resources;
* whether the request largely repeats previous requests and a reasonable interval hasn’t elapsed; or
* whether it overlaps with other requests (although if it relates to a completely separate set of information it is unlikely to be excessive).

When deciding whether a reasonable interval has elapsed between the current request and the one that it is largely repeating, you should consider:

* the nature of the data – this could include whether it is particularly sensitive; and
* how often the data is altered – if information is unlikely to have changed between requests, you may decide you do not need to respond to the same request twice. However, if you have deleted information since the last request you should inform the individual of this.

Note that whether a request is excessive depends on the particular circumstances. A SAR will not necessarily be excessive just because an individual has requested a large amount of information, even if you might find the request burdensome. (In such cases, you could consider asking the individual to clarify their request – see in Part C, **Can you ask an individual to clarify their SAR?**).

As with the ‘manifestly unfounded’ exemption, SARs should be considered on a case by case basis and that you should not assume that a SAR is manifestly excessive just because an individual has previously submitted a manifestly unfounded or excessive request. Importantly, the ICO guidance emphasises that the word ‘manifestly’ means there must be an obvious or clear quality to the request being excessive and you must be able to demonstrate this to the individual and the ICO.

For other types of request (objection to processing, erasure, restricting processing, rectification, and data portability), the ICO guidance indicates that a request may be excessive if:

* it repeats the substance of previous requests; or
* it overlaps with other requests.

However, whether a request is excessive depends on the particular circumstances. A request will not necessarily be excessive just because an individual:

* makes a request about the same issue. An individual may have legitimate reasons for making requests that repeat the content of previous requests, e.g. if [COMPANY] has not handled previous requests properly;
* makes an overlapping request relating to a completely separate set of information; or
* has previously submitted requests which have been manifestly unfounded or excessive.

As is clear from the above, there is a high threshold for being able to use the ‘manifestly unfounded or excessive’ exemption. If you rely upon this exemption, you must be able to justify your decision and demonstrate why the request ismanifestly unfounded or excessive. Your reasoning should be documented for accountability purposes.

Other exemptions may apply in relation to certain individual rights as set out in Part C, below (although be alert to the fact that these exemptions will rarely provide [COMPANY] with an exemption from complying with *all* aspects of a data protection request).

**Can you charge a fee for processing a data protection request?**

You can only charge a fee in the following limited circumstances:

* the request is manifestly unfounded or excessive (see **Can you refuse to comply with a data protection request?**); or
* in the case of a SAR, the individual has requested additional copies of information.

If you decide to charge a fee, you should base it on the reasonable administrative costs of complying with the request. In the context of SARs, the ICO guidance indicates that this may include the costs of assessing whether you are processing the requested information, locating and retrieving it, providing a copy of it and communicating the response to the individual. This may include the costs of photocopying, printing, equipment, supplies, etc. It can also include the cost of staff time involved in complying with the request – based on a reasonable hourly rate. [*If you have a policy on how you calculate the amount of any fee, you could insert details here.*]

You should contact the individual promptly and inform them that you are charging a fee, along with your reasons for doing so (and the information regarding complaints as detailed in **Do you have to notify individuals of a refusal to comply with a data protection request?**, below).

In cases where you are charging a fee, you do not need to comply with the data protection request until you have received the fee.

For accountability purposes, you must keep a record of your justification for charging a fee.

**Do you have to notify individuals of a refusal to comply with a data protection request?**

Yes. If you are not going to comply with a data protection request in the first instance (whether this is because you are relying on the ‘manifestly unfounded or excessive’ or other exemption(s), you intend to charge a fee, or you are requesting additional identification information) you need to let the individual know and provide them with specific information regarding complaints and enforcement of their rights.

You must inform the individual of a refusal to comply without undue delay (and, in any event, within one month of receipt of the data protection request). Your communication to the individual should include details of:

* the reasons [COMPANY] is not taking action;
* the individual’s right to make a complaint to the appropriate supervisory authority (i.e. the ICO in the UK); and
* their ability to seek to enforce this right through a judicial remedy.

**Do you have to communicate your response to a data protection request in writing?**

As a general rule, information and communications in response to a data protection request should be in writing. However, they can be provided by other means (including electronic means) where appropriate (see in Part C **How should you provide the results of a SAR to the individual?**).

All communications relating to the request must be in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

**PART C: INDIVIDUAL RIGHTS**

Whenever you are handling individuals’ data protection requests you must be able to demonstrate compliance with the general requirements set out above in Part B. You will also need to demonstrate compliance with the specific requirements in relation to the particular data protection request you are handling, as set out below in this Part C.

1. **Subject access requests (SARs)**

**What is a SAR?**

As a controller, [COMPANY] must supply a copy of and information about the personal data that it holds about an individual upon receipt of a request from that individual (subject to some exemptions). This is known as a subject access request or SAR.

A SAR may be framed widely, for example it might seek ‘any personal data that is processed’ about the individual or it might be limited by reference to, for example, subject matter, dates or, in relation to emails, the persons sending or receiving emails.

For general information regarding the principles, administration and time limits applicable to SARs, please see Part B, above.

**What is an individual entitled to under a SAR?**

Individuals making a SAR have the right to obtain the following from [COMPANY]:

* confirmation that [COMPANY] is processing their personal data;
* a copy of their personal data; and
* supplementary information relating to the data (see below).

The following supplementary information must be provided to the individual:

* the purposes of processing the data;
* the categories of personal data concerned;
* the recipients (or categories of recipients) to whom we disclose the personal data and, in particular, details of recipients in other countries and the appropriate safeguards in place in relation to such data transfers, if applicable (e.g. IDTA, UK Addendum to the EU standard contractual clauses, or binding corporate rules);
* the retention period for storing the personal data or, if that is not possible, the criteria used to determine that period;
* the individual’s additional rights to require rectification or erasure of personal data, or to restrict or object to processing of personal data;
* the right to lodge a complaint with the relevant supervisory authority (e.g. the ICO in the UK);
* the source of the data if it was not collected directly from the individual;
* whether there is any automated decision-making taking place in relation to the individual’s personal data (including profiling) and, if so, the reasons for this, its significance and the envisaged consequences of such automated decision-making for the data subject.

Note that if you are refusing to comply with an individual’s SAR, there is other specific information you must provide when communicating your refusal (see above in Part B **Do you have to notify individuals of a refusal to comply with a data protection request?**).

**Can you ask an individual to clarify their SAR?**

In some circumstances, you can ask for clarification of the SAR.

The requirement to search for and identify all the personal data [COMPANY] holds on an individual, or all the personal data covered by the SAR, can be onerous and time-consuming. If [COMPANY] processes a large amount of personal data concerning the individual, you can ask them for more information to clarify their SAR, provided that you only ask for the information that you reasonably need to find the personal data covered by the request. For example, you could ask the individual to clarify the type of information or processing activities to which the SAR relates (e.g. whether information relates to information held on email or in hard copy).

For accountability purposes, you should record your reasons for seeking clarification of a SAR.

Let the individual know as soon as possible (and, in any event, before the initial one month time limit for responding has expired) that you need additional information from them.

If the individual refuses to provide any additional information, [COMPANY] cannot ignore the SAR. [COMPANY] must try to comply by making reasonable searches for the information requested.

The time limit for responding to a SAR will be paused while you wait for clarification from the individual. If you wish to seek clarification of a SAR, you should contact the individual promptly and without undue delay to provide an explanation of: (a) the reasons why clarification is being sought; (b) the fact that the clock has been stopped until they respond; and (c) whether they need to provide clarification within a certain time (although you should try to accommodate the individual as much as possible).

If there is any information that you can provide without seeking clarification, you should provide that information within one month. For example, you could provide a general confirmation that you hold personal data about the individual as well as some of the supplementary information that you are required to give when responding to a SAR (e.g. the individual’s right to request rectification, erasure or restriction, or to object to processing; and the right to complain to the ICO). This could be done via a link to our privacy notice, which already contains that information.

If you do not receive any response to your request for clarification within a reasonable period of time (generally, one month), the SAR can be considered ‘closed’.

**What efforts should you make to find the information requested in a SAR?**

Data protection law places a high expectation on [COMPANY] to provide information in response to a SAR. You must make reasonable efforts to find and retrieve the information requested. This will include, for example, conducting searches of hard copy filing systems, computer hard drives, mobile devices, emails, messaging platforms and applications, company social media accounts, etc. It may also involve searching electronic archives (although you will not be expected to use technological solutions to recreate data that has been permanently deleted).

You are not required to conduct searches that would be unreasonable or disproportionate. To determine whether searches may be unreasonable or disproportionate, you must take into account: the circumstances of the request; any difficulties involved in finding the information; and the fundamental nature of the right of access.

The burden of proof is on [COMPANY] to be able to justify why any particular search is unreasonable or disproportionate. Accordingly, if you are considering limiting the searches you conduct on this basis, you must first seek guidance from the [Data Protection Officer/Data Protection Team/Data Protection Lead]. You should also consider whether seeking further details from the individual as to the scope of their request could help you to find the information they have requested (see **Can you ask an individual to clarify their SAR?** above).

**How should you provide the results of a SAR to the individual?**

You should, generally, provide the results of the SAR in hard copy. However, where the individual makes the SAR by electronic means (e.g. by email), you should provide the information in a commonly used electronic form (e.g. secure file share or email) unless the individual has requested otherwise. Where the information includes special category data, or other information that the individual would consider particularly private, you should ensure that you transfer it to the individual using an appropriately secure method.

Regardless of the format, the information provided under a SAR must be concise, transparent, intelligible and easily accessible, using clear and plain language. (See **Do you have to communicate your response to a data protection request in writing?** in Part B above, for further details.)

If any of the information to be provided under a SAR is in a coded form (e.g. through encryption or using [COMPANY] specific short-form codes or acronyms) which the average person would be unable to understand, you should provide enough information to allow the individual to understand the meaning of the coded information. However, you are not required to ensure that that the information is provided in a form that can be understood by the particular individual making the request. For example, if an individual would struggle to understand the information provided under a SAR because their English comprehension skills are poor, [COMPANY] is not required to provide a translation or simplified version, provided the information could be understood by an average person. To the extent that it is reasonable, it is good practice for you to help individuals understand the information [COMPANY] holds about them.

Note that, sometimes, personal data may be contained within a document or email that includes other information that is not the individual’s personal data, an example being emails that an individual is copied into but which do not otherwise contain any of the individual’s personal data. While the individual’s name and email address are their personal data and should therefore be disclosed when responding to the SAR, the ICO acknowledge that supplying information in summary form in these circumstances is acceptable. For example, stating in your response to the individual that “1,000 emails contain only your name and email address”.

**Can you edit the individual’s personal data before you respond to a SAR?**

As a general rule, you should not amend or delete the personal data to be provided under a SAR unless an exemption applies. It is a criminal offence to alter, deface, block, erase, destroy or hide personal data that relate to the request with the intention of preventing disclosure.

However, the ICO has stated that routine use of the data may result in it being amended or even deleted while you are dealing with a request. In these circumstances, it is not unreasonable to supply the information that is held by [COMPANY] at the time it processes the SAR (even if this is different from the data held when the SAR was first received), provided always that any changes are not carried out with the intention of preventing disclosure. **Any action carried out with the intention of preventing disclosure could lead to disciplinary action (including dismissal), as well as criminal liability.**

**What should we do if the information covered by a SAR includes information relating to other people?**

Sometimes, the results of a SAR include information that relates to the individual making the request *and* to another individual. When responding to a SAR, you do not have to disclose information about another individual (a ‘third party’) who can be identified from that information, unless:

* the third party has consented to the disclosure; or
* it is reasonable to comply with the request without the third party’s consent.

If the third party consents to you disclosing the information relating to them, then it would be unreasonable not to do so. However, if there is no such consent, you must decide whether to disclose the information anyway.

The ICO guidance recommends taking a three step approach.

**First**, you should consider whether you can comply with the SAR without revealing information about the third party. You should take into account the information you are disclosing and any information you reasonably believe the individual who made the SAR may have, or could obtain, that would identify the third party.

You may be able to redact or edit documents to remove information about the third party. For example, if the information covered by the SAR includes a spreadsheet detailing pay and bonuses for all employees in a particular department, you could redact it to remove the other employees’ data and disclose a copy of the spreadsheet showing only the pay and bonus data for the individual who made the request.

By contrast, redacting material to remove a third party’s data would not be appropriate if the data is mixed, such that redaction would impact the personal data of the individual who made the SAR. For example, if the information covered by the SAR includes an email chain between two managers discussing the performance of the individual who made the SAR, redacting the managers’ names and other identifiers (e.g. email addresses) would impact on the personal data of the individual who made the SAR, as it is relevant to them to know *who* took the view of their performance that is expressed in the email. If redacting the third party data would make it impossible to properly comply with the SAR, you should move on to the second step.

**The next step** is to consider whether you can ask for consent from the third party to disclose the information about them. It is generally considered good practice to do so, but it is not a legal requirement and doing so may not be appropriate in certain circumstances, such as where:

* you don’t have the third party’s contact details;
* it would potentially reveal to the third party personal data relating to the individual who made the SAR that the third party is not already aware of; or
* it would be inappropriate for the third party to know that the individual made a SAR.

**Finally**, if you have not been able to obtain consent from the third party, you must consider whether it is reasonable to disclose information about them without their consent. This is a difficult exercise which involves balancing the rights of the individual who is making the SAR against those of the third party. You must take into account all of the relevant circumstances, including but not limited to:

* the type of information that you would disclose;
* any duty of confidentiality you owe to the third party;
* any steps you have taken to seek consent from the third party;
* whether the third party is capable of giving consent; and
* any express refusal of consent by the third party.

With regard to the duty of confidentiality, the ICO guidance notes that there are certain types of relationship that would usually carry a duty of confidence with them, including the employment relationship. However, it also flags that you should not always assume confidentiality – e.g. if the information in a letter that is marked ‘confidential’ is widely available elsewhere. In most cases where a duty of confidence does exist, it is usually reasonable to withhold third party information, unless you have their consent to disclose it.

It is also relevant whether the third party information is already known to the individual who made the SAR (in which case there would be less reason to withhold it), as well as the significance of the information to that individual.

(Note that consent in relation to disclosure of third party data in response to a SAR is different from consent as a legal basis for processing personal data, so the difficulties with seeking consent from employees (due to the imbalance of power in the employment relationship) are not applicable here. This is because your legal basis for processing (i.e. for disclosure of data in response to a SAR) is your legal obligation to comply with the SAR. The question of whether a third party consents to disclosure of their data as part of your response to an individual’s SAR is a factor you must consider when complying with your legal obligation; it is not your legal basis for processing.)

For accountability purposes, it is important to record your reasoning for withholding or disclosing third party data. When you withhold third party data, where possible, you should also explain your reliance on this exemption to the individual making the request.

**What exemptions apply to SARs?**

In addition to the “manifestly unfounded or excessive” ground for refusing to comply with a request (see **Can you refuse to comply with a data protection request?** above in Part B), there are a number of other exemptions which apply in relation to SARs. Most exemptions are not absolute and will only apply in specific circumstances.

The most common exemptions which are likely to apply include:

*Third party information*: Where the data requested under a SAR would reveal information about both the individual who is making the request and a third party, you do not always have to disclose information about the third party (see above **What should we do if the information covered by a SAR includes information relating to other people?**).

*Confidential references*: Confidential references given or received for employment, education or training purposes.

*Management forecasting*: Information that is processed for the purposes of management forecasting or management planning, if disclosure would be likely to prejudice the conduct of the business.

*Negotiations*: Information that records [COMPANY]’s intentions in relation to negotiations with the individual making the SAR, if disclosure would be likely to prejudice the negotiations.

*Legal professional privilege*: Anything covered by legal professional privilege or covered by a duty of confidentiality owed by a professional legal adviser to a client.

*Self-incrimination*: Information which, if disclosed, would reveal evidence of commission of a criminal offence (some limited exceptions) and expose [COMPANY] to proceedings for that offence.

*Prevention or detection of crime*: Information that is processed for the purposes of the prevention or detection of crime, if complying with the SAR would be likely to prejudice that purpose.

Exemptions should not routinely be relied upon or applied in a blanket fashion. You must consider each exemption on a case-by-case basis.

For accountability purposes, you must justify and document your reasons for relying on an exemption.

[Where possible, you should also explain your reliance on any exemptions to the individual making the request.]

Note that the fact that an individual has signed a settlement agreement with [COMPANY] does **not** mean that [COMPANY] is exempt from complying if the individual subsequently makes a SAR. If a settlement agreement states that it limits the individual’s right of access, then it is likely this part of the settlement agreement will be unenforceable under data protection legislation.

Similarly, the fact that an individual has submitted a grievance, or commenced tribunal or court proceedings against [COMPANY], does **not** provide [COMPANY] with an exemption from the requirement to comply with a SAR if the individual makes one. This is the case even if there may be some overlap between information that [COMPANY] must provide in response to the SAR and information the individual will obtain through the tribunal or court disclosure process.

1. **Right to object to processing**

**What is the ‘right to object to processing’?**

Where [COMPANY] is processing an individual’s personal data, the individual has a specific right to object to that processing in certain circumstances.

For general information regarding the principles, administration and time limits applicable to the right to object to processing, please see Part B, above.

**When can an individual object to processing?**

The most likely situations where this right could apply are when [COMPANY] processes an individual’s personal data:

* for direct marketing purposes (including profiling related to direct marketing); or
* on grounds of [COMPANY]’s ‘legitimate interests’ (or those of a third party).

**Objections to direct marketing**

An individual can ask [COMPANY] to stop processing their personal data for direct marketing (or related ‘profiling’ purposes) at any time. This is an **absolute** right and there are **no exemptions or grounds for refusal**. Upon receipt of an ‘objection’ to processing for direct marketing purposes, this type of processing must stop immediately.

**Objections to ‘legitimate interests’ processing**

If an individual is objecting to [COMPANY]’s processing of their personal data on the legal ground of its ‘legitimate interests’ (or those of a third party), they must specify why they are objecting in relation to their particular situation. However, the right to object to ‘legitimate interests’ processing is not an absolute right.

In addition to rejecting requests which are manifestly unfounded or excessive (see **Can you refuse to comply with a data protection request?** in Part B, above), [COMPANY] can reject an objection to ‘legitimate interests’ processing if:

* it can demonstrate that there are compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
* the processing is necessary for the establishment, exercise or defence of legal claims.

When assessing whether there are compelling legitimate grounds, you must consider the reasons why the individual has objected to the processing of their data. In particular, if an individual objects on the grounds that the processing is causing them substantial damage or distress (e.g. the processing is causing them financial loss), the grounds for their objection will have more weight. When deciding whether to reject an objection on this basis, bear in mind that it is [COMPANY]’s responsibility to be able to demonstrate that its legitimate grounds override those of the individual.

If you are satisfied that [COMPANY] does NOT need to stop processing the personal data in question, you should let the individual know and provide the necessary information (as set out above in Part B, **Do you have to notify individuals of a refusal to comply with a data protection request?**).

**Do you need to erase personal data to comply with an objection?**

Where you have received an objection to the processing of personal data and there are no grounds to refuse, [COMPANY] must stop processing the data. This may mean that you need to erase personal data, as the definition of processing is very broad, and includes storing data.

However, erasure may not be appropriate if the data is also processed for other purposes and you need to retain the data for those purposes.

For example, when an individual objects to the processing of their data for direct marketing, rather than erasing the individual’s details entirely, it may be more appropriate to place their details onto a suppression list to ensure that you continue to comply with their objection. If you do this, you should retain just enough information about the individual to ensure that their preference not to receive direct marketing is respected in future. You must ensure that the data is clearly marked so that it is not processed for the purposes the individual has objected to.

1. **Right to erasure**

**What is the ‘right to erasure’?**

The right to erasure enables individuals to request that their personal data is erased. It is often referred to as ‘the right to be forgotten’. The right to erasure is not an absolute right and only applies in certain circumstances.

For general information regarding the principles, administration and time limits applicable to the right to erasure, please see Part B, above.

**When does the right to erasure apply?**

The right to erasure is only applicable in relation to certain categories of personal data, including data that:

* is no longer necessary for the purpose for which it was collected/otherwise processed;
* was processed on the basis of consent but the individual has withdrawn consent;
* was processed on the basis of legitimate interests but the individual objects to that and there are no overriding legitimate grounds for processing;
* was processed for direct marketing purposes and the individual objects to that processing;
* was processed unlawfully;
* must be erased to comply with a legal obligation.

However, see **When can you refuse to comply with a request for erasure?**, below, for details of circumstances in which the right will not apply.

**Do you have to erase personal data from ‘back-up’ data?**

Yes, if a valid request has been made and there are no exemptions that apply, then [COMPANY] will have to take steps to erase the relevant personal data from back-up systems as well as live systems.

However, the ICO recognises that, while erasure requests may be instantly fulfilled in respect of live systems, data can remain within the back-up environment for a certain period of time until it is overwritten. In these circumstances, the ICO explains that the key issue is to put the back-up data ‘beyond use’, even if it cannot be immediately overwritten.

Essentially, if you do not use personal data within the back-up for any other purpose, i.e. the back-up is simply held on your systems until it is replaced in line with an established schedule, then it is unlikely that the retention of the back-up would pose a significant risk.

You must be clear with individuals as to what will happen to their data when their erasure request is fulfilled, including in respect of backup systems.

**Who must you notify about the right to erasure?**

Where an individual has submitted a valid request for erasure of their personal data, which [COMPANY] has carried out, data protection laws require us to notify other organisations about the erasure of the personal data in some circumstances.

In particular, the notification obligation arises where:

* the personal data has been disclosed to others; or
* the personal data has been made public in an online environment (for example on social networks, forums or websites).

If [COMPANY] has disclosed the personal data to others, you must inform each recipient of the erasure, unless this proves impossible or involves disproportionate effort.

A recipient is defined as a natural or legal person, public authority, agency or other body to which data are disclosed. The definition includes controllers (i.e. organisations like [COMPANY], who determine how data is processed), processors (i.e. organisations who process data under instructions from a controller, such as a payroll provider) and persons who, under the direct authority of the controller or processor, are authorised to process personal data. If requested, you must also inform the individual exercising the right to erasure about these recipients.

Where the individual’s personal data has been made public online, [COMPANY] should take reasonable steps to inform other controllers who are processing the personal data to erase any links to, or copy or replication of that data. When deciding what steps are reasonable, you must take into account available technology and the cost of implementation.

**When can you refuse to comply with a request for erasure?**

In addition to rejecting requests for erasure which are manifestly unfounded or excessive (see **Can you refuse to comply with a data protection request?** in Part B, above), [COMPANY] does not have to comply with a request for erasure if processing is necessary for certain reasons. Those that are most likely to apply to the processing carried out by [COMPANY] are where continued processing is necessary:

* to exercise the right of freedom of expression and information;
* to comply with a legal obligation; or
* for the establishment, exercise or defence of legal claims.

If you are satisfied that [COMPANY] does NOT need to erase the personal data in question, you should let the individual know and provide the necessary information (as set out above in Part B, **Do you have to notify individuals of a refusal to comply with a data protection request?**).

1. **Right to restrict processing**

**What is the right to restrict processing?**

Individuals have the right to restrict [COMPANY]’s processing of their personal data in certain circumstances where individuals have a particular reason for wanting the restriction (e.g. they dispute the accuracy of the data that we hold).

By exercising this right, an individual can limit the way that [COMPANY] uses their data. It is, effectively, an alternative to requesting the erasure of their data. In most cases, [COMPANY] will not be required to restrict processing of an individual’s personal data indefinitely, but will need to have the restriction in place for a certain period of time.

For general information regarding the principles, administration and time limits applicable to the right to restrict processing, please see Part B, above.

**When does the right to restrict processing apply?**

An individual has the right to restrict the processing of their personal data where:

* the individual contests the accuracy of the personal data – processing is restricted for a period to enable you to verify its accuracy;
* processing is unlawful, but the individual requests restriction of processing rather than erasure of the data;
* you no longer need the data for the purpose for which it was collected, but the individual needs it to establish, exercise or defend legal claims;
* you are seeking to process data based on the legal ground of ‘legitimate interests’, and the individual has objected to the processing under their right to object (see above) – in this situation, you are prevented from processing while you seek to establish your compelling legitimate grounds that will override the individual’s objection.

Bear in mind that you may be able to refuse to comply with a request to restrict processing where the request to exercise this right is manifestly unfounded or excessive (see **Can you refuse to comply with a data protection request?** in Part B, above).

**How do we restrict processing?**

Processing personal data involves a very broad range of operations, from collection and storage to disclosure and destruction. Therefore, the methods of restriction will depend on the type of processing that you are carrying out.

Examples of different methods of restriction include:

* temporarily moving the data to another processing system;
* making the data unavailable to users; or
* temporarily removing the data from a website.

Where an individual has requested that you restrict your processing of personal data (but, effectively, is also requesting that you do not erase the data), consider carefully how you store that data. For example, if you are using an automated filing system, you need to use technical measures to ensure that any further processing cannot take place. The data cannot be changed whilst the restriction is in place. It is also advisable to note on your system that the processing of this data has been restricted.

**Is there anything that *can* be done with restricted data?**

Where processing has been restricted, [COMPANY] can continue to store the data, but cannot do any other processing except in certain very limited circumstances, the most common being where:

* [COMPANY] needs to continue processing the data to establish, exercise or defend legal claims;
* the individual has given their consent;
* processing is necessary for the protection of the rights of another person (natural or legal).

**When can a restriction on processing the data be lifted?**

In many cases, the restriction of processing is only temporary, for example, where the restriction is linked to an individual disputing the accuracy of the personal data and you are investigating this. Alternatively, the individual may have objected to [COMPANY] processing their personal data on the grounds of ‘legitimate interests’ and [COMPANY] is considering whether its legitimate interests override those of the individual.

Once a decision has been made e.g. regarding the accuracy of the data or whether [COMPANY]’s legitimate interests override those of the individual, you may decide to lift the restriction. In this situation, [COMPANY] must inform the individual BEFORE the restriction is lifted. See **Do you have to notify individuals of a refusal to comply with a data protection request?** in Part B above, for details of the information that you need to include in the communication to individuals to inform them that you will be lifting the restriction on processing.

**Do we have to notify others of a restriction on processing personal data?**

Yes. If you have disclosed the personal data in question to others, you must contact each recipient and inform them of the restriction on processing the personal data, unless this proves impossible or involves disproportionate effort. If requested, you must also inform the individual making the request for restriction on processing about these recipients. See **Who must you notify about the right to erasure?** above, for the definition of a recipient.

1. **Right to rectification or correction of personal data**

**What is the right to rectification or correction?**

The right to rectification (or ‘correction’, as it is sometimes referred to) enables an individual to require [COMPANY] to correct any inaccurate personal data concerning him or her and to complete any incomplete personal data (depending on the purposes of the processing). This may involve providing a supplementary statement to the incomplete data.

For general information regarding the principles, administration and time limits applicable to the right to rectification or correction, please see Part B, above.

**When is data inaccurate?**

Personal data is inaccurate if it is incorrect or misleading as to any matter of fact.

Problems can arise where the data in question involves opinions rather than facts. Opinions are subjective and it can be difficult to conclude that the record of an opinion is inaccurate. Provided that it is clear that the relevant data is recording an opinion and, where appropriate, whose opinion it is, [COMPANY] can assert that this is not a case of inaccuracy that needs to be rectified.

For reasons of practicality, therefore, [COMPANY] treats matters that are not ‘verifiable’ facts as ‘opinions’. This covers obviously subjective opinions (e.g. a statement by A that he thought B appeared aggressive) and, potentially, different individuals’ versions of events (e.g. a statement by A that he saw B in a particular place at a particular time). This latter example might appear to be factual in nature but, unless [COMPANY] has access to CCTV footage of the relevant location, it would be extremely difficult, even impossible, for [COMPANY] to verify. By contrast, a verifiable fact is information whose accuracy [COMPANY] can check in an objective manner (e.g. a statement that A was absent from work on a particular date, or that B graduated from university with a 2:1).

Complications may also arise if the data refers to a mistake that has subsequently been resolved. It may be possible to argue that the record of the mistake is, in itself, accurate and should be kept. In such circumstances, both the fact that a mistake was made and also the correct information should be included in the individual’s data.

**How should you handle a request for rectification?**

Assuming that the request for rectification is not manifestly unfounded or excessive (see **Can you refuse to comply with a data protection request?** in Part B above), [COMPANY] must take reasonable steps to confirm that the data is accurate and to rectify the data if necessary.

What amounts to reasonable steps depends on the nature of the personal data and what it will be used for. The more important it is that the personal data is accurate, the greater the effort that needs to be made to check its accuracy and, if necessary, rectify it. For example, you should make a greater effort to rectify inaccurate personal data if it is used to make significant decisions that will affect the individual or others. Make sure that you take into account the arguments and evidence provided by the individual making the request and record your findings regarding accuracy for accountability purposes.

While we are checking the accuracy of an individual’s personal data, they have the right to request that we restrict its processing (see **Right to restrict processing**, above). However, the ICO has recommended that, as a matter of good practice, processing should be restricted whilst accuracy is being checked regardless of whether the individual has exercised their right to restriction.

If you find that the personal data in question is inaccurate, you must take steps to correct it. If the inaccurate personal data appears in multiple records that you hold (e.g. an employee’s biography information might be included on an internal directory on your intranet, but also on your customer-facing website), you will need to rectify the inaccuracy in all of those records in order to comply with the data protection law ‘accuracy principle’.

**What should you do if you are satisfied that the data is accurate?**

If you find that the data is accurate, you need to inform the individual that you will not be amending their personal data. See **Do you have to notify individuals of a refusal to comply with a data protection request?** in Part B above, for details of the information that you need to include in the communication to the individual to inform them of your decision.

**Do you have to notify others if personal data is rectified/corrected?**

Yes. If you have disclosed the personal data in question to others, you must contact each recipient and inform them of the rectification (or completion) of the personal data, unless this proves impossible or involves disproportionate effort. If requested, you must also inform the individual making the request for rectification about these recipients.

See **Who must you notify about the right to erasure?** above, for the definition of a recipient.

1. **Restrictions on automated decision-making and profiling**

**What is automated individual decision-making and profiling?**

Automated decision-making is a decision made by automated means without any human involvement. An example of automated decision-making in the HR context could be a recruitment aptitude test which uses pre-programmed algorithms and criteria to shortlist candidates.

Profiling is a form of automated decision-making that consists of evaluating certain personal aspects relating to an individual to analyse or predict aspects concerning that person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. For example, in an HR context, this could involve recording an individual’s productivity levels on certain types of machinery with a view to making decisions relating to output bonuses.

**What restrictions apply to automated decision-making and profiling?**

As a general rule, individuals have the right not to be subjected to solely automated individual decision-making (including profiling) that produces legal or similarly significant effects. In other words, [COMPANY] is restricted from using these methods to make decisions that could have a serious negative impact on an individual (such as e-recruiting practices without human intervention).

However, data protection laws do permit automated decision-making (including profiling) in very limited circumstances – namely, where the automated decision is:

* based on the individual’s explicit consent (but note that consent is subject to many restrictions if it is to be valid and there are also difficulties with obtaining valid consent in an employment context); or
* necessary to enter into or perform a contract with the individual; or
* required or authorised by law.

Where special category data is concerned, the permitted circumstances for this type of processing are even more limited. The permitted circumstances are where the automated decision is:

* based on the individual’s explicit consent (again, consent is subject to restrictions and there are difficulties with obtaining valid consent in an employment context); or
* necessary for reasons of substantial public interest.

As this type of processing is considered to be high risk under data protection law, [COMPANY] should carry out a data protection impact assessment (DPIA) before beginning the processing, so as to ensure that the risks involved have been identified, assessed and addressed appropriately.

It will also be necessary to put in place additional safeguards, including:

* providing meaningful information about the logic involved in the decision-making process, as well as the significance and the envisaged consequences for the individual;
* using appropriate mathematical or statistical procedures;
* ensuring that individuals are able to:
* obtain human intervention in the process;
* express their point of view; and
* obtain an explanation of the decision and challenge it
* implementing appropriate technical and organisational measures to ensure you can correct inaccuracies and minimise the risk of errors; and
* securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and that prevents discriminatory effects.

**Assistance with requests to restrict automated decision-making and profiling**

The use of automated decision-making and profiling is a highly regulated area of individuals’ data protection rights. Detailed information regarding the handling of requests to restrict such processing is therefore outside the scope of this Guide.

[*If you do not currently use automated decision-making/profiling:* [COMPANY] does not currently use automated decision-making/profiling and, accordingly, you are unlikely to receive any individual requests concerning the right to restrict such decision-making.]

[*If you use any automated decision-making/profiling:* [COMPANY] currently only uses automated decision-making/profiling in the following limited circumstances: *insert details*. [*If you conducted a DPIA in respect of the automated decision-making/profiling:* We have conducted a DPIA to ensure that any associated risks have been identified, assessed and appropriately mitigated. Details of the DPIA are available from the [Data Protection Officer/Data Protection Team/Data Protection Lead].] If you receive a request to restrict automated decision-making/profiling, you should immediately contact the [Data Protection Officer/Data Protection Team/Data Protection Lead] for advice on how to respond.]

If [COMPANY] chooses to introduce any [additional] automated decision-making process (or profiling) this should be administered on a case by case basis, following careful review after a DPIA has been carried out. For details of what a DPIA involves, see [COMPANY]’s [template Employee Data Protection Impact Assessment].

1. **Right to data portability**

**What is the right to portability?**

The right to data portability allows individuals to move, copy or transfer their personal data easily from one IT environment to another in a safe and secure way, without affecting its usability. By doing this, individuals can take advantage of applications and services that will use the data to find them a better deal, or help them understand their spending habits.

**Assistance with requests to exercise the right to portability**

The right to data portability is very unlikely to be relevant to [COMPANY], particularly in the HR context. It is primarily intended to improve the ‘interoperability’ of data processing systems and to prevent individuals from finding themselves “locked-in” to a service contract with a particular provider, e.g. mobile phone service providers who refuse to port departing customers’ information to a new provider.

The right to data portability is also a highly regulated area of individuals’ data protection rights. As this right is unlikely to be relevant to [COMPANY], detailed information for handling a request to exercise this right is outside of the scope of this Guide.

If [COMPANY] does receive an individual request to exercise the right to portability, this must be handled on a case by case basis and you should contact the [Data Protection Officer/Data Protection Team/Data Protection Lead] for advice on how to respond.

**PART D:** **CONSEQUENCES OF FAILING TO DEAL PROPERLY WITH AN INDIVIDUAL RIGHTS REQUEST**

If an individual believes that [COMPANY] has not properly dealt with their individual rights request, they have a number of options for recourse, including:

* A complaint to the ICO (or, if the individual is resident in an EEA country, the supervisory authority in that country). The ICO/other supervisory authority can ask questions about the allegation via an information notice (which [COMPANY] must answer), or issue an enforcement notice (which [COMPANY] must comply with). The ICO/other supervisory authority can also issue a monetary penalty of up to £17.5million, or 4% of global annual turnover, whichever is higher, but the amount will be determined based on the facts of the individual case and the ICO’s Regulatory Action Policy has indicated that fines should be set at a level that is “effective, proportionate and dissuasive”.
* An application to Court for an order requiring [COMPANY] to comply with the individual rights request.
* An application to Court for damages caused by the breach (including damages for distress). There is a defence to a claim for damages if [COMPANY] can show that it was in no way responsible for the event giving rise to the damage.
* A complaint to the ICO/other supervisory authority or an application to Court supported by a representative body, such as a trade union.

Where [COMPANY] fails to deal properly with an individual rights request made by an employee, in addition to the above potential consequences, the employee may argue that the breach of their individual rights amounts to a breach of [COMPANY]’s implied duty of trust and confidence, or is part of a series of events which eventually leads to a breakdown of trust and confidence, entitling them to resign and claim constructive dismissal. This is likely to apply only in serious cases, such as where the breach of individual rights has a specific impact on the employee, causing them damage and/or serious distress.