Subject Access Request Guidance

Contents

Chapter 1 : What is a Subject Access Request?

An individual's Fundamental Right

A Subject Access Request (SAR) is the right of access, allowing an individual to obtain records to their personal information, held by an organisation. The UK General Data Protection Regulation (UK GDPR; GDPR), which became applicable in May 2018, provides individuals with the right of access to information. A SAR is a fundamental right for individuals. It helps them understand how and why you are using their data and check you are doing it lawfully.

What is a Data Subject?

An identifiable natural person (living individual), who can be identified, directly or indirectly, by reference to an identifier (such name, address, telephone number, date of birth and other examples set out in Article 4(1) of the GDPR. A deceased person is not a data subject under the UK GDPR.

What is Personal Data/Information?

Personal data or personal information relates to living persons, who can be identified or who are identifiable, either directly from information held by the data controller, or indirectly from that information in combination with other information. Examples of personal data include a name, identification number, location data, online identifier, or one or more factors relating to that person's physical, physiological, genetic, mental, economic, cultural, or social identity.

Who is a Data Controller?

The UK GDPR defines a data controller as "a natural or legal person, which alone or jointly with others, determines the purposes and means of personal data processing."

The role of a data controller is to determine who shall be responsible for compliance with data protection rules and how data subjects can exercise their rights. Putting it simply, they are the manager of personal data, they instruct the data processor. The data controller will decide the purpose for which personal data is required and what personal data is necessary to fulfil that purpose.

In the United Reformed Church, there are typically two data controllers, responsible for the processing of personal data in different departments, committees, and activities:

- The United Reformed Church
- The United Reformed Church Trust

Who is the Data Processor?

The UK GDPR defines a data processor as "a natural or legal person that processes personal data on behalf of the data controller."

A data processor is a person or organisation who deals with personal data as instructed by a controller for specific purposes and services offered to the controller that involve personal data processing.

The role of a data processor could include storing data, retrieving data, running the payroll for a business, carrying out marketing activities, or providing security for data. The list is endless.

Chapter 2 : Data Subject Rights

Rights of the Data Subject

Chapter three of the GDPR, details all the rights an individual has, when it comes to their personal data. I've outlined each of these rights below, but I will not go into detail, as this guidance is for the sole purpose of exploring the right of access by the data subject. For further information on the other rights, please see the Data Protection Guidance document.

A data subject, under the GDPR can exercise their right to:

- Request access to their personal data
- Request correction of their personal data
- Request erasure of their personal data
- Object to processing of their personal data
- Request restriction of processing their personal data
- Request transfer of their personal data
- Right to withdraw consent

Personal Data Access Right

When exercising the right to access personal data, a data subject ideally is exercising their right to:

- Obtain confirmation from the controller that it is processing their personal data.
- Access their processed personal data, including receiving a copy on request unless providing a copy adversely affects the rights and freedoms of others.
- Obtain certain information about the controller's processing including:
    - purposes of data processing;
    - categories of personal data processed;
    - recipients or categories of recipients who receive personal data from the controller;
    - how long the controller stores the personal data, or the criteria the controller uses to determine retention periods;
    - information on the personal data's source if the controller does not collect it directly from the data subject;
    - information on the safeguards used to secure cross-border data transfers, if applicable; and
    - whether the controller uses automated decision-making, including profiling, the auto-decision logic used, and the consequences of this processing for the data subject.
- Notification of their rights to:
    - request rectification or erasure of personal data.
    - restrict or object to certain types of personal data processing; and
    - make a complaint with the Information Commissioner.

Reasons for Making a Subject Access Request?

Data Subjects tend to make subject access requests to find out:

- what personal information an organisation holds about you.
- how they are using it;
- who they are sharing it with; and

- where they got your data from.

Chapter 3 : Data Controller Obligations Under the UK GDPR

Data Controller Responsibilities

The UK GDPR imposes several obligations on controllers, including obligations that relate specifically to a data subject's rights and their ability to exercise those rights. According to Article 12(2) of the UK GDPR, a controller must facilitate the exercise of data subject rights. They must also comply with certain requirements relating to data subjects' rights when:

- Communicating with data subjects
- Responding to data subject requests
- Handling data portability requests
- Acting as a joint controller
- Using solely automated processing, including profiling, to make decisions affecting data subjects
- Handling a personal data breach

Communicating with Data Subjects

A controller must provide data subjects with certain information about its personal data processing activities. The UK GDPR requires controllers to provide this information and communicate with data subjects, including data subject request responses, in a manner that is:

- Concise.
- Transparent.
- Intelligible.
- Easily accessible.
- In clear and plain language.
- In writing, including by electronic means if appropriate. However, the controller may provide information orally on the data subject's request if it can verify the data subject's identity.

Chapter 4 : Making a Subject Access Request

How to Make a Request

The UK GDPR does not set out formal requirements for a valid request: An individual can make a SAR verbally or in writing (be it via post or electronically), including by social media. They can make it to any part of the organisation, and they do not have to direct it to a specific person or contact point.

The data controller should provide means for requests to be made. Standard forms can make it easier for organisations to recognise a request and for those making them to include all the details that might be needed to locate their information.

There is a subject access request form (see Chapter 11), a data subject can use, to submit their SAR, to the United Reformed Church or the United Reformed Church Trust.

Provision of Information on Data Subject's Identity

In complying with its data security obligations, a data controller receiving a request is likely to want to make sure that the request comes from the person who is purporting to make it. The data controller must request proof of identity from the data subject, unless it is clearly not a necessity (i.e., the request is done in person, or from the data controller's work email address, which only they have access to).

To help establish a data subject's identity, they must provide identification that clearly shows their name, date of birth and current address. As the data controller, we can accept a photocopy or a scanned image of one of the following as proof of identity:

- Passport or photo identification such as a driving licence.
- Birth or adoption certificate.
- A copy of a bank or credit card statement or utility bill, showing current address, dated within the last three months.

If there has been a change of name, we'd need the relevant documents evidencing the change.

A data controller may request additional information from a data subject, to help confirm their identity and their right to access, and to provide them with the personal data a data held by the data controller. A data controller reserves the right to refuse to act on a data subject's request if they cannot be identified.

Scope of Request

A request may be framed widely. For example, it might seek "any personal data that is processed" about the data subject. Although there is no requirement to be more specific, failing to set out the characteristics of the personal data that the data subject is seeking may mean that the request is less effective than it might be. In general, it is best to try to focus or limit a request. Recital 63 of the UK GDPR indicates that where a data controller processes a large quantity of information, it should be able to request that, before responding to the request, the data subject should specify the information or processing activities to which the request relates.

In many contexts, there will be thousands (and perhaps hundreds of thousands) of pieces of data processed about a data subject (for example, computer log-on files, records of web searches made, emails and associated metadata). If a request is not limited, the data controller may argue that it is

"manifestly unfounded or excessive" and seek to charge a fee or refuse to act on the request (Article 12(5), UK GDPR, see Chapter 5, *Manifestly unfounded or excessive requests*). The more focused and reasonable a data subject is, the harder that argument will be.

Chapter 5 : Responding to A Subject Access Request Under the UK GDPR

Initial Assessment

On receipt of a request, the data controller should make an assessment considering:

- Whether or not it processes data concerning the data subject.
- The scope of the request.
- Whether it intends to respond.
- If it is going to respond, whether the nature or scope of the data subject's request will have an impact on the timing of a detailed response.
- What its approach to finding the data subject's personal data will be.

Unclear Request

If it is genuinely unclear whether a data subject is making a subject access request, the time for responding does not begin until the data controller has clarified whether the data subject is doing so and, if so, what personal data they are requesting. The data controller should contact the data subject as quickly as possible (by phone or email where this is appropriate) and explain why it is seeking further details. The data controller should keep a record of any conversation about the scope of the data subject's request and the date when it sought and received any further explanation. The data controller should feel able to justify its position to the ICO if asked to do so.

Deceased Individuals

The definition of personal data covers information which relates to a living individual. If a data controller receives a subject access request but becomes aware that the data subject has died before the data controller has provided a response, the data controller is not obliged to respond to the request. This is because the data ceases to be personal data once the data subject has died.

Checking the Identity of the Requester

A data controller receiving a request must make sure that the request comes from the person who is purporting to make it (because of the security obligations in Article 5(1)(f) of the UK GDPR). In addition, under Article 12(6), there is an express power to seek additional information if the data controller has reasonable doubts concerning the identity of the data subject.

The key point is that any request in relation to confirming identity, must be reasonable and proportionate and should not involve a request for information, where someone's identity is obvious, which is particularly likely to be the case, where there is an ongoing relationship.

Where information about identity is sought, formal identification documents should not be requested unless necessary. There may be other reasonable and proportionate ways to verify identity using existing measures such as usernames and passwords.

Timing

The starting point for the rules regarding timing are as follows:

- A data subject access request must be dealt with, without undue delay and in any event within one month of receipt of the request.

- That one-month period may be extended by two further months where necessary, considering the complexity and number of requests.

The number of requests (for example, where a data subject makes a subject access request, a request for erasure and a request for data portability simultaneously) can be considered separately from complexity when deciding if the one-month period should be extended.

- The data controller must inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. (Article 12(3), UK GDPR.)

Please note that the time limit starts to run from either receipt of the request, or receipt of:

- Any information requested to confirm a data subject's identity.
- A fee where a data controller has been entitled to charge one (i.e., for manifestly unfounded or excessive requests).

Specific provision is made for cases in which the data controller processes a large amount of information about a data subject and needs to ask the data subject to clarify the information or processing activities their request relates to, before responding. In such cases, the time limit for responding to request is paused (referred to as "stopping the clock"), until the data controller receives clarification.

Regarding counting time, the data controller should calculate the time limit from the day it receives the request (or, where applicable, the day it receives the requested information or fee), whether that day is a working day or not, until the corresponding calendar date in the next month. This accords with updated guidance the ICO published in August 2019 on responding to data subject requests which made clear that, when calculating the period for response, the day of receipt is day one rather than the day after receipt. For example, if a data controller receives a request on 3 September it will have until 3 October to respond.

If such a calculation 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, the data controller will have until the next working day to respond.

The application of these rules means that the exact number of days a data controller has to comply with a subject access request will vary, depending on the month in which a request is received. The Access Guidance recommends that, for practical purposes, if a consistent number of days is required (for example, for a data controller's operational or system purposes), it may be helpful to adopt a 28-day period to ensure compliance is always within a calendar month.

When is a Request Complex?

Whether a request is complex depends upon the specific circumstances and the request. What may be complex for one data controller, may not be for another. The data controller's size and resources are likely to be relevant factors in determining that question.

Here are examples of factors that may, in some circumstances, add to the complexity of a request:

- Technical difficulties in retrieving the information (for example, where data is electronically archived).

- Applying an exemption that involves large volumes of particularly sensitive information.
- Any specialist work involved in obtaining the information or communicating it in an intelligible form.
- Clarifying potential confidentiality issues around the disclosure of sensitive medical information.
- Needing to obtain specialist legal advice. However, if legal advice is routinely obtained it is unlikely to be complex.
- In the case of public authorities, searching large volumes of unstructured manual records.

The fact that a request involves a large volume of information may add to the complexity of a request, but a request will not be complex solely because the data subject has requested a large amount of information.

A request will not be complex simply because a data controller must rely on a processor to provide the information it needs to respond.

Understanding what the Data Subject Wants: Clarifying a Request

Where the data controller processes a large amount of information about a data subject, before embarking on an exercise to search for a data subject's personal data, if it is not clear what information the data subject is requesting, the data controller may find it helpful to ask the data subject in more detail what information they are after and where it is likely to be. Recital 63 of the UK GDPR indicates that, where a data controller processes a large quantity of personal data, the data controller should be able to ask the data subject to specify the information or processing activities to which the request relates. This may help the data controller in its search. Although the aim of the request should not be to narrow the scope, it is possible that once the question has been asked, the data subject will decide to narrow the scope.

The time limit for responding to the request is paused until the data controller receives the clarification needed.

If a data controller requests and receives clarification on the same day, the clock will not stop (the extension of the time limit is calculated in terms of days, not hours). It should be remembered that the clock only stops where the data controller seeks clarification about the information requested and not where the data controller seeks clarification about any other matter (for example, the format of the response).

Where the data controller seeks clarification, but does not receive a response, it should wait for a reasonable period before considering the request to be "closed". While one month is generally reasonable, a data controller needs to follow a proportionate and reasoned approach. If the data controller believes that a data subject may have difficulty in providing additional details within a specified timeframe, it should try to and accommodate the data subject as far as possible (for example, where complex issues are involved or when there are accessibility issues).

A data controller should not seek clarification on a blanket basis and should only do so where:

- It is genuinely required to respond to a subject access request; and
- The employer processes large amounts of information about the employee.

The Access Guidance provides that a data controller can ask a data subject to provide additional details about the information they want to receive, such as the context in which the data controller may have processed their information and the likely dates of it being processed. However, a data

subject cannot be forced to narrow the scope of their request, as they are still entitled to ask for "all the information you hold" about them. Where a data subject responds by either repeating their request or by refusing to provide any additional information, a data controller must still comply with the request by making reasonable searches for the information.

A data controller should ensure that the process of seeking and obtaining clarification is quick and easy for the data subject and, as far as possible, a data controller should provide advice and assistance to help them clarify their request. Where possible, a data controller should contact a data subject in the same format they made the request (for example, if a data subject has emailed the subject access request a data controller should email them to ask for clarification). The data controller should explain that the clock stops from the date that clarification is requested and will resume once the data subject responds. The data controller should also specify whether the data subject needs to reply by a certain time.

Establishing Steps for Responding to a Subject Access Request

Controllers should establish steps for responding to all data subject access requests by:

- Appointing an appropriate person to oversee handling the request.
- Confirming that the request is in writing. If the data subject makes the request orally, ask the person to put it in writing for tracking purposes.
- Confirming receipt of the request in writing.
- Verifying the identity of the person making the request. If the data subject provides insufficient information to confirm his/her identity, the controller may (but is not required to) request more information (Articles 12(2) and 12(6)) of UK GDPR.
- Confirming that the request provides enough information to locate the personal data relating to the data subject and his request. If the data subject provides insufficient information to locate the personal data, request more information.
- Determining whether any exemptions apply that permit the controller to refuse to respond to the request or that exempt the controller from providing certain types of personal data in response to the request.
- Refusing to respond to the request when:
    - the controller cannot verify the identity of the data subject (Article 12(2)); or
    - local law contains an exemption permitting the controller to refuse to respond.
- Locating the relevant personal data.
- For any third-party personal data collected in response to the request:
    - consider seeking the third party's consent to disclose the data; or
    - redact the third party's personal data from the information gathered in response to the request.
- Responding in writing or electronically when the data subject makes an electronic request, unless the data subject requests the response in another format (Article 12(3)). Controllers should only respond orally to the data subject:
    - when requested by the data subject; and
    - after verifying the data subject's identity (Article 12(1)).
- Responding to and complying with the request within one month of receiving the request, unless the controller:
    - needs additional time to respond (Article 12(3)); or
    - will not take the requested action (Article 12(4)).

- Following the escalation procedures to obtain approval for additional response time if the controller cannot provide the response within one month. The controller should also inform the data subject within one month of receiving the request of:
    - any extension of up to two months (Article 12(3));
    - the reasons why it will not take action; and
    - the data subject's right to make a complaint with a supervisory authority or seek a judicial remedy. (Article 12(4)).
- Responding free of charge unless the request is:
    - unfounded; or
    - excessive.
- Demonstrating the unfounded or excessive nature of a request, and either:
    - charging a reasonable fee considering the administrative costs of providing the information or taking the requested action; or
    - refusing to act on the request (Articles 12(6)).
- Taking additional steps required, for a subject access request (mentioned in Chapter 2 (under *Personal Data Access Right*)).
- Notifying third parties processing the data subject's personal data about any correction, rectification, or restriction requests (Articles 17(2) and 19).
- Following all procedures for documenting and tracking responses to data subject requests, including any responses provided orally.

Manifestly Unfounded or Excessive Requests

Although subject access requests are generally free, if a request is manifestly unfounded or excessive, the employer may either, under Article 12.5, UK GDPR:

- Charge a reasonable fee (considering the administrative costs of providing the information or taking the action requested, and subject to any regulations made under section 12(1)(a) of the Data Protection Act (DPA) 2018)).
- Refuse to act on the request.

In such circumstances, the data controller must be able to demonstrate that the request is indeed manifestly unfounded or excessive. If it decides not to act on the request, it must give reasons and tell the data subject that if there is a dispute, they may complain to the Information Commissioner or apply to the court (see Article 12(4) of the UK GDPR, Decision not to take action on a request and Challenges to the response to a subject access request).

Data controllers should not be too cavalier in asserting that requests are unfounded or excessive. The Access Guidance considers "manifestly unfounded or excessive" means and the ICO is likely to look closely at the data controllers. It may be a better and more attractive approach to act on the request to the extent that the data controller believes it is reasonable and proportionate, reserving assertions that the request is excessive or unfounded for use if that approach is challenged by the data subject.

Data controllers must take the following into account when determining whether a request is manifestly unfounded or excessive:

- Each request should be considered individually: data controllers should not have a blanket policy.
- Data controllers should not presume that a request is manifestly unfounded or excessive just because a data subject has previously submitted a manifestly unfounded or excessive request.

- The inclusion of the word "manifestly" means there must be an obvious or clear quality to the unfoundedness or the excessiveness.
- Data controllers should ensure they have strong justifications when they consider a request to be manifestly unfounded or excessive, which they can clearly demonstrate to the data subject and the ICO.

Manifestly Unfounded Requests

The Information Commissioner suggests that a request may be manifestly unfounded if:

- The individual making the request clearly has no intention of exercising their right of access. For example, they make a request, but then offer to withdraw it in return for some form of benefit from the employer.
- The request is malicious in intent and is being used to harass the data controller with no real purposes other than to cause disruption. For example, where:
    - the individual has explicitly stated, in the request itself or in other communications, that they intend to cause disruption;
    - the request makes unsubstantiated accusations against the data controller or particular data subjects which are clearly prompted by malice;
    - the individual is targeting a particular employee against whom they have some personal grudge; or
    - the individual systematically sends different requests to the employer as part of a campaign, for example, once a week, with the intention of causing disruption.

Manifestly Excessive Requests

A request may be excessive if it is clearly or obviously unreasonable which should be answered with reference to the question of whether the request is proportionate when balanced with the burden or costs involved in dealing with the request.

This will mean taking account of all the circumstances of the request, including:

- The nature of the requested information;
- The context of the request, and the relationship between the data controller and the data subject;
- Whether a refusal to provide the information or even acknowledge the data controller holds it, may cause substantive damage to the data subject;
- The data controller's available resources;
- Whether the request largely repeats previous requests and a reasonable interval has not yet elapsed; or
- Whether the request overlaps with other requests (although if it relates to a separate set of information it is unlikely to be excessive).

A request is not necessarily excessive simply because the data subject requests a large amount of information. The data controller must consider all the circumstances of the request and should also consider asking the data subject for more information to help you locate the information they want and whether the data controller can make reasonable searches for the information.

When deciding whether a reasonable interval has elapsed the data controller should consider:

- The nature of the data. This could include whether it is particularly sensitive.

- How often the data is altered. If information is unlikely to have changed between requests, the data controller may decide it does not need to respond to the same request twice. However, if the data controller has deleted information since the last request you should inform the individual of this.

Although a data subject is not required to explain the purpose of the request, and their motivation for making the request is not a bar, their purpose and motivation may be relevant in considering what is or is not excessive or proportionate. The Article 12(5) rule (UK GDPR) may apply to parts of a request. So, a data controller may say that elements of a request are excessive and entitle it to refuse to comply but take a different approach with other elements.

Is a Subject Access Request Free?

Personal information requested by a data subject must be provided free of charge (Article 12(5), UK GDPR), although reasonable fees may be charged in certain circumstances, such as manifestly unfounded or excessive requests.

Manifestly Unfounded or Excessive Requests: Charging a Reasonable Fee

When a data controller is determining a reasonable fee, it can consider the administrative costs of:

- Assessing whether the employer is processing the information.
- Locating, retrieving, and extracting the information.
- Providing a copy of the information.
- Communicating the response to the individual, including contacting the individual to inform them that you hold the requested information (even if you are not providing the information).

A data subject should not be "double-charged" where there is overlap across these activities.

A reasonable fee may include the costs of:

- Photocopying, printing, postage, and any other costs involved in transferring the information to the employee (for example, the costs of making the information available remotely on an online platform).
- Equipment and supplies (for example, discs, envelopes, or USB devices).
- Staff time.

Data controllers should base the costs of staff time on the estimated time it will take staff to comply with the specific request, charged at a reasonable hourly rate. While section 12(1)(a) of the DPA 2018 allows for the Secretary of State to issue regulations specifying limits on the fees that may be charged to deal with a manifestly unfounded or excessive request, regulations are yet to be issued. It is therefore incumbent on data controllers to ensure that they charge a reasonable rate.

To ensure that fees are charged in a reasonable, proportionate, and consistent manner, the guidance recommends that it is good practice for data controllers to establish an unbiased set of criteria for charging fees which explains:

- The circumstances in which they charge a fee.
- The data controller's standard charges (including a costs breakdown where possible, for example, the costs per A4 photocopy).
- How the data controller calculates the fee, explaining the costs they consider including the costs of staff time.

These criteria should be clear, concise, and accessible. While they should be made available on request, there is no need for them to be published online. Data controllers should include a copy of their criteria when they request a fee and explain any charge that is unclear.

When a data controller charges a fee, it will not have to comply with the individual's subject access request, until it has received the fee. However, the data controllers should ensure that they request the fee promptly and at the latest within one month of receiving the subject access request. Data controllers must not unnecessarily delay requesting it, nearing the end of the one-month time limit. Neither should they ask for a fee as a way of extending the period they have to respond to a request. Where a data controller is unable to request the fee as soon as reasonably possible, it should document the reasons why and be able to provide reasons to the ICO, if asked.

A data subject should be given a reasonable period to respond to a request for a fee. It will generally be reasonable to close a request if the data controller does not receive a response within one month, although what is reasonable will depend on the circumstances.

Decision Not to Take Action on a Request

Other than in exceptional cases, a data controller will be under a duty to act on a request by responding. There are, however, some circumstances in which the data controller may decide not to act, in which case it must inform the data subject without delay, and at the latest within one month of receipt of the request, of the reasons for not acting and that the data subject may lodge a complaint with the ICO or take legal proceedings (Article 12(4), UK GDPR).

Examples might be where the person to whom the subject access request was addressed is not the controller (perhaps because it is acting as a processor or someone else is the controller) or where the request is manifestly unfounded or excessive.

Except in circumstances which are clear and in which the data controller is confident it can justify a decision not to act on a request (as might be the case if it is not the controller), a data controller should engage with the data subject and seek to limit the request where appropriate.

Chapter 6 : Finding, Retrieving, and Redacting Personal Data

Extent of the Duty

Dealing with a subject access request can be demanding and time-consuming, particularly in an employment context in which much data will be unstructured and will relate not only to the data subject but also to other individuals. Such data will almost inevitably require redaction.

Although on the face of Article 15 there is no limit on the personal data to which data subject can seek access, there are constraints derived from EU law and Article 12(5) of the UK GDPR which are reflected in Access Guidance.

While a data controller must make genuine and extensive efforts, it does not have to go so far as to leave no stone unturned. The Access Guidance suggests that the data controller must make "reasonable efforts" to find requested information but provides that data controllers are not required to "conduct searches that would be unreasonable or disproportionate to the importance of providing access to the information". To decide whether searches may be unreasonable or disproportionate, the data controller must consider:

- The circumstances of the request.
- Any difficulties involved in finding the information.
- The fundamental nature of the right of access.

The burden of proof will be on the data controller to justify why a search is unreasonable or disproportionate. It should also bear in mind that while searching for some information may be unreasonable or disproportionate, it will still be required to search for other information that is within the scope of a request. The data controller should also consider whether to seek clarification from the data subject, to search for the information they have requested. Data controllers should also ensure that their information management systems are well-designed and maintained, so that they can efficiently locate, and extract requested information and, where necessary, redact third-party data.

Finding the Data Subject's Personal Data

The primary task is to find the relevant personal data. How that is done depends on its nature, how it is stored and, more generally, on the data controller's approach to information management. Normally the data will be on the data controller's main servers. But it may also be in other locations.

Most electronic information can be found and sorted relatively easily. Emails are usually the starting point and, because of their unstructured nature, the most difficult to deal with. Typically, a data controller would:

- Look at several individuals' mailboxes and use search tools to identify emails that refer to the data subject. In using search tools, it would be normal to search for the data subject's name and other identifiers commonly used such as abbreviations, nicknames, and initials.
- Having identified a pool of emails that refer to the data subject, the data controller may then search and seek to narrow that pool by dates (if relevant) or by other appropriate criteria (for example "redundancy" or "performance").

- Taking emails that contain personal data relating to the data subject and analyse them to see whether there is also personal data relating to other individuals. That data falls into two categories:
    - personal data which relates to other individuals which does not relate in any way to the data subject ("non-relevant personal data"); and
    - personal data which is information about the data subject but also information about another individual.

If the personal data is also information relating to another individual, unless that individual has consented, the data controller must consider whether it is reasonable to disclose the information without consent.

- If it is not reasonable to disclose the information without consent, the data controller should consider whether, by redacting information (information that would identify the other individual), it would be possible to provide the data subject with at least some of the personal data sought. If so, the data controller would then redact that "other individual" personal data.
- Review information which is not personal data at all, for example information on financial performance or business expansion plans. Such information falls outside the scope of the subject access request and there is no requirement to disclose it. It may be redacted, though unless it is confidential many data controllers provide it to avoid the time and effort of redaction.
- Having redacted data about the data subject that identifies other individuals and any information that is not personal data at all, the data controller will normally redact any non-relevant personal data.

Other Places to Look

Although most personal data will normally be found on the data controller's main servers, it is possible that there will be relevant data in backup servers or disks or data held on other systems or devices, for example on an individual's work hard drives, mobile devices, or home computers.

- Back up. To the extent that search mechanisms allow an employer to find backed up data for its own purposes, it should use the same effort to find data to respond to a subject access request.
- Deleted data. If data has been deleted, it is generally done with a view to removing it, as far as possible, from the data controller's system. Although it may be possible, at least in theory, to recreate it, that is not something that the Information Commissioner expects or requires.
- Data held on other systems. Unless the controller is data controller in relation to data held on other systems, it falls outside the scope of a subject access request. If data subjects hold data on the hard drive of their work PC, that will be covered by the request. If data subjects are permitted to hold personal data relating to work on their own devices, they may be acting as the data controller's agent and, if so, that data would be within the scope of the subject access request.

Changes to Data

The data controller is required to provide a copy of the personal data undergoing processing. The UK GDPR does not specify explicitly that data should be determined at the date of receipt of the request. But that is likely to be the position. Most data will not change at all; to the extent that data would change in the normal course (even if no subject access request had been made) the data

"undergoing processing" will be the data as modified. For example, data on total earnings in a particular tax year will change with every payroll; there is no requirement to freeze it in time or to reverse engineer it.

But the data controller must not delete data to defeat a subject access request. It is an offence for a controller, or a person employed by the data controller to alter or erase information with the intention of preventing disclosure (section 173(3), DPA 2018). There is a defence if the alteration or erasure would have occurred even if no data subject request had been made (section 173(5), DPA 2018). Doing so would breach the data protection principles (Article 5.1(a) in particular) and it would be unsurprising if the Information Commissioner took enforcement action.

Chapter 7 : Dealing with Information Relating to Another Individual

Data subjects' rights, including the right of subject access, are designed to protect privacy. There would be a potential clash of rights if, in responding to a request, a data controller needed to disclose information relating to another individual, potentially prejudicing his or her privacy. An example would be an email that said the data subject's work was poor. That is both information about the data subject and about the individual making the comment. A data controller is not required to disclose such information unless:

- The other individual has consented to the disclosure of the information to the data subject.
- It is reasonable to disclose the information to the employee without the consent of the other individual.

In approaching this, there are three main issues:

1. Does the request require disclosure of information that identifies another individual?
2. If it does, has the other individual consented to the disclosure?
3. Would it be reasonable to disclose without consent?

Does the Request Require Disclosure of Information that Identifies Another Individual?

The data controller should take account of not only the information itself but also any other information that they reasonably believe the data subject is likely to have, or may obtain, that would identify the third party.

Another individual is treated as identified if he or she is identified as the source of information regarding the data subject. For example, A's statement that "B's work is poor and he is always late" does not explicitly identify A. But B might identify A if B read that information in the light of his knowledge that A was his line manager, had concerns about his work and timekeeping and was likely to have expressed such a view.

Has the Other Individual Consented to the Disclosure?

If the other individual has consented, the data controller must disclose the information regarding that individual. Although the Information Commissioner's view is that, in general, it is good practice to seek consent, there is no obligation to seek consent and, in some cases, doing so may be impracticable or inappropriate. This may be the case where:

- The data controller does not have contact details for the third party.
- It would potentially disclose personal data about the data subject making the request to the third party that they were not already aware of.
- It would be inappropriate for the third party to know that the employee has made a subject access request.

If the individual refuses consent, that is a matter to which the data controller must have regard in considering whether to disclose without consent.

Would it be Reasonable to Disclose without Consent?

In deciding whether it is reasonable to disclose information without consent, the data controller must have regard to all relevant circumstances, including:

- The type of information that would be disclosed.
- Any duty of confidentiality.
- Any steps taken by the data controller with a view to seeking the consent of the other individual.
- Whether the other individual can give consent.
- Any express refusal of consent by the other individual (see paragraph 16(3) of Schedule 2 to the DPA 2018).

Exemptions to Providing Subject Access

There is no obligation to comply with a subject access request in relation to:

- Personal data in respect of which a claim of legal professional privilege could be maintained in legal proceedings (paragraph 19, Schedule 2, DPA 2018). This applies only to documents which carry legal professional privilege for the purposes of English law or its equivalent under Scottish law.
- Purely personal or household activity (see Article 2.2(a)). This covers personal information, but probably not records made personally in a work context.
- A reference given (or to be given) in confidence for employment, training, or educational purposes. The exemption covers the personal data within the reference whether processed by the reference giver or the recipient. (paragraph 24, Schedule 2, DPA 2018).
- Personal data processed for the purposes of management forecasting or management planning in relation to a business or other activity to the extent that complying with a subject access request would prejudice the conduct of the business or activity (paragraph 22, Schedule 2, DPA 2018). For example, it is likely to prejudice the conduct of a business if information on a staff redundancy programme is disclosed in advance of it being announced to the rest of the workforce.
- Personal data consisting of records of intentions in relation to negotiations between the data controller and the data subject to the extent that compliance with the subject access request would be likely to prejudice the negotiations (paragraph 23, Schedule 2, DPA 2018).

There are other exceptions relating to regulatory functions, judicial appointments and proceedings, the honours system, criminal investigations, tax collections and various corporate finance services (see Schedule 2 to the DPA 2018).

If an exemption to the rules on subject access is relevant, that personal data should be redacted or otherwise removed.

Chapter 8 : Supplying Information to the Data Subject: Required Contents

A response to a subject access request should include a copy of the personal data being processed plus certain additional information as explained below (Article 15(1), UK GDPR).

Much of the additional information is generally provided in the data controller's privacy notice and will appear in any record of processing activities prepared by the data controller for the purposes of Article 30, UK GDPR.

Form of Response

The data controller's response should be in writing or, if appropriate, by electronic means (Article 12(1), UK GDPR). If the request was made originally by electronic means, information should be provided "in a commonly used" electronic form unless otherwise requested by the data subject (Article 15(3), UK GDPR). There

If the employee requests, the information may be provided orally if the employer is satisfied as to the identity of the data subject (Article 12(1), UK, GDPR). Except in the most straightforward of cases, it is hard to see this having much application. You can find the responder's initial response letter template in chapter 12; and the responder's detailed response template in chapter 13. When using, please ensure you send your final draft on the organisation's headed paper.

Copy of the Personal Data

The data controller must supply a copy of the personal data concerning the data subject, subject to the rules on data that also identifies other individuals.

The following should be borne in mind:

- Although the requirement is to provide a copy of personal data, not a specific document, it will often be easiest to produce a copy of the document with redactions. The level of redaction will depend in part on the approach of the data controller.
- Redactions may be made to protect the identity of another individual who is identified through the data subject's personal data. Personal data that does not concern the data subject is also likely to be redacted. The data controller has no obligation to provide information that is not personal data at all (for example, information relating to business performance or to organisational arrangements), but it is often easiest and cheapest to supply that data unredacted.
- Although it will often be easiest to produce a copy document with redactions, the personal data could be extracted and copied to a different document.
- Personal data may be repeated in various places. If it is the same, it only need be provided once.
- Where there is a large quantity of largely repetitive data, a possible approach may be to summarise the data fairly and in reasonable detail. If such an approach is taken, it is essential that it is not used to hide information that the data controller prefers not to disclose; as a rule, if there is such data, that must be disclosed. This approach is underpinned by the principle of proportionality, so may be challenged by the data subject, and examined closely by the Information Commissioner.

- Make sure that when providing copies, there is no inadvertent disclosure of personal data about others. The Information Commissioner has produced some useful though quite technical guidance (see ICO: How to disclose information safely: removing personal data from information requests and datasets). The guidance looks at what it calls "Hiding in plain sight", of which a simple example would be Excel spreadsheets with hidden rows and columns that may contain data about others.

While the data controller must provide an initial copy of the data to the data subject, for any further copies requested by the data subject, the data controller may charge a reasonable fee based on administrative costs (Article 15(3), UK GDPR).

Purpose of Processing

When responding to a request, the data controller must provide information on the purposes of the processing. If the earlier statement of purposes was accurate, for reasons of consistency, the data controller should seek to use the description used in the privacy notices and record of processing activities.

Categories of Personal Data

Information should be provided on the categories of personal data concerned (see Article 15(1)(b)). It is not clear what categories are envisaged, but again it may have been referred to in the privacy notice (i.e., please see the URC website, for our Privacy Notice), or in an Article 30 record of processing activities.

Recipients of Categories of Recipient

The information should include the recipients or categories of recipient to whom personal data has been disclosed or to whom it will be disclosed (Article 15(1)(c)). A data controller need not identify each recipient; it is sufficient to identify categories of recipient. A recipient means a person, public authority, agency, or another body to which the personal data are disclosed, whether a "third party" (Article 4(9)). So, a recipient may be one of the data controller's employees.

Although it is context specific, some data will be disclosed to a range of recipients. For example, salary data is likely to be disclosed internally to a payroll department and to line managers in connection with salary reviews, to auditors and then to the employer's bank in connection with payment. Identifying recipients not only assists an individual in forming a view as to whether data is being processed fairly, lawfully, and otherwise consistently with the data protection principles, but also enables that individual to continue to track their data by making requests to other data controllers.

Information on Source of Personal Data

Except where the information originally came from the data subject making the request, the data controller should provide any available information on the source of the data (Article 15(1)(g)).

It is not entirely clear what "source" means. For example, if a GP supplies a medical report to life insurers who pass the information in it to an individual's employer, which then holds the information in its HR department, the source may be the GP, or, if the report by the GP is based on what the individual told the GP, the individual. If the data controller knew of the chain through which the information was passed, it would need to dig deeper than its HR department. Providing data subjects with information on the source of data enables them to follow their data back up the chain to ensure that the data controller at source is also processing lawfully.

Retention Periods

The response should, where possible, set out the envisaged period for which personal data will be stored. If it is not possible to set out a specific period, it should set out the criteria used to determine the period. Please contact the URC Records Management for further information on specific retention schedules.

Existence of Data Subject Rights

The information in the response should include the existence of the right to request rectification or erasure of personal data, the right to restrict processing of personal data and the right to object to processing of personal data. As these rights only apply in certain circumstances, the data controller may think it appropriate to explain more than the existence of the right or to provide a link to more information on the rights. (See Article 15(1)(e).)

Existence of Automated Decision-Making Including Profiling

If the data controller makes decisions based solely on automated processing, including profiling which produce legal or other significant effects, the data controller must provide information on the existence of the decision-making, the logic and envisaged significance for the data subject (see Article 15(1)(h)).

It is unlikely that a data controller will use automated decision-making, except perhaps at a job application stage when in some context's decisions may be automated. Although profiling is not uncommon in an employment context, decisions based solely on a profile are unusual. An example might be where an employer profiles employee absence and limits pay increases to staff with fewer than ten days' absence.

Transfer to a Third Country or International Organisations: safeguards

If personal data is transferred to a third country or to an international organisation, the data subject has a right to be told of any "safeguards" in place (see Article 15.2). These safeguards are listed in Article 46 and include standard model clauses and binding corporate rules.

Right to complain to the Information Commissioner's Office

The information should state that there is a right to lodge a complaint with the Information Commissioner (Article 15(1)(f)).

Chapter 9 : Challenges to the Response to a Subject Access Request

A data subject who is aggrieved and who believes that the data controller has failed to comply with the requirements of the UK GDPR has two main routes to challenging the response to a subject access request:

- Complaining to the Information Commissioner (Article 57(1)(f) read with section 165 of DPA 2018).
- Applying to a court for a compliance order (section 167, DPA 2018).

Complaint to the Information Commissioner

Most data subjects who are aggrieved will complain to the Information Commissioner. Even those who ultimately intend to apply to a court are likely to complain first to the Information Commissioner.

Data subjects can complain if they consider that, in connection with personal data relating to them, there has been an infringement of the UK GDPR (see Article 77 and section 165 of the DPA 2018). On receipt of a complaint, the Information Commissioner is under a duty to handle a complaint and to investigate the subject matter of the complaint "to the extent appropriate". The Commissioner must then inform the data subject of the progress of the complaint and the outcome of the investigation within a reasonable period, if further investigation is necessary (see Articles 57(1)(f), 77 and 78).

In handling the complaint, the Commissioner has two main options:

- First, the Commissioner may decide that having investigated to some extent, though there may be an infringement of the UK GDPR, the position is not clear. If so, it may say that it is not appropriate to investigate further in the circumstances, including, for example, the nature of the alleged infringement or its own priorities on allocation of resources.
- The data subject may apply to the Information Tribunal if the Commissioner "fails to take appropriate steps to respond" to a complaint (see section 166 of the DPA 2018). The tribunal may make an order requiring the Commissioner to take specified steps (see section 166(3)).

Although it is not clear how the Information Tribunal would treat such an application, it may be that an employee could apply to a tribunal on the basis that the service of an assessment order was an appropriate step and, in the circumstances of the case, seeking an order that the Commissioner serve an assessment notice.

- Second, the Commissioner may take the view that further investigation or action is appropriate. In those cases, in addition to simply continuing its investigation, the Information Commissioner may serve an assessment notice on the employer (section 146, DPA 2018). In these circumstances, the Commissioner has wide-ranging powers, including powers to enter premises, see documents, observe the processing of personal data in action and interview specified staff.

The Commissioner has power to use an assessment notice whether there is a specific complaint. It may use the process if on receiving one or more complaints it believes that there may be serious wrongdoing which warrants use of the extensive powers granted by section 146.

Failure to comply with an assessment notice can lead to the service of a penalty notice (see section 155 of the DPA 2018).

The Commissioner is under a duty to produce guidance on assessment, enforcement and penalty notices and may cover other functions such as complaints handling.

The fact that a data subject can apply to the Information Tribunal in relation to the handling of a complaint may lead to greater formality and "judicialisation" in the resolution of disputes.

Remedy against a Controller or Processor

A data subject can apply to a court alleging an infringement of his or her rights under the UK GDPR or DPA 2018 (section 165, DPA 2018). The court "may make an order for the purposes of securing compliance" (section 167(2), DPA 2018). The court will seek a fair balance between the rights of the data subject and the interests of the controller

Factors to be considered depend on the circumstances but may include:

- The nature and gravity of the breach.
- Whether there is a more appropriate route to obtaining information, such as disclosure (this does not affect the right to make the request but may be relevant in the exercise of discretion by the court).
- Whether the real aim is to see documents rather than personal data.
- The reason for making the subject access request
- The potential benefit to the data subject and whether he or she legitimately wishes to check the accuracy of personal data.

Chapter 10 : Responding to a Subject Access Request: checklist

- Check that a subject access request has been received.
- Decide who does what. There are frequently three levels of staff involved:
    - senior manager taking overall responsibility for ensuring that a compliant response is sent and who, if necessary, liaises with the Information Commissioner.
    - operational manager responsible for: instructing staff to search for relevant data. approving access to individual mailboxes; deciding on any difficult issues such as sensitive redactions or, in marginal cases, whether data is personal data; where data relates to other individuals, deciding whether to seek consent or whether it is reasonable to disclose without consent; and finalising and approving the information in the response.
    - operational and administrative support involving locating data; searching the data (and logging searches made); and identifying data relating to other individuals and, if appropriate, seeking consent.

Input from IT may also be appropriate, particularly if access to individual mailboxes is required.

- Ensure that staff working on the subject access request have sufficient training to carry out their roles.
- Make an initial assessment:
    - check identity of data subject making request;
    - work out the final date for response;
    - decide whether to clarify the scope of the request with data subject and what he or she wants;
    - consider whether or not request is manifestly unfounded or excessive and, if so, approach to take; and
    - if practicable, make a rough estimate of the number of documents to review.
- Decide whether to extend time and, if so, notify data subject.
- Find and retrieve personal data:
    - identify pool of data that is personal data about the data subject;
    - seek to narrow data in the pool using appropriate criteria;
    - review data identified to see if they contain data relating to other individuals;
    - decide whether to seek consent of other individuals, disclose without consent or refuse to disclose;
    - make any redactions;
    - consider whether any exemptions to the subject access rules apply and, if so, redact or otherwise remove that data; and
    - finalise copy data to be disclosed.
- Prepare response to data subject with copies of documents and information on:
    - purposes of processing;
    - categories of personal data;
    - recipients or categories of recipient;
    - information on source of personal data;

- retention periods;
- existence of data subject rights;
- existence of automated decision-making including profiling;
- safeguards on transfers to a third country or international organisation; and
- right to complain to the Information Commissioner.

Chapter 11 Subject Access Request Form

The Data Protection Act 2018 grants you the right to access your personal data held by The United Reformed Church and The United Reformed Church Trust. This includes:

- The right to obtain confirmation that we process your personal data.
- The right to receive certain information about the processing of your personal data. [This is information about the purposes for the processing, the categories of data concerned, the recipients or categories of recipients, where possible the period for which we store the data and any information about the source of the data where this is not direct from you. Where relevant this also includes information about automated decision-making and international transfers.
- The right to obtain a copy of the personal data we process.

For us to respond to your request, we ask that you submit this request in writing:

Post
United Reformed Church House,
86 Tavistock Place,
London, WC1H 9RT

Email
info@urc.org.uk

We expect to respond to your request within one month of receipt of a valid request. You do not have to use this form but using this form should make it easier for you to check you have provided us with all relevant information, including proof of identity, and for us to process your request.

In addition to exercising your access right, you have the right to:

- Request correction or erasure of your personal data.
- Restrict or object to certain types of data processing.
- Make a complaint with the local data protection authority (in the UK this is the Information Commissioner, see https://ico.org.uk).

For more information on your rights, see our Privacy Notice available at: https://urc.org.uk/privacy-policy.html

1. Requester name (data subject) and contact information

Please provide the data subject's information below. If you are making this request on the data subject's behalf, you should provide your name and contact information in paragraph 3.

We will only use the information you provide on this form to identify you and the personal data you are requesting access to, to respond to your request and to keep a record of your request and our response.

First and last name:	

Any other names that you have been known by (including nicknames and previous surnames):	
Home address:	
Date of birth:	
Telephone number:	
Email address:	
Are you a current or former worker of The United Reformed Church?	
If so, please tell us which department/synod and your approximate date of commencement:	

2. Proof of data subject's identity

We require proof of your identity before we can respond to your access request. To help us establish your identity, you must provide identification that clearly shows your name, date of birth and current address. We accept a photocopy or a scanned image of one of the following as proof of identity:

- Passport or photo identification such as a driving licence.
- Birth or adoption certificate.

Please also attach a copy of a bank or credit card statement or utility bill showing your current address and dated within the last three months. If you have changed your name, please provide the relevant documents evidencing the change.

If you do not have any of these forms of identification available, please contact us info@urc.org.uk for advice on other acceptable forms of identification.

We may request additional information from you to help confirm your identity and your right to access, and to provide you with the personal data we hold about you. We reserve the right to refuse to act on your request if we are unable to identify you.

3. Requests made on a data subject's behalf

Please complete this section of the form with your name and contact details if you are acting on the data subject's behalf.

First and last name:	
Home address:	
Date of birth:	
Telephone number:	
Email address:	
What is your relationship to the data subject (for example, solicitor, another adviser, parent, carer)?	
Do you have legal authority to request the data subject's information?	

If the data subject is under 13, do you have parental authority to act for them?	

We accept a photocopy or a scanned image of one of the following as proof of your identity:

- Passport or photo identification such as a driving licence.
- Birth or adoption certificate.

If you do not have any of these forms of identification available, please contact us info@urc.org.uk for advice on other acceptable forms of identification. We may request additional information from you to help confirm your identity if necessary.

We also require proof of the data subject's identity before we can respond to the request. To help us establish the data subject's identity, you must provide identification that clearly shows the data subject's name, date of birth and current address. We accept a photocopy or a scanned image of one of the following as proof of identity:

- Passport or photo identification such as a driving licence.
- Birth or adoption certificate.

Please also attach a copy of a bank or credit card statement or utility bill showing the data subject's current address and dated within the last three months. If the data subject has changed his **or** her name, please provide the relevant documents evidencing the change.

We accept a copy of the following as proof of your legal authority to act on the data subject's behalf:

- A written consent signed by the data subject.
- A certified copy of a power of attorney.
- Evidence of parental responsibility.

We may request additional information from you to help confirm the data subject's identity. We reserve the right to refuse to act on your request if we are unable to identify the data subject or verify your legal authority to act on the data subject's behalf.

4. Information requested

To help us process your request quickly and efficiently, please provide as much detail as possible about the personal data you are requesting access to. Please include time frames, dates, names, types of documents, file numbers, or any other information to help us locate your personal data.

For example, you may specify that you are seeking:

- Employment records or personnel records.
- Pensions or other benefit records.
- Personal data held by a specific department.
- Medical records.
- Email or other electronic communications (specify the approximate dates, times, and correspondents).
- Billing information.
- Photographs.

- Video footage.
- User activity logs.
- Transaction histories.
- Correspondence between [NAME] and [NAME] between [DATE] and [DATE].

We will contact you for additional information if the scope of your request is unclear or does not provide sufficient information for us to conduct a search (for example, if you request "all information about me"). We will begin processing your access request as soon as we have verified your identity and have all the information, we need to locate your personal data.

In response to your request, we will provide you with the information we are required to provide, including information on:

- The purposes of processing.
- Categories of personal data processed.
- Recipients or categories of recipients who receive personal data from us.
- How long we store the personal data, or the criteria we use to determine retention periods.
- Any available information on the source of the personal data if we do not collect it directly from you.
- Whether we use automated decision-making, including profiling, meaningful information about the auto-decision logic used, and the significance and consequences of this processing.
- Your right to:
    - request correction or erasure of your personal data;
    - restrict or object to certain types of processing with respect to your personal data; and
    - make a complaint to the local data protection authority.

If the information you request reveals personal data about a third party, we will either seek that individual's consent before responding to your request, consider if it is otherwise reasonable to provide it to you or we will redact third parties' personal data before responding. If we are unable to provide you with access to your personal data because disclosure would infringe the rights and freedoms of third parties, we will notify you of this decision.

Applicable law may allow or require us to refuse to provide you with access to some or all the personal data that we hold about you, or we may have destroyed, erased, or made your personal data anonymous in accordance with our record-retention obligations and practices. If we cannot provide you with access to your personal data, we will inform you of the reasons why, subject to any legal or regulatory restrictions.

Signature and acknowledgement

I, [ ], confirm that the information provided on this form is correct and that I am the person whose name appears on this form. I understand that:

- The United Reformed Church/The United Reformed Church Trust (please delete one) must confirm proof of identity and may need to contact me again for further information.
- My request will not be valid until The United Reformed Church/The United Reformed Church Trust (please delete one), receives all the required information to process the request.

- I am entitled to one free copy of the personal data I have requested, and acknowledge that, for any further copies I request, The United Reformed Church/The United Reformed Church Trust (please delete one) may charge a reasonable fee based on administrative costs.

If you would like to receive a copy of the personal data you are requesting access to, please indicate below whether you would like a hard copy or an electronic copy:

	Hard copy.
	Electronic copy.

……

Signature

……

Date

Authorised person signature

I, [ ], confirm that I am authorised to act on behalf of the data subject. I understand that The United Reformed Church/The United Reformed Church Trust (please delete one) must confirm my identity and my legal authority to act on the data subject's behalf and may need to request additional verifying information.

……

Signature

……

Date

Chapter 12 : Data Controller's Initial Response Letter

[REQUESTER NAME]

[ADDRESSEE]

[ADDRESS LINE 1]

[ADDRESS LINE 2]

[POSTCODE]

[DATE]

Dear [REQUESTER]

Your data subject access request

I write to acknowledge receipt of your data subject access request [and the copy of your [driving licence **OR** passport **OR** IDENTIFY DOCUMENT] as confirmation of your identity] which we received on [DATE].

EITHER

[We intend to respond to your request as soon as possible but will respond at the latest within one month from the date of receipt referred to above.

OR

[ORGANISATION] processes a large amount of information about you and it is not clear from your request what information you are asking for. [While we have not been able to search fully at this stage, we anticipate that there may be some [NUMBER] emails and [NUMBER] documents to review.] To enable us to best deal with your request we need you to specify the information or processing activities that your request relates to. Please provide the following details about the information that you want to receive: [SET OUT REQUIRED INFORMATION SUCH AS THE CONTEXT IN WHICH THE ORGANISATION MAY HAVE PROCESSED INFORMATION, THE LIKELY DATES OF IT BEING PROCESSED AND IDENTITIES OF PARTIES INVOLVED IN PROCESSING].

[We need you to respond by [DATE] [because SET OUT REASONS].]

The time for [ORGANISATION] to respond to your request will now be paused and will restart from the date that we receive your response [when we will contact you again to advise when we will be able to provide a detailed response to your request].

OR

Your request is complex for the following reasons [SET OUT REASONS].

We will endeavour to respond to your request as quickly as possible and in any event within three months of the receipt of your request.

[In the meantime, please find enclosed a copy of [ORGANISATION]'s privacy notice which sets out the types of information we hold about you, how we process that information and your rights in relation to that information.]

[DATA PRIVACY OFFICER **OR** DATA PROTECTION MANAGER **OR** IDENTITY] will be responsible for overseeing the response to your request. If you have any questions about your request or the content of this letter, please contact them [PROVIDE CONTACT DETAILS].

Yours sincerely,

…….

[NAME OF SENDER]

Chapter 13 : Data Controller's Detailed Response

[REQUESTER'S NAME]

[ADDRESSEE]

[ADDRESS LINE 1]

[ADDRESS LINE 2]

[POSTCODE]

[DATE]

Dear [DATA SUBJECT]

Response to your data subject access request

We write further to your subject access request [and our acknowledgment letter of [DATE]].

Enclosed with this letter are copies of personal data relating to you.

[Further to your request to us dated [DATE], we can provide the following details which may enable you to determine whether you wish to make a subject access request relating to a particular matter.

Your rights in connection with personal data

You may be interested to know of certain rights that you have in connection with your personal data. You have the right to correct the personal data that we hold about you or restrict the processing of your personal data under certain circumstances. You may also, under certain circumstances, have the right to object to the processing or to request erasure of your personal data. [These rights are set out in the enclosed copy of the privacy notice [which was previously provided to you [INSERT DETAILS].]

Additionally, [as also explained in the privacy notice,] you have the right to make a complaint to the Information Commissioner's Office (ICO) which is an independent body whose role is to uphold information rights. For further information, see the ICO website at *https://ico.org.uk/make-a-complaint/*.

We can confirm the following in respect of the data existing on the date your request was made:

THE PURPOSES FOR WHICH THE PERSONAL DATA IS PROCESSED

[LIST OF PURPOSES]

THE CATEGORIES OF PERSONAL DATA CONCERNED

[LIST OF CATEGORIES OF PERSONAL DATA]

THE RECIPIENTS OR CATEGORIES OF RECIPIENTS TO WHOM THE PERSONAL DATA HAS OR MAY HAVE BEEN DISCLOSED

[LIST OF RECIPIENTS (BY NAME OR GENERIC CLASS) TO WHOM DATA DISCLOSED]

THE PERIOD FOR WHICH PERSONAL DATA WILL BE STORED OR CRITERIA USED TO DETERMINE THAT PERIOD

[LIST OF CATEGORIES OF DATA AND PERIOD STORED OR CRITERIA USED TO DETERMINE THAT PERIOD]

ANY INFORMATION AVAILABLE TO THE UNITED REFORMED CHURCH/THE UNITED REFORMED CHURCH TRUST ON THE SOURCE OF THE DATA

[IDENTIFY SOURCES OF DATA HELD]

[Some names and identifying particulars have been deleted to protect the identity of third parties.]

[SOME PERSONAL DATA HAS BEEN OMITTED FOR THE FOLLOWING REASONS:]

[It is subject to legal privilege.]

[It consists of a confidential reference given by us for employment purposes.]

[It consists of records of intentions in relation to negotiations between us and you, disclosure of which we consider would be likely to prejudice those negotiations.]

[It consists of health records and we consider that disclosure would be likely to cause serious harm to another person.]]

We have done our best to respond to your request and hope that you have found our approach helpful. You will see that when providing copies of personal data, we have sometimes gone beyond what is required in that not all the information provided, strictly speaking, constitutes personal data relating to you.

Please do not hesitate to contact us if you have any questions about the contents of this letter.

Yours sincerely,

……

[NAME OF SENDER]