MAZE LONG KESH Development Corporation

Managing Subject Access and other GDPR Requests

Author:	
Version:	1.0
Date:	4 September 2018
HP Records Manager Ref:	FI1/18/789902

CONTENTS

INTRODUCTION

This document sets out the procedures that the Maze Long Kesh Development Corporation (MLKDC) will follow should it receive a request under the General Data Protection Regulation (GDPR) to exercise rights available to an individual. The most likely request is a Subject Data Request (SAR) asking for personal information held by MLKDC but this document also covers the additional rights of data subjects under data protection legislation in relation to their personal data. These additional rights are:

- Rectification;
- Erasure;
- Restriction of processing;
- Portability (of their data);
- Objection to processing;
- Rights in respect of automated decision making and profiling.

A further right, the right to be informed, is addressed through MLKDC's Privacy Notice that is available on its website, although you should consider when responding to a request whether further information should be given (see Section 1.8.2 below).

The procedures are aimed at all MLKDC staff who should read the *Quick Guide on SARs for MLKDC Staff* below. If you have any questions arising from the procedures ask the MLKDC Data Protection Officer (DPO).

This procedures document reflects the changes to data protection brought in by the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018) that both came into force on 25 May 2018. You should read this procedures document in conjunction with the MLKDC GDPR and Data Protection Policy and Procedures

If you receive a request for information under the data protection legislation, a request to exercise a 'GDPR right', or a request for information relating to personal information possibly held by MLKDC you must inform the MLKDC Data Protection Officer (DPO) immediately. In the absence of the DPO inform the Chief Executive Officer (CEO).

QUICK GUIDE ON SARS FOR MLKDC STAFF

A flow chart, summarising the steps in the MLKDC process for dealing with SARs under GDPR is shown in Figure 1 below. The following is a broad overview of what you should do if you think you may have received a SAR. The process applies, with appropriate modifications, to all of the rights noted above.

You must act on a SAR without undue delay and within one month of receipt. For all practical purposes this is a 28 day time limit (see Section 2.3 below). This time limit applies for all the other data protection subject requests (see Section 3 below).

You are responsible for identifying SARs and telling the DPO and/or the CEO who will then manage the process.

Remember, this is personal data so the records for dealing with a SAR must be appropriately secured and restricted in HPRM.

MLKDC's procedures are set out in three main parts. First, *Dealing with a Subject Access Request (SAR***)** on page 7; second, *Right of Access by the Data Subject* on page 12, which summarises the legal bases for SARs and third, *Other GDPR Rights of the Individual* on page 14.

Although you may be asked to search for or otherwise account for the personal data asked for in a SAR or other request, MLKDC's response should only be made by the DPO or the CEO (or in the absence of either, the person nominated to do so by the CEO or the DPO).

WHAT IS A SAR?

A SAR is the individual asking for details of their personal data held by MLKDC. If it is not asking for personal data then it is not a SAR, but it may be a Freedom of Information request instead, so still inform the DPO/CEO.

The GDPR does not specify how to make a valid request.

- An individual can make a SAR to MLKDC verbally or in writing.
- A SAR can be made to any part of MLKDC (including by social media). A SAR does not have to be to a specific person or contact point such as the DPO, although MLKDC encourages individuals to email the DPO.
- The request does not even need to state that it is a SAR or that it is a request made under the provisions of the GDPR or the Data Protection Act 2018.

An individual is only entitled to their own personal data, and not to information relating to other people (unless the information is also about them, or they are acting on behalf of someone and authorised to do so).

A *Subject Access Request Process Flowchart* can be found at Figure 1 below. The steps for dealing with a SAR can be summarised as follows:

1. Log and acknowledge (see Section 1.1 below).
2. Verify the subject's identity (see Section 1.2 below).
3. If a third party is acting on behalf of the data subject, verify their identity, the identity of the data subject and verify authorisation from the data subject (see Section 1.3 below).
4. If it is not already clear, request clarification of the personal information being asked for (see Section 1.4 below).
5. Carry out searches for the information requested (see Section 1.5 below).
6. Collate the results of the information into a suitable format (see Section 1.6 below).
7. Confirm that there are no reasons for refusing the request in full or in part (see Section 1.7 below).
8. Respond to the request by providing the information or if refusing the request explaining why not (see, Section 1.8 below).
9. Ensure all the necessary records have been filed in HPRM and update the logs (see Section 1.9 below).

WHAT IS PERSONAL DATA?

Personal data means any information relating to an identified or identifiable natural person (data subject). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. GDPR does not apply to deceased individuals.

The Information Commissioner's Office (ICO) guide to What is personal data? expands on this.

- If it is possible to identify an individual directly from the information you are processing, then that information may be personal data.
- If you cannot directly identify an individual from that information, then you need to consider whether the individual is still identifiable. You should take into account the information you are processing together with all the means reasonably likely to be used by either you or any other person to identify that individual.
- Even if an individual is identified or identifiable, directly or indirectly, from the data you are processing, it is not personal data unless it relates to the individual. That is, the information does more than simply identifying them. It must concern the individual in some way.
- When considering whether information relates to an individual, you need to take into account a range of factors, including the content of the information, the purpose or purposes for which you are processing it and the likely impact or effect of that processing on the individual.

- Information which has had identifiers removed or replaced in order to pseudonymise the data is still personal data for the purposes of GDPR. However, information which is truly anonymous is not covered by the GDPR.
- Even if information that seems to relate to a particular individual is inaccurate (i.e. it is factually incorrect or is about a different individual), the information is still personal data, as it relates to that individual.

The ICO recommends that all SARs should be recorded and logged and in particular, it recommends keeping a log of verbal requests. The DPO will keep this log.

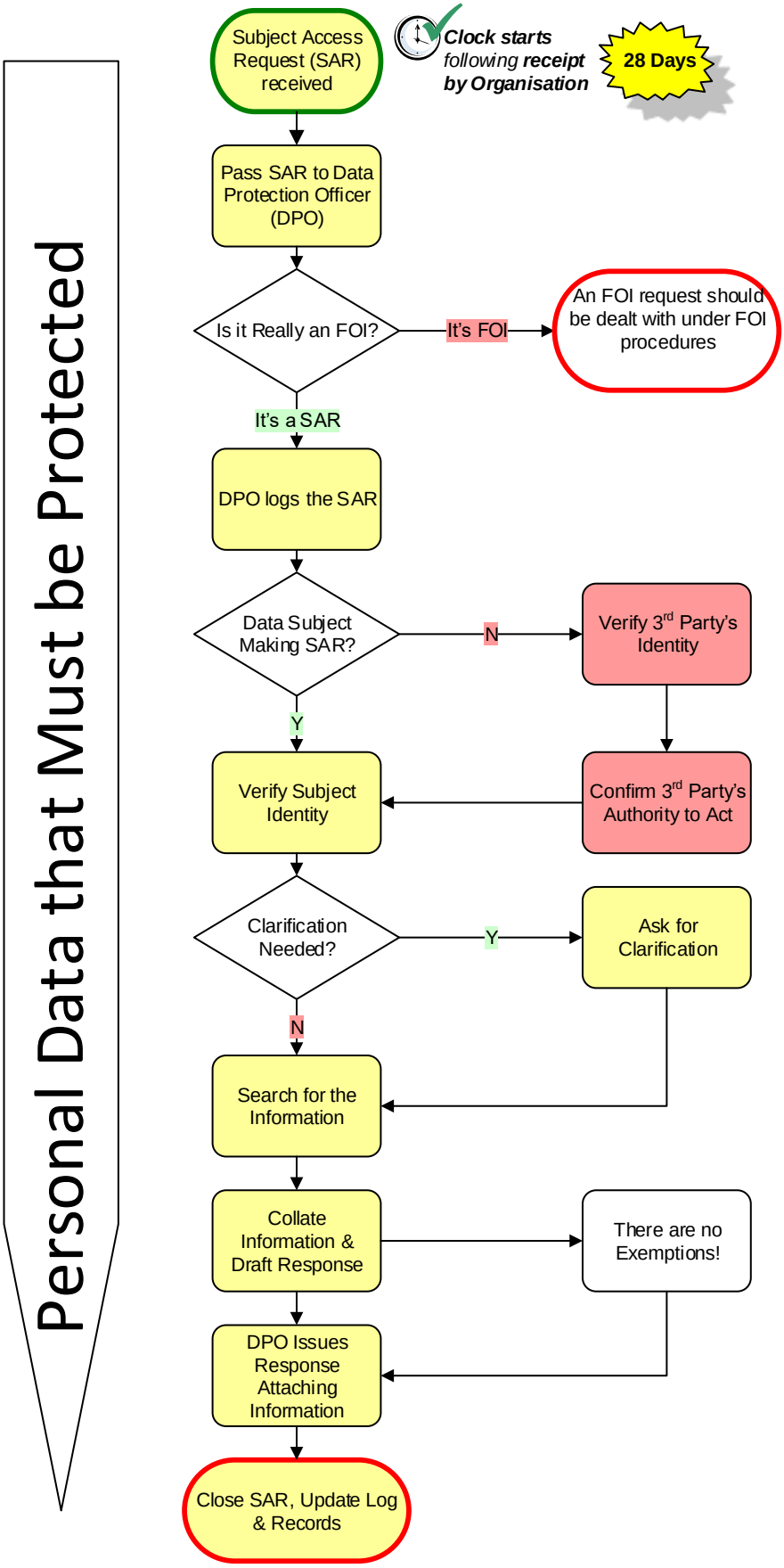

Figure 1: Subject Access Request Process Flowchart

1. DEALING WITH A SUBJECT ACCESS REQUEST (SAR)

You must not deal with a SAR on your own. Always make sure that the DPO and/or the CEO have been informed of the request. They may delegate tasks in dealing with the SAR but one of them will manage the process.

Remember, this is personal data so the records for dealing with a SAR must be appropriately secured and restricted in HPRM.

See Section 3 below for the other kinds of subject request that might be made. These instructions should be adapted as appropriate.

1.1 Log and acknowledge the request

The steps are:

1. Create an HPRM container – see Section 1.1.1 below.
2. File the SAR and any subsequent correspondence and records in this container.
3. Where appropriate, create a Subject Access Request Log to keep track of progress, actions taken and to provide a summary record of how MLKDC dealt with the SAR. In all but the simplest of cases this will always be appropriate.
4. Send out the appropriate acknowledgement (see the standard wordings starting at Appendix 2 below).

1.1.1 HPRM Containers

Under GDPR, MLKDC has to keep various records. All documentation on data protection requests is kept in HPRM. The DPO will set up individual containers for each SAR named in the format 'Subject Access Request - SAR <yynn> - <data subject name> - <dd-mmm-yy>' (e.g. Subject Access Request - SAR 1701 – James Bond - 26-Oct-17). By default, access to the containers should be restricted to the DPO and CEO.

1.2 Verifications

You must be sure of the identity of the person making the SAR before providing any personal information to them.

Confirm that they are the data subject. The GDPR provides that this should be done using what it describes as 'reasonable means' (Article 64). However the ICO guidance makes clear you should only request information that is necessary to confirm who they are, the key being proportionality.

- You need to let the individual know as soon as possible that you need more information from them to confirm their identity before responding to their request. The period for responding to the request begins when you receive the additional information.
- You will appreciate that fraudsters who want to steal identities or others seeking information may pretend to be someone else and persuade MLKDC to release personal data. It is vital that MLKDC does not fall victim to a scam or impersonation.
- You should ask for enough information to judge whether the person making the request is the individual to whom the personal data relates. At the same time you must be reasonable and not demand large amounts of information.

There are a number of ways to verify identity, some more intrusive than others. In general MLKDC will be content with a photocopy or scanned image of documents. Original documents should not be asked for.

- Proof of identity in the form of passports, driving licenses, birth certificates and utilities letters.
- Phoning the person to ask them questions based on the data which you hold. Questions to which only the real subject would know the answer. (This must be documented).
- On a balance of rights versus obligations, annoying someone by asking them to provide additional information is preferable to disclosing confidential data to the wrong person.

1.3 Requests on behalf of others

The GDPR does not prevent an individual making a subject access request via a third party. This may be a solicitor acting on behalf of a client or someone holding power of attorney.

In these cases, you need to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney. The ICO gives examples where it may be reasonable to voluntarily disclose information and other examples where it would not be unreasonable to require more formal authority.

If someone is acting on behalf of the data subject they must provide:

- Their authorisation – the data subject's written authority, their power of attorney, etc.
- Proof of the data subject's identity (as noted in Section 1.2 above).
- Similarly, proof of their own identity (as noted in Section 1.2 above).

1.4 Clarifications

Unlike the Freedom of Information legislation, there is no formal process for an organisation to ask for clarification on what is being requested under GDPR. The ICO view is that delaying responding to a SAR is only justified as follows:

You can extend the time to respond by a further two months if the request is complex or you have received a number of requests from the individual. You must let the individual know within one month of receiving their request and explain why the extension is necessary.

However, it is the ICO's view that it is unlikely to be reasonable to extend the time limit if:

- It is manifestly unfounded or excessive.
- An exemption applies.
- You are requesting proof of identity before considering the request.

Where an organisation processes a large amount of information about an individual it can ask them for more information to clarify their request. It should only ask for information that it reasonably needs to find the personal data covered by the SAR. It is unlikely that MLKDC would be such an organisation.

You need to let the individual know as soon as possible that you need more information from them before responding to their request. The period for responding to the request begins when MLKDC receives the additional information asked for but this must not be used as a means of extending the deadline for responding to a SAR.

If an individual refuses to provide any additional information, you must still endeavour to comply with their request: i.e. by making reasonable searches for the information covered by the request.

1.5 Searching for the information

Potentially, personal information may be stored anywhere. It may be paper based or electronic and it may have multiple formats (e.g. a recording would be personal information if it identified and related to an individual). See 'What is Personal Data?' below.

1.5.1 Searching HPRM

You can carry out a search of HPRM for personal information relating to the data subject. However, you need to take steps to make sure the search is comprehensive.

1. Your access rights within HPRM may mean that you miss some hits because you do not have access. For example, some finance containers will be restricted to finance staff.
2. Always formally request an HPRM administrator (through ITAssist) to carry out the search or at least get an administrator to double-check your results. Administrators will not have access restrictions on what they can see. Also they have much higher limits on the number of 'hits' that they can see.
3. It is not enough to rely on record titles, you need to do a full text search of the document content in HPRM (search on 'Document Content'). Searches for phrases should be

enclosed with inverted commas, e.g. 'james bond'. Full text search does work in HPRM. For example, a SAR from James Bond would require you to search at least for < 'james bond' or 'jim bond' or 'bond, james' or 'bond, jim' or '007' >.

1.5.2 Other Data within MLKDC

You should check all possible places where the personal data may be stored in MLKDC, including paper records. This might include but is not limited to:

- Individual staff Outlook email accounts.
- Hard disks on computers (e.g. ask the relevant staff to confirm that they have both searched for and provided all the personal data on their hard drives relevant to the SAR).
- Photographs, etc.
- Other database or computer systems (e.g. Finance).

Do not forget personal information may be held by data processors acting for MLKDC.

The following documentation maintained by MLKDC should help in identifying which information assets may hold personal data, and that may be pertinent to the SAR:

- GDPR Data Controller Register; and
- Information Asset Register.

The ICO advises the following (in Right of access):

If we use a processor, does this mean they would have to deal with any subject access requests we receive?

'Responsibility for complying with a subject access request lies with you as the controller. You need to ensure that you have contractual arrangements in place to guarantee that subject access requests are dealt with properly, irrespective of whether they are sent to you or to the processor. More information about contracts and liabilities between controllers and processors can be found here.

You are not able to extend the one month time limit on the basis that you have to rely on a processor to provide the information that you need to respond. As mentioned above, you can only extend the time limit by two months if the request is complex or you have received a number of requests from the individual.'

1.6 Collating the search results

You should collate the information into a suitable format for passing to the requestor. The format should match or relate to the way the request was made. If the request was by way of an email then an email enclosing the information may be appropriate. However, you must bear in mind the security of transmission since this is personal data. The ICO advises, *'If an individual makes a request electronically, you should provide the information in a commonly used electronic format, unless the individual requests otherwise.'* You should confirm with the requestor how they wish to receive the data.

1.7 Grounds for refusing a request and exemptions

The only grounds for MLKDC refusing to comply with a SAR are if it is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature.

If you consider that a request is manifestly unfounded or excessive MLKDC can:

- Request a 'reasonable fee' to deal with the request. A reasonable fee should be based on the administrative costs of complying with the request. Any decision on charging a fee can be taken only by the DPO and the CEO after consultation. If MLKDC were to decide to charge a fee, you should contact the individual promptly and inform them. MLKDC would not need to comply with the request until you have received the fee but **this must not be used as a means of extending the deadline for responding to a SAR;** or

- Refuse to deal with the request.

In either case MLKDC has to justify its decision.

There are no exemptions as such under GDPR but it does allow individual states to determine exemptions. There are other exemptions from the right of access in the UK Data Protection Act 2018, which will apply in certain circumstances, broadly associated with why an organisation is processing the data. The ICO (at June 2018) states that, *'We will provide guidance on the application of these exemptions in due course'.*

1.7.1 Information relating to another individual

Responding to a SAR may involve providing information that relates both to the individual making the request and to another individual.

The Data Protection Act 2018 says that you do not have to comply with the request if it would mean disclosing information about another individual who can be identified from that information, except if:

- The other individual has consented to the disclosure; or
- It is reasonable to comply with the request without that individual's consent.

In determining whether it is reasonable to disclose the information, you must take into account all of the relevant circumstances, including:

- The type of information that you would disclose.
- Any duty of confidentiality you owe to the other individual.
- Any steps you have taken to seek consent from the other individual.
- Whether the other individual is capable of giving consent.
- Any express refusal of consent by the other individual.

Although you may sometimes be able to disclose information relating to a third party, you need to decide whether it is appropriate to do so in each case. This decision will involve balancing the data subject's right of access against the other individual's rights. If the other person consents to you disclosing the information about 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.

For the avoidance of doubt, you cannot refuse to provide access to personal data about an individual simply because you obtained that data from a third party. The rules about third party data apply only to personal data which includes both information about the individual who is the subject of the request and information about someone else.

1.8. Providing the information

The GDPR requires that the information MLKDC provides to an individual is in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

At its most basic, this means that the additional information MLKDC provides in response to a request (see Section 1.8.2 below) should be capable of being understood by the average person. However, MLKDC is not required to ensure that that the information itself is provided in a form that can be understood by the particular individual making the request.

1.8.1 Personal Information

The data subject has the right to obtain the following from MLKDC:

- Confirmation that it is processing their personal data.
- A copy of their personal data.
- Other supplementary information. This largely corresponds to the information that is provided in the MLKDC privacy notice (see Section 1.8.2 below).

1.8.2 Other Information

In addition to a copy of their personal data, you also have to provide individuals with the following information:

- The purposes of MLKDC's processing.

- The categories of personal data concerned.
- The recipients or categories of recipients MLKDC discloses the personal data to.
- MLKDC's retention period for storing the personal data or, where this is not possible, its criteria for determining how long it will store the data.
- The data subject's right to request rectification, erasure or restriction or to object to such processing.
- The right to lodge a complaint with the ICO or another supervisory authority.
- Information about the source of the data, where it was not obtained directly from the individual.
- The existence of automated decision-making including profiling. (MLKDC does not use automated decision-making).
- The safeguards MLKDC provides if it were to transfer personal data to a third country or international organisation. (MLKDC does not do this).

Much of this information should already be in MLKDC's Privacy Notice available on its website but check whether there is any additional information that you should provide.

1.9 Record Keeping

Make sure that you record all the actions that MLKDC takes to deal with the SAR and file everything securely in HPRM (see Section 1.1.1 above).

The records relating to the SAR will of necessity contain personal information themselves. They need to be appropriately secured and are also subject to the same rules on personal data under GDPR: e.g. they should be kept no longer than needed. The ICO does not provide specific guidance on this although in relation to Freedom of Information (Retention and destruction of requested information) it does recommend that *'…a public authority retain the requested information for a period of at least six months from the date of the last communication about the request, or related appeals, to allow for the appeal process.'* The NICS retention schedule for Freedom of Information (followed also by MLKDC) is three years.

Bear in mind that the personal information will already be in MLKDC's records system (for its original purpose) and subject to a retention and disposal schedule. The only records relevant to MLKDC are demonstrating that it received a request and how it dealt with it. Therefore the MLKDC DPO's recommendation is:

- The SARs Action Log (Section 1.1 above) should be retained for three years. This provided a record that the SAR was made, references the sources of the personal information, and that MLKDC dealt with it. This is long enough to deal with any enquiries, manage business statistics and deal with repeat SARs.
- The correspondence and other records directly relating to the SAR need be retained for one year and no longer than three years. This should be long enough to deal with repeat SARs.
- The register of SARs should have the same retention as MLKDC's general business records, which is six years.

2. RIGHT OF ACCESS BY THE DATA SUBJECT

A key provision of GDPR is Article 15, which provides for a 'Right of access by the data subject'. It is the right of all individuals to know what data is held about them by businesses and other organisation and how that data will be used.

In summary:

- Individuals have the right to access their personal data.
- This is commonly referred to as subject access.
- Individuals can make a subject access request verbally or in writing.
- You have one month to respond to a request.
- You cannot charge a fee to deal with a request in most circumstances.

The ICO provides guidance on the right of access on its website.

2.1 What is the individual entitled to?

Individuals have the right to obtain the following from MLKDC:

- Confirmation that MLKDC is processing their personal data.
- A copy of their personal data held by MLKDC.
- Other supplementary information. This largely corresponds to the information that MLKDC specifies in its privacy notice.

An individual is only entitled to their own personal data, and not to information relating to other people unless the information is also about them or they are acting on behalf of someone. Therefore, it is important that you establish whether the information requested falls within the definition of personal data.

2.2 Other Information

In addition to a copy of their personal data, MLKDC also has to provide individuals with the following information:

- The purposes of its processing.
- The categories of personal data concerned.
- The recipients or categories of recipient that MLKDC discloses the personal data to.
- The retention period for storing the personal data or, where this is not possible, MLKDC's criteria for determining how long it will store the data.
- The existence of the data subject's right to request rectification, erasure or restriction or to object to such processing.
- The right to lodge a complaint with the ICO or another supervisory authority.
- Information about the source of the data, where it was not obtained directly from the individual.
- The existence of automated decision-making including profiling. MLKDC does not have automated decision making.
- The safeguards that MLKDC provides if it were to transfer personal data to a third country or international organisation outside the EU. MLKDC does not export personal data outside the EU.

2.3 Time Limit – One Month (28 days)

MLKDC must act on a SAR without undue delay and at the latest within one month of receipt.

The ICO states that you should calculate the time limit from the day after you receive the request whether the day after is a working day or not until the corresponding calendar date in the next month.

ICO Example

An organisation receives a request on 3 September. The time limit will start from the next day (4 September). This gives the organisation until 4 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. This means that the exact number of days you have to comply with a request varies, depending on the month in which the request was made.

ICO Example

An organisation receives a request on 30 March. The time limit starts from the next day (31 March). As there is no equivalent date in April, the organisation has until 30 April to comply with the request.

If 30 April falls on a weekend, or is a public holiday, the organisation has until the end of the next working day to comply.

The ICO recommends that for practical purposes, if a consistent number of days is required (e.g. for operational or system purposes), it may be helpful to adopt a 28 day period to ensure compliance is always within a calendar month. MLKDC (and the NICS) has adopted this principle.

3. OTHER GDPR RIGHTS OF THE INDIVIDUAL

As well as the right to access their personal information, a SAR and the right to be informed, data subjects have additional rights under GDPR. They may make requests to MLKDC in exercise of these additional rights. Broadly, you should deal with these requests in the same way as a SAR with appropriate adjustments. Note that the one month time limit for dealing with requests also applies to them.

In all the cases listed under this section you should follow the same process for dealing with the request as set out in Section 1 above (subject to appropriate modifications).

It is important that all requests are recorded and logged including verbal requests (see Section 1.1 above).

3.1 Rectification

Individuals have a right to have inaccurate personal data rectified, or completed if it is incomplete (see 'Right to rectification' on the ICO website).

- An individual can make a request for rectification verbally or in writing.
- MLKDC has one calendar month to respond to a request.
- In certain circumstances MLKDC can refuse a request for rectification.

3.2 Erasure (A right to be forgotten)

GDPR introduces a right for individuals to have personal data erased, also known as *'the right to be forgotten'* (see 'Right to erasure' on the ICO website).

- Individuals can make a request for erasure verbally or in writing.
- MLKDC has one month to respond to a request.
- The right is not absolute and only applies in certain circumstances.
- Note also that this right is not the only way in which the GDPR places an obligation on MLKDC to consider whether to delete personal data.

3.3 Restriction of processing

Individuals have the right to request the restriction or suppression of their personal data (see 'Right to restrict processing' on the ICO website).

- This is not an absolute right and only applies in certain circumstances.
- When processing is restricted, MLKDC would be permitted to store the personal data, but not use it.
- An individual can make a request for restriction verbally or in writing.
- MLKDC has one calendar month to respond to a request.

3.4 Portability of their data

GDPR includes a right that allows individuals to obtain and reuse their personal data for their own purposes across different services (see 'Right to data portability' on the ICO website).

- It allows a data subject to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.
- Doing this enables individuals to take advantage of applications and services that can use this data to find them a better deal or help them understand their spending habits.
- The right only applies to information an individual has provided to a controller (i.e. MLKDC).
- MLKDC must act upon the request without undue delay and at the latest within one month of receipt.

Note that the right to data portability only applies when:

- MLKDC's lawful basis for processing this information is consent or for the performance of a contract; and
- MLKDC is carrying out the processing by automated means (i.e. excluding paper files).

Therefore MLKDC is very unlikely to receive such a request (e.g. the MLKDC website does not track individuals). However, it is possible that some data sets created by MLKDC staff that involve personal data may be subject to this part of the legislation (see Section 3.6 below).

3.5 Objection to Processing

GDPR includes a right that allows individuals to object to the processing of their personal data in certain circumstances (see 'Right to object' on the ICO website).

- Individuals have an absolute right to stop their data being used for direct marketing (which MLKDC does not do).
- In other cases where the right to object applies, MLKDC may be able to continue processing if it can show that it has a compelling reason for doing so.
- MLKDC must tell individuals about their right to object (this is covered in MLKDC's Privacy Notice).
- An individual can object verbally or in writing.
- MLKDC has one calendar month to respond to an objection.

3.6 Rights relating to automated decision making and profiling

The GDPR has provisions on:

- Automated individual decision-making (making a decision solely by automated means without any human involvement); and
- Profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.

MLKDC does neither of the above. If you receive a request related to automated decision making and profiling this should be referred to the DPO immediately. More information can be found at 'Rights related to automated decision making including profiling' on the ICO website.

SUBJECT ACCESS REQUEST (SAR) LOG

HPRM Container Reference	
Data Subject's Name	
Name of Requestor (if different)	
HPRM Reference for Request	
Date Received	
Target Response Date: [Date received + 28 calendar days]	

Date	Action Taken	Taken By	Related Documents	Notes

APPENDIX 2 STANDARD TEXT FOR SARS

Provided below is standardised text to help in drafting correspondence relating to SARs. These may be adapted as necessary. Normally the correspondence should be sent by the DPO, or in his absence, the CEO. Responses should be in the same format used for the original request so far as possible (e.g. MLKDC would not normally respond to a verbal request verbally but rather by providing the information requested in an email or a letter), or unless the requestor asks for the information in a particular format.

A2.1 Standard Text: Initial Acknowledgement

As noted above, ideally you should respond to a SAR in the same format as it was made. If the request was made by letter then the text below should be adapted for a letter in response. Remember to either print on headed paper or copy to a Word template that uses the MLKDC header and footer.

If the request was made by email then adapt the text in an email. If the request was made through social media or verbally (e.g. in a meeting or by telephone) then the requestor should be asked for an email address for correspondence.

A2.1.1 For SARs made by individuals themselves

a) Where you are satisfied that the individual is who they say they are (see Section 1.2 above) then use the following text.

Our Ref: [HP Records Manager Reference]

[Name and Address of Requestor]

[Date]

Dear [Name],

Your Subject Access Request under GDPR

Thank you for your request concerning your personal information held by MLKDC.

Your request was received on [date] and I am dealing with it under the terms of the relevant legislation.

Please contact me if you have any queries about this [email / letter].

b) Where you need to verify the identity of the individual (see Section 1.2 above), then use the following text. Remember, the GDPR provides that this should be done using what it describes as *'reasonable means'* (Article 64). However the ICO guidance makes clear you should only request information that is necessary to confirm who they are, the key being proportionality.

Our Ref: [HP Records Manager Reference]

[Name and Address of Requestor]

[Date]

Dear [Name],

Your Subject Access Request under GDPR

Thank you for your request concerning your personal information held by MLKDC.

Your request was received on [date] and I am dealing with it under the terms of the relevant legislation. In order to comply with data protection legislation I must verify your identity in order to confirm that you are entitled to the information that you have requested. Please would you send to me a copy or scan of two documents, one from each of the two categories listed below. Do not send original documents.

A passport, driving license, birth certificate or other formal identity document (e.g. an official pass or voter identity card).

A utility bill, bank statement or similar document addressed to you at your current address.

If you prefer, I am happy for you to bring the documents in person to MLKDC's office at the address shown below so that I may verify your identity – please call me to arrange a date.

Please contact me if you have any queries about this [email / letter].

A2.1.2 When the SAR is made on behalf of an individual

When a SAR is made on behalf of an individual you must be satisfied that:

- Both the requestor and the individual are who they say they are; and
- That the requestor is authorised to make the request on behalf of the individual. (See section 1.3 above).

If the requestor is a solicitor or similar professional and you can verify them and their address then you do not need to confirm their identity but you must still confirm that they are authorised to act for the individual. Amend the text accordingly.

Our Ref: [HP Records Manager Reference]

[Name and Address of Requestor]

[Date]

Dear [Name],

Subject Access Request Under GDPR for [Name of Individual]

Thank you for your request concerning personal information held by MLKDC.

[I confirm receipt of the authority signed by [name of individual] / Please provide an authority signed by [name of individual] to confirm that you are acting for them in making a subject access request.]

The request was received on [date] and I am dealing with it under the terms of the relevant legislation. In order to comply with data protection legislation I must verify your identity and the identity of [Name of Individual]. For each of you, please would you send to me a copy or scan of two documents, one from each of the two categories listed below. Do not send original documents.

A passport, driving license, birth certificate or other formal identity document (e.g. an official pass or voter identity card).

A utility bill, bank statement or similar document addressed to you at your current address.

If you prefer, I am happy for you to bring the documents in person to MLKDC's office at the address shown below so that I can verify them – please call me to arrange a date.

Please contact me if you have any queries about this [email / letter].

If you have not receive a valid authority, you must ask for one and this must be recorded in HPRM.

A2.1.3 Acknowledging Proof of Identity

Our Ref: [HP Records Manager Reference]

[Name and Address of Requestor]

[Date]

Dear [Name],

Subject Access Request under GDPR

Thank you for providing the following:

[List the documents/authority/etc. provided]

I am dealing with your request under the terms of the relevant legislation and will contact you shortly.

Please contact me if you have any queries about this [email / letter].

A2.2 Standard Letter: Final Response

Ideally you should respond to a SAR in the same format as it was made. If the request was made by letter then the text below should be adapted for a letter in response. Remember to either print on headed paper or copy to a Word template that uses the MLKDC header and footer.

If the request was made by email then adapt the text in an email. If the request was made through social media or verbally (e.g. in a meeting or by telephone) then the requestor should be asked for an email address for correspondence.

Responses to SARs should be made by the DPO or the CEO.

A2.2.1 When MLKDC has the information requested

Our Ref: [HP Records Manager Reference]

[Name and Address of Requestor]

[Date]

Dear [Name],

Subject Access Request under GDPR

I refer to your request for information which we received on [date]. I am writing to confirm that the Maze Long Kesh Development Corporation (MLKDC) has now completed its search for this information.

Attached is [description of information provided].

I should draw to your attention that you [or the name of the data subject if the request was from another person] have other rights in respect of your personal information held by MLKDC.

You have a right to rectification, which concerns correcting your personal data that is held by MLKDC. If you believe the data held is not accurate, you can request that it is corrected without undue delay. Similarly if data is incomplete you can ask that it is completed.

You have 'a right to be forgotten'. This allows you to request that we delete our records or some of our records in so far as they identify you. It does not apply in all circumstances.

You have a right to request restriction of processing, which means that you can ask that access to your personal information held by MLKDC is limited in certain circumstances.

If you object to MLKDC processing your personal data please let me know the grounds for your objection.

If you are unhappy with our response to your request, you have the right to complain to the Information Commissioner. The Information Commissioner can be contacted at:

The Information Commissioner's Office

Wycliffe House

Water Lane

Wilmslow

Cheshire

SK9 5AF

www.ico.gov.uk

You can find further information in MLKDC's Privacy Notice, which is available on our website. Please contact me if you have any queries, remembering to quote the reference number above in any future communications.

A2.2.2 When MLKDC does not have the information requested

If MLKDC does not hold (any part of) the information requested, the following form of words should be used:

MLKDC does not record or hold details of [information requested].