MAZE LONG KESH

Development Corporation

General Data Protection Regulation and Data Protection Policy & Procedures

Author:

Version: 1.0

Date: August 2019

HPRM Ref: FI1/18/628798[*v2*]

GENERAL DATA PROTECTION REGULATION

AND DATA PROTECTION POLICY AND PROCEDURES

1. BACKGROUND

This policy note is aimed at MLKDC staff who may either handle personal data or who may receive a 'Subject Data Request' asking for personal information held by MLKDC. It 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.

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

MLKDC will generally follow the same data protection procedures as the Department of Finance (DoF) to the extent that MLKDC's policies and procedures do not cover the situation. This document is an outline of MLKDC's policy and procedures. It is not a substitute for seeking the advice of the DPO in all cases where personal data may be involved.

All MLKDC staff are required to take on-line data protection training which is mandatory.

2. THE DATA PROTECTION OFFICER

MLKDC has appointed a Data Protection Officer (DPO). You should seek their advice on any project or other work in MLKDC that involves personal data. You can find a copy of MLKDC's Privacy Notice on the MLKDC website. The policy applies to you and your personal data as well as the public in their interactions with MLKDC.

3. PROCESSING PERSONAL DATA WITHIN MLKDC

When dealing with personal data you must comply with MLKDC's *Records & Information Management Policy & Procedures* - DF1/13/690810 and the requirements of the data protection legislation including GDPR. In whatever format (e.g. electronic, paper, recording, etc.) you must manage all personal data securely at all times, restricting access where appropriate to those with legitimate business needs.

4. PROTECTING PERSONAL DATA

You must avoid potential data security breaches by ensuring that any personal data that you deal with is adequately protected, which is now a legal requirement. Data stored within HP Records Manager (HPRM) is protected but you may need to further restrict access to some records appropriate to the circumstances.

Practically all personal data breaches have to be reported to the Information Commissioner's Office (ICO) within 72 hours. Under GDPR, failure to protect personal information can lead to substantial fines.

Most security breaches occur by mistake. Publicised mistakes by public bodies in the past have included:

- **Sending personal data by email over the internet.** Even internally there is the potential for an email to be read by those for whom it was not intended. It is better to send a reference to the data in HP Records Manager. Encryption is a protection but it is not fool proof and electronic data is easily copied multiple times.
- **Emailing personal data to the wrong recipients.** To an address group rather than individuals and sending multiple people's personal data to multiple people.
- **Sending unencrypted personal data** (eg. a database copied onto a DVD) in the ordinary post and in some cases losing it. At a minimum data must be encrypted and

sent using a signed-for courier service. It is better if you can personally and physically transport and deliver sensitive data (which must be encrypted) in person.

- **Losing unencrypted data (**eg. on laptops and USB memory sticks containing personal data). MLKDC's laptops are encrypted but it is still embarrassing and damaging to reputation when data is lost.
- **Unintended revelations** In 2015 a clinic, specialising in HIV and other sexual health services revealed to all 780 recipients the full names and email addresses of fellow clinic users who had signed up to an email service, allowing them to receive test results and book appointments by email, and to receive the clinic's newsletter. It was fined £180,000 in May 2016. Using a distribution group or a 'BCC' list for the recipients would have avoided the problem.

Misusing or failing to protect personal data can be a criminal offence. DPA 2018 brings new data protection offences into UK law, including:

- Knowingly or recklessly obtaining or disclosing personal data without the consent of the data controller.
- Procuring such disclosure, or retaining the data obtained without consent.
- Selling, or offering to sell, personal data knowingly or recklessly obtained or disclosed.
- Taking steps, knowingly or recklessly, to re-identify information that has been 'de-identified' could also result in a criminal conviction, although one of the defences that could be raised is where that action can be justified in the 'public interest'.
- Deliberately altering or concealing information which should be provided in response to a data subject access request.

Please see also MLKDC's *Security Policy and Procedures* - DF1/13/714272.

If there is a data breach involving personal or sensitive personal information, see MLKDC's *Procedures on Loss or Theft of Data or ICT Device* - DF1/13/714279. Note that any breaches must be notified to the DPO or the CEO immediately as there is only a 72 hour window for reporting them to the Information Commissioner's Office (ICO).

5. BACKGROUND

The General Data Protection Regulation (GDPR) is EU wide legislation that came into force on 25 May 2018. At the same time a new Data Protection Act (DPA 2018) came into force in the UK. The DPA 2018 supplements the reforms to data protection laws that are contained in the GDPR and it replaces the previous DPA 1998.

6. WHO DOES GDPR APPLY TO?

GDPR applies to data 'controllers' and 'processors' A controller determines the purposes and means of processing personal data. A processor is responsible for processing personal data on behalf of a controller.

The GDPR places specific legal obligations on processors. For example, they are required to maintain records of personal data and processing activities and they will have legal liability if they are responsible for a data breach. You may be required by the DPO either to maintain the entries for your projects (that involve personal data) or provide the information to enable the DPO to update the records.

However, as a data controller, MLKDC is not relieved of its obligations where a processor is involved. The GDPR places further obligations on controllers to ensure that their contracts with processors comply with the GDPR. Whenever a controller uses a processor it needs to have a

written contract (data processing agreement) in place. The legislation and the ICO impose specific requirements for contracts between data controllers and data processors.

The potential ability to view personal data counts as data processing. For example, the IT administrators or technical support for a database containing personal information will be data processors.

GDPR apples to personal data and sensitive personal data. However, it does not apply to purely personal or household activities.

7. PERSONAL DATA

Personal data means any information relating to an identified or identifiable natural person (the '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. A natural person is a real living human being (as opposed to a legal person, thus excluding companies or a deceased individual).

8. SPECIAL CATEGORIES OF PERSONAL DATA

Additional rules apply to processing 'special categories of personal data'. There are eight special categories:

1. racial or ethnic origin
2. political opinions
3. religious or philosophical beliefs
4. trade union membership
5. the processing of genetic data
6. biometric data for the purpose of uniquely identifying a natural person
7. data concerning health
8. data concerning a natural person's sex life or sexual orientation

If you are involved with special categories of personal data you must seek the advice of MLKDC's DPO. Special categories of personal data automatically count as 'high-risk' processing activity.

9. DATA PROTECTION PRINCIPLES AND ACCOUNTABILITY

Under GDPR there are six principles relating to the processing of personal data. Personal data has to be:

1. **Processed lawfully, fairly and transparently** (see Section 10 below).
2. **Collected for specified, explicit and legitimate purposes**, and
    - Not further processed in any manner incompatible with those purposes;
    - The purposes should be specified in MLKDC's privacy notice.
3. **Adequate, relevant and limited** ('data minimisation').
4. **Accurate and where necessary, kept up to date.**
5. Kept in a form which **permits identification of data subjects for no longer than is necessary**.
6. Processed in a manner that **ensures appropriate security of the personal data**.

There are two other 'principles' that you need to be aware of in other parts of the legislation. These are 'Data Subject Rights' and 'Data Transfers' (see Section 11 below).

In addition MLLKDC, as data controller, is responsible for and must be able to demonstrate compliance with the data protection principles. This means that MLKDC has to keep records of data and data processing and it may be subject to audits by the ICO at any time. (Prior to GDPR this might have happened only where there was a data breach).

10. LAWFUL PROCESSING

For processing to be lawful under the GDPR, there has to be a legal basis. There are six legal bases:

1. **Consent** of the data subject.
2. Processing is **necessary for the performance of a contract** (involving the data subject).
3. **Compliance with a legal obligation**.
4. To **protect the vital interests** of the data subject or of another natural person.
5. **Public Task** for the performance of a task carried out in the public interest.
6. For **legitimate interests**.

In the majority of cases, 'Public Task' will be the legal basis used by MLKDC (and other public authorities).

11. THE RIGHTS OF THE INDIVIDUAL

The GDPR provides eight rights for individuals (the 'data subject').

1. The right to be informed;
2. The right of access;
3. The right to rectification;
4. The right to erasure;
5. The right to restrict processing;
6. The right to data portability;
7. The right to object;
8. Rights in relation to automated decision making and profiling.

12. SUBJECT ACCESS REQUESTS

A data subject can make a 'subject access request' (SAR) to access their personal data. There is no specified form for a SAR and a request could be made to anyone in MLKDC. If you think you have received a SAR you must immediately inform the DPO or the CEO.

- Individuals can make a subject access request verbally or in writing.
- **MLKDC has one month to respond to a request.**
- MLKDC cannot charge a fee to deal with a request in most circumstances.

In response to a SAR, MLKDC has to tell the data subject whether or not any their personal data is being processed. If it is being processed, they are entitled to:

- A description of the personal data, the purposes for which it is being processed, recipients, retention period and rights of rectification, erasure, restriction and objections.
- Know the existence of any automated decision making (which MLKDC does not do).
- Any transfer safeguards that exist.

- A copy of the information comprising the data and details of the source of the data. (Data can include opinions, voice recordings and manual records).

13. DATA PROTECTION BY DESIGN AND BY DEFAULT

Under the GDPR, a controller has a general obligation to implement technical and organisational measures to show that it has considered and integrated data protection into its processing activities.

The ICO has published guidance on privacy by design.

- The GDPR requires you to put in place appropriate technical and organisational measures to implement the data protection principles and safeguard individual rights. This is 'data protection by design and by default'.
- This means you have to integrate data protection into your processing activities and business practices, from the design stage right through the lifecycle.
- This concept is not new. Previously known as 'privacy by design', it has always been part of data protection law. The key change with the GDPR is that it is now **a legal requirement**.
- Data protection by design is about considering data protection and privacy issues upfront in everything you do. It can help you ensure that you comply with the GDPR's fundamental principles and requirements, and forms part of the focus on accountability.

You should begin data protection by design at the initial phase of any system, service, product, or process. This means it should be a fundamental part of the Project Initiation Document (PID) at the beginning of any project that involves personal data.

Where any project involves, or is likely to involve, personal data you should engage with the DPO at the earliest possible stage.

14. DATA PROTECTION IMPACT ASSESSMENTS

A Data Protection Impact Assessment (DPIA) is undertaken to identify potential areas of non-compliance and minimise the risk. You must carry out a DPIA before beginning any new 'high-risk' processing activity (e.g. processing sensitive data or profiling activities). The ICO also requires you to do a DPIA in a number of specified circumstances. **Effectively this makes them mandatory. At the very least you must record why you considered that a DPIA was not required** and this record needs to be included in MLKDC's records as a data controller.

DPIAs should include the following as a minimum:

- A description of the processing activity and the purpose;
- An outline of the risks and the measures taken in response;
- The formal advice of the DPO.

DPIA templates are available.