.

 **Data Protection Impact Assessment Policy and Procedure**

**Version history**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Version** | **Date** | **Amended By** | **Summary of Change** | **File Location** | **Approved by/ Date** |
| 0.1  | 26/10/2020 | ISM | Initial document prior to approval   |  Network |  MD |
| 1.0 | 26/11/2020 | ISM  | After approval |  Intranet |   MD |
| 1.1 | 06/12/2021 | ISM | Reviewed with no changes | Intranet | MD |
| 1.2 | 07/12/2022 | IAM | Reviewed with no changes | Intranet | MD |
| 2.0 | 22/01/2024 | IAM | Changed the penalty cost to Sterling Pounds.  | Intranet | MD |
| 2.1 | 4/12/2024 | ISM | Reviewed with no changes | Intranet | MD |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Table of Contents

[Purpose of the document 3](#_Toc187144192)

[Scope 3](#_Toc187144193)

[Data protection by design and default 4](#_Toc187144194)

[Key roles and Responsibilities 4](#_Toc187144195)

[Senior Information Risk Owner (SIRO 4](#_Toc187144196)

[Data Protection Officer (DPO) 4](#_Toc187144197)

[Information Asset Owners (IAO) 5](#_Toc187144198)

[Project Sponsors 5](#_Toc187144199)

[Project Managers 5](#_Toc187144200)

[Specialist Advice 5](#_Toc187144201)

[Staff Responsibilities 5](#_Toc187144202)

[Identifying the need for a DPIA 6](#_Toc187144203)

[Undertaking a DPIA 6](#_Toc187144204)

[Consultation with the ICO 6](#_Toc187144205)

[Review of DPIAs 7](#_Toc187144206)

[Policy review 7](#_Toc187144207)

# Purpose of the document

Data Protection Act 2018 introduced a new obligation upon organisations to conduct a Data Protection Impact Assessment (DPIA) before carrying out types of processing likely to result in high risk to individuals’ interests. GDPR require Microlink as a data controller to consider and apply appropriate measures designed to implement their key principles effectively.

Projects that involve personal or sensitive (special category) information (including pseudonymised data) or new technologies to process personal data give rise to privacy issues and concerns. Necessary safeguards must be incorporated into all activities involving the processing of personal data in order to ensure that the rights and freedoms of individuals are protected. This is known as “Data Protection by Design”.

 DPIA therefore serves as a tool to help Microlink to identify, evaluate and mitigate risks to individuals arising as a result of the processing of their personal data. At the same time, a DPIA should ensure compliance with data protection law and other legal and regulatory requirements (for example, the Equality Act 2010). To enable organisations to address any privacy concerns and risks, Data Protection Impact Assessment (DPIA) endorsed by the Information Commissioner’s Office (ICO) must be used.

failure to undertake a DPIA when required under the GDPR may result in a fine of up to £8.7 million or 2% of total global annual turnover, whichever is higher.

# Scope

MicrolinkPC ensures that part of the solution to reduce the risk is to ensure that DPIA process is advocated for the relevant projects.

This Policy is therefore applicable to any member of staff who is responsible for project, managing a new ‘project’ or ‘plans’ to modify or procure any system (information asset).

This Policy outlines Microlink’s approach and methodology for conducting DPIAs for new and existing systems and processes.

This policy and procedure should be read in connection with the policies and procedures listed in Table 1.

Table 1 Related Policies and Procedures

|  |  |
| --- | --- |
| Title  | Version  |
| Microlink Security Policy  | 1.6 |
| Microlink Security Procedures  | 2.4 |
| Microlink HR Policy and Procedures  | 2022 |
| Microlink Business Continuity and Disaster Recovery Plans  | 3.0 |
| Microlink Data subject Access request procedures  | 5.1 |
| Microlink Privacy policy and procedures for clients  | 5.0 |
| Microlink Data Protection Policy and Procedures  | 4.2 |
| ISMS IT operations manual  | 17.1 |
| Microlink Risk Management policy | 1.0 |

# Data protection by design and default

According to ICO, “GDPR requires you to put in place appropriate technical and organisational measures to implement the data protection principles effectively and safeguard individual rights. This is ‘data protection by design and by default’. With the change with GDPR, this is 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.

We at Microlink always ensures that appropriate technical and organisational measures to implement the data protection principles and safeguard individual rights are in place.

If a DPIA identifies a high risk that is unable to be mitigated, MicrolinkPC should consult the ICO before the Project can go ahead.

As a minimum, a DPIA will include:

• Data Flow Mapping

• An assessment of:

(i) the need for and proportionality of the processing

(ii) the risks to data subjects (as viewed from the perspective of data subjects)

• A list of the measures envisaged to mitigate those risks and ensure compliance with the GDPR.

 Examples of projects (not limited to) that would require a DPIA:

• A new IT system for storing and accessing Personal Confidential Data (PCD).

• Using existing PCD for a new, unexpected or more intrusive purpose.

• A new database which consolidates information held by separate parts of an organisation.

• cloud-based systems.

• AI systems

• Use of data that appears to be pseudonymised or anonymised but could be identifiable if

 combined with other information. Pseudonymisation is the process of distinguishing individuals in

 a dataset by using a unique identifier which does not reveal their ‘real world’ identity’, and

 anonymisation is the process of rendering data into a form which does not identify individuals and

 where identification is not likely to take place.

# Key roles and Responsibilities

 Senior Information Risk Owner (SIRO)

The SIRO is responsible for ensuring Information Risk is developed, implemented, reviewed and its effect monitored. DPIA is one element of the management of information risk. Information risks need to be handled in a similar manner to other major risks such as financial, legal and reputational risks.

The SIRO is the key role for identifying and managing risk.

• Take ownership of the Microlink’s information risks.

• Acts as the advocate for information risk on the Governing Body.

## Data Protection Officer (DPO)

The DPO is responsible for Data Protection compliance within Microlink and ‘approves’ all full scale DPIAs for recommendation of endorsement to the SIRO. The DPO can **provide advice** on:

• whether a DPIA is required

• how the DPIA should be conducted

• what measures and safeguards can be taken to mitigate risks

• whether the DPIA has been carried out correctly; and

• the outcome of the DPIA and whether the processing can go ahead.

The DPO’s advice to Project Managers is recorded on the final version of the full scale DPIA. **If you do not follow the DPO’s advice, you should record your reasons for not doing so** ensuring that you are able to justify your decision and inform the DPO. This information should be recorded using the **Risk Acceptance form (RA form).** The RA form should be duly completed and approved by the CISO before returning the form to the DPO.

The DPO also monitors updates from the project managers regarding the ongoing performance of the DPIA, including how well the planned actions have been implemented to address the risks.

## Information Asset Owners (IAO)

Information Asset Owners are able to understand and address risks to the information assets they ‘own’ and to provide assurance to the SIRO on the security, confidentiality and integrity and use of the assets. Any Risks identified by the IAO should be added to their Team risk register.

Information Asset Owners are responsible for ensuring that DPIAs for the assets they own are maintained throughout the lifetime of a project and for liaising with the Head of IT to ensure that their information systems are recorded on the Microlink’s Information Asset Register.

## Project Sponsors

The Project Sponsor is the individual (often a senior manager or executive) with overall accountability for the project. The Project Sponsor is primarily concerned with ensuring that the project delivers the agreed business benefits.

## Project Managers

Project Managers must ensure that:

• any project that involves processing of personal data is assessed to identify if a DPIA is required

• DPIAs are revisited regularly throughout the lifetime of the project to identify any changes made to

 the proposed use of information i.e. data flow

• the DPO is consulted, in a timely manner, in all issues relating to the protection of personal data

• where Microlink has completed a DPIA on behalf of the provider of a service it has

 commissioned, the ‘signed off’ DPIA is shared with the provider to enable them to put it through

 their own formal governance process

• the DPO is informed of Projects that have been ‘abandoned’ or put ‘on hold’.

## Specialist Advice

Specialist advice can be provided by individuals of Microlink i.e. Head of IT, SIRO and DPO depending on the issues identified as an outcome of completing a full-scale DPIA. The Information Governance Function is available to provide the expert knowledge and guidance around the legal framework.

## Staff Responsibilities

All staff employed by the Microlink must follow the requirements of this Policy and associated policies, particularly those relating to Information Governance and Data Security. Where breaches of confidentiality, security alerts etc are identified relating to an information system, a DPIA must be undertaken to provide assurance that information risk is being managed.

In practice, it is the responsibility of the staff member or team leading an Initiative to undertake the screening questions and produce the first draft of a DPIA if necessary, i.e. the project manager, system owner, etc. This can then be further worked up in collaboration with the Data Protection Officer and CISO, and other relevant stakeholders.

Draft DPIAs should be sent to the DPO at dpo@microlinkpc.com

# Identifying the need for a DPIA

1. A DPIA must be undertaken *before* the processing of any personal data which is “*likely to result in*

 *a high risk to the rights and freedoms*” of individuals. As such, it is necessary to identify whether

 there are any factors that warrant the need for a DPIA to be undertaken.

2. In the case of any Initiatives involving the processing of personal data that were commenced

 before 25th May 2018 (when the GDPR came into force) and which are ongoing, such Initiatives

 should be reviewed and the need to undertake a DPIA considered.

3. DPIA to be undertaken where any Initiative will involve the processing of special categories of

 personal data on a large scale.

4. Where any new Initiative will involve the processing of personal data, the DPIA Screening

 Questionnaire should be completed.

5. Before completing the questionnaire, it is important to:

a. identify the key stakeholders in the Initiative so that they can provide their input into the questionnaire; and

b. have a clear understanding of the scope and objectives of the Initiative so that the questionnaire can be completed as fully and accurately as possible.

6. If there is any uncertainty regarding completion of the questionnaire or the outcome, the Data

 Protection Officer should be consulted.

7. Where the outcome of the questionnaire suggests that the processing is unlikely to result in a high

 risk to individuals, there may be circumstances where it is advisable to undertake a DPIA anyway

 due to:

a. the nature, scope, context and purposes of processing personal data

b. the level of investment in the Initiative in terms of time, financial and other resources; or

c. the visibility of the Initiative internally and externally.

8. Where it has been concluded that a DPIA is unnecessary and will not be undertaken, the reasons

 for this should be clearly documented. The Screening Questionnaire should be retained to

 evidence the decision made and may need to be revisited and reviewed at a later date.

# Undertaking a DPIA

If you decide that a DPIA is necessary or desirable for a particular Initiative, the Risk Assessment for DPIA Template should be completed. The template can be obtained by contacting the DPO. The DPIA Template explains the objectives and requirements of each section. Where any section is not completed because it is not applicable or not considered necessary, this should be explained.

# Consultation with the ICO

1. If we have carried out a full scale DPIA that identifies a high risk, and we are unable to implement

 measures to reduce this risk then, GDPR requires that the processing cannot commence before

 the Information Commissioner’s Office (ICO) has been consulted.

2. The ICO should be consulted via the Data Protection Officer, who will usually initiate contact with

 the ICO. Consultation with the ICO should only be necessary in very exceptional instances as it is

 expected that Microlink will be able to apply measures to appropriately mitigate or eliminate risk

 on most occasions.

3. The Data Protection Officer will contact the ICO, sending a copy of the DPIA together with a cover

 letter to dpiaconsultation@ico.org.uk. The ICO intends to respond to requests for consultation

 within eight weeks, though it can extend such period by a further six weeks in complex cases.

4. The ICO will provide a written response confirming whether the risks identified are acceptable or

 whether further action is required. In some cases, the ICO may recommend that the processing is

 not undertaken.

# Review of DPIAs

1. A DPIA should be undertaken at the earliest opportunity in the development of an Initiative and

 re-assessed prior to commencement of the relevant processing activities to identify whether any

 changes to the Initiative impact upon the outcomes of the DPIA and whether the controls and

 measures identified in the DPIA have been integrated into the Initiative.

2. Once the processing of personal data has commenced in respect of an Initiative, the DPIA should

 be reviewed regularly having regard to the nature and risks associated with the processing, taking

 into account any changes to the processing activities or scope of the Initiative. A review should be

 undertaken at least annually by the staff member or team leading or owning the Initiative.

# Policy review

This Policy will be reviewed as required and at least once a year by DPO.