Microlink

Data Protection Policy and Procedures

Version history

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Version** | **Date** | **Amended By** | **Summary of Change** | **File Location** | **Approved by/ Date** |
| 0.1 | 20/4/2018 | ISM | Initial document prior to approval | Network |  |
| 1.0 | 01/05/2018 | ISM | After approval | Network | MD |
| 2.0 | 01/05/2019 | ISM | Section 3.3 updated. Added a new point at the end of the section.  Section 3.7 new bullet point added at the end of the section | Network | MD |
| 2.1 | 26/11/2020 | ISM | Reviewed with no changes. Document format updated | Intranet | MD |
| 3.0 | 06/12/2021 | ISM | Added seventh principle, added Data retention policy and right to erasure policy to table 1 | Intranet | MD |
| 4.0 | 07/12/2022 | ISM | 3.6.4 updated | Intranet | MD |
| 4.1 | 23/01/2024 | ISM | Reviewed with no changes | Intranet | MD |
| 4.2 | 02/12/2024 | ISM | Reviewed with no changes | Intranet | MD |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Contents

[1 Introduction 4](#_Toc187144292)

[2 Data Protection Policy 5](#_Toc187144293)

[2.1 Policy scope 6](#_Toc187144294)

[2.2 Data protection risks 6](#_Toc187144295)

[2.3 Responsibilities 7](#_Toc187144296)

[2.4 Definitions 8](#_Toc187144297)

[2.4.1 Business purposes 8](#_Toc187144298)

[2.4.2 Personal data 8](#_Toc187144299)

[2.4.3 Special Categories of Personal Data 8](#_Toc187144300)

[2.4.4 Processing 9](#_Toc187144301)

[2.4.5 filing systems 9](#_Toc187144302)

[2.4.6 Controller 9](#_Toc187144303)

[2.4.7 Processor 9](#_Toc187144304)

[2.4.8 Third party 9](#_Toc187144305)

[2.4.9 Consent 9](#_Toc187144306)

[2.4.10 Personal data breach 9](#_Toc187144307)

[2.4.11 Supervisory Authority 9](#_Toc187144308)

[2.5 Monitoring and Review 10](#_Toc187144309)

[2.6 Retention 10](#_Toc187144310)

[3 Data Protection Procedures 10](#_Toc187144311)

[3.1 Special Category Data 10](#_Toc187144312)

[3.2 Security of Data 11](#_Toc187144313)

[3.3 Processing of Personal Data 11](#_Toc187144314)

[3.4 Data Subject (clients and staff) Rights 12](#_Toc187144315)

[3.5 Data Request: Access to their data. 13](#_Toc187144316)

[3.6 Collecting Data 13](#_Toc187144317)

[3.6.1 Consent 13](#_Toc187144318)

[3.6.2 Privacy Notice 14](#_Toc187144319)

[3.6.3 Storage of personal data 14](#_Toc187144320)

[3.6.4 Data Subject request for Rectification 14](#_Toc187144321)

[3.6.5 Data Subject withdraws consent. 14](#_Toc187144322)

[3.6.6 Data Subject’s request for erasure 15](#_Toc187144323)

[3.6.7 Data Subject’s request to restrict processing 15](#_Toc187144324)

[3.6.8 Data Subject’s request to object 15](#_Toc187144325)

[3.7 Disclosing Personal Data to Suppliers. 16](#_Toc187144326)

[3.8 Using third party controllers and processors 16](#_Toc187144327)

[3.8.1 Contracts 16](#_Toc187144328)

[3.9 Conducting a Data Protection Impact Assessment 17](#_Toc187144329)

[3.10 Suspect loss or exposure of data 17](#_Toc187144330)

[3.11 Criminal offence data 18](#_Toc187144331)

[3.11.1 Criminal record checks 18](#_Toc187144332)

[3.12 Audits, monitoring and training 18](#_Toc187144333)

[3.12.1 Data audits 18](#_Toc187144334)

[3.12.2 Monitoring 18](#_Toc187144335)

[3.13 Reporting breaches 18](#_Toc187144336)

[3.13.1 Failure to comply 18](#_Toc187144337)

# Introduction

This Data Protection Policy document is part of a set of policy documents that together represent the policy of the Microlink organisational approach to security. Therefore, this set of policies and procedures 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 breach and Information Security Incidence Reporting procedures | 3.2 |
| ISMS IT operations manual | 17.1 |
| Document retention and records management policy | 7.0 |
| Right to erasure policy | 1.4 |
| Microlink Risk Management policy | 1.0 |

The Board of Microlink recognises the fundamental importance of data protection. The Board, and staff are working together to ensure that, everyone at Microlink complies with the requirements of the relevant data protection legislation. This Policy Statement sets out the framework within which the organisation will operate in data protection matters.

In accordance with the core values of the organisation our policy for data protection will observe the principles of ethics, legality, prudence, equality, safety, timeliness, fairness, transparency and simplicity.

Microlink needs to gather and use certain information about individuals.

These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company’s data protection standards — and to comply with the law.

As our data protection officer (DPO), Dr Dayani Jayasinghe has overall responsibility for the day-to-day implementation of this policy. You should contact the DPO for further information about this policy if necessary.

email: dpo@microlinkpc.com phone: direct 023 8024 0342\*2046

Internal: 2046

The data protection officer is responsible for liaison and registering with the Information Commissioner’s office.

# Data Protection Policy

This data protection policy ensures that Microlink

* Complies with data protection law and follows good practice.
* Protects the rights of staff, customers and partners.
* Is open about how it stores and processes individuals’ data.
* Protects itself from the risks of a data breach.

To ensure that our responsibilities under Data Protection Act 2018 and UK data protection legislation are carried out in a manner which is compatible with our principles, our policy is to:

I. Comply with the seven principles set out in the Data Protection Act and UK General Data Protection Regulation.

These require that data is:

* fairly and lawfully processed.
* processed for limited purposes (purpose limitation)
* adequate, relevant and not excessive (data minimisation)
* accurate
* not kept longer than necessary (storage limitations)
* processed in accordance with individuals’ rights (integrity and

confidentiality)

* Accountability

II. In addition, there is still a requirement to (not a principle)

* keep the data secure.
* Restrictions on transferring data to countries outside the UK

1. Make directors, managers and staff aware of the types of personal data the organisation holds and processes and the reasons for which it is processed.
2. Ensure that all staff are aware of their responsibilities under the UK GDPR.
3. Ensure that the organisation’s data systems, both electronic and paper-based, are adequately controlled, secure and comply with the current data protection legislation, through a rolling programme of audits.
4. Ensure that staff are aware of their obligations under the UK GDPR.
5. Ensure that there is a procedure to allow staff and other data subjects to access personal data held about themselves where that access does not infringe the confidentiality owed to others.
6. Obtain the data subject’s consent where required to process and hold personal data.
7. Address the concerns of individuals when it is necessary to process sensitive information about an individual.
8. Retain all information only for as long as specified in the record retention schedule.
9. Ensure that where suppliers need to have Personal data of our staff and clients, they also have the appropriate policies and procedures for handling personal data under the UK GDPR.
10. Where personal data is in use for new systems and projects, a data protection impact assessment must be carried out.

The responsibilities of the organisation and its staff are detailed in the Microlink Data Protection Procedures.

## Policy scope

This policy applies to:

* The head office of Microlink
* All staff of Microlink
* All contractors, suppliers and other people working on behalf of Microlink

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 2018. This can include:

* Names of individuals
* Postal addresses
* Email addresses
* Telephone numbers
* any other information relating to individuals

## Data protection risks

This policy helps to protect Microlink from some very real data security risks, including:

* **Breaches of confidentiality.** For instance, information being given out inappropriately.
* **Failing to offer choice.** For instance, all individuals should be free to choose how the company uses data relating to them.
* **Reputational damage.** For instance, the company could suffer if hackers successfully gained access to sensitive data.

## Responsibilities

Everyone who works for or with Microlink has responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

* The **board of directors** is ultimately responsible for ensuring that Microlink meets its legal obligations.
* The **Data Protection Officer** is responsible for:
  + Keeping the board updated about data protection responsibilities, risks and issues.
  + Reviewing all data protection procedures and related policies, in line with an agreed schedule.
  + Arranging data protection training and advice for the people covered by this policy.
  + Handling data protection questions from staff and anyone else covered by this policy.
  + Dealing with requests from individuals to see the data Microlink holds about them (also called ‘subject access requests’).
* The **IT manager,** is responsible for:
  + Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
* Performing regular checks and scans to ensure security hardware and software is functioning properly.
* Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.
* The **Marketing Manager,** is responsible for:
* Approving any data protection statements attached to communications such as emails and letters.
* Addressing any data protection queries from journalists or media outlets like newspapers.
* Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

## Definitions

### Business purposes

The purposes for which personal data may be used by us:

* Personnel, administrative, financial, regulatory, payroll and business development purposes.
* Providing workplace adjustment services to the customers.

Business purposes include the following:

* Compliance with our legal, regulatory and corporate governance obligations and good practice
* Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests
* Ensuring business policies are adhered to (such as policies covering email and internet use)
* Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting, credit scoring and checking
* Investigating complaints
* Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments
* Monitoring staff conduct, disciplinary matters
* Providing workplace adjustment services to the customers.
* Improving services

### 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.

### Special Categories of Personal Data

Special categories of data include information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings, and genetic and biometric information —any use of special categories of personal data should be strictly controlled in accordance with this policy.

### Processing

processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

### filing systems

‘Filing system’ means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

### Controller

‘controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined the controller.

### Processor

processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

### Third party

third party’ means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

### Consent

‘consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

### Personal data breach

‘Personal data breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

### Supervisory Authority

This is the national body responsible for data protection. The supervisory authority for our organisation is the Information Commissioners Office (ICO).

## Monitoring and Review

This Policy will be reviewed every year: including a review of the progress in implementing the Policy and include any recommendations for revision of the Policy where appropriate.

## Retention

The default policy for data records to be kept are:

* Accounting information will be kept for 6 years
* Employment history 6 years after the person has left the company. (Refer to Data Retention Policy)

If data retention policy is required outside of this period, the board should be informed and this policy will be updated.

Additional Retention periods can be found here

[Document Retention and Records Management Policy v 7.0.docx](https://microlinkpc.sharepoint.com/:w:/r/Compliance%20&%20Governance/_layouts/15/Doc.aspx?sourcedoc=%7BA00BA564-156F-4A42-AD66-1396432101AD%7D&file=Document%20Retention%20and%20Records%20Management%20Policy%20v%207.0.docx&action=default&mobileredirect=true)

# Data Protection Procedures

Please note that Microlink as a body is the data controller, and that the Board of Directors are ultimately responsible for the implementation. The Data Protection Officer is responsible for day-to-day matters. All staff have a responsibility to adhere to the seven principles of data protection, as indicated in the Data Protection Policy. These Guidelines have been drawn up to assist staff in their interpretation of the Data Protection Policy. Any queries or uncertainties should be referred to the Data Protection Officer.

**Please note that ‘data’ refers to information held about individuals in paper-based and electronic formats.**

All staff have a duty to ensure that they comply with the data protection principles which are set out in the Data Protection Policy. Staff must ensure that records are:

* accurate
* up to date
* fair
* kept and disposed of safely, and in accordance with organisation policy

## Special Category Data

Staff may process data about **customers** on a regular basis, day-to day business, when writing reports or auditing, or as part of a supervisory role. For staff, Microlink will ensure via UK GDPR induction training that all staff understand this, and are notified of the categories of processing, as required by the UK GDPR. The information that staff deal with on a day-to-day basis will be 'standard' and will cover categories such as:

* General personal details such as names and addresses.
* Report and notes of the medical condition of the customers.

Information relating to Staff’s Special Category Data (physical or mental health, sexual life, political or religious views, trade union Staff’s or ethnicity or race) is sensitive and can only be collected and processed with the staff’s consent. When such data collection occurs, it should only be done using standard forms which have been authorised by the Data Protection Officer.

Staff are not allowed to hold or process sensitive data of the customer unless explicit consent is obtained by the customer. The only exception to this will be if a member of staff is satisfied that the processing of data is necessary:

* In the best interests of the customer or staff member, or a third person, or Microlink; and
* He or she has either informed the authorised person of this or has been unable to do so and processing is urgent or necessary in all the circumstances (e.g. medical emergency).

## Security of Data

Staff are responsible for ensuring that all data they maintain is kept securely. Remember that this refers both to paper-based and electronic formats.

Staff must not disclose personal data about **customers** to anyone, including other members of staff, unless for normal business operational purposes, authorised from the Data Protection Officer or in line with Microlink policy.

Staff shall not disclose personal data to any other member of staff, unless for normal administrative purposes or in line with Microlink policy.

## Processing of Personal Data

Before processing any personal data **about customers**, all staff should consider the following checklist:

* Have we obtained and recorded explicit consent to process the data? (see the procedure for obtaining the data)
* Are there any restrictions on processing a particular person’s personal data (check to see if any data is flagged “not for processing”)?
* Do you really need to record the information? We should have a legitimate interest. Collecting data for the purpose of direct marketing (including profiling) or non-disclosed purposed is prohibited without explicit consent from the data subject.
* Has the Data Subject been told that this type of data will be processed?
* Is the information listed as a Special Category (sensitive)? If so, check again that you have the data subject’s explicit consent?
* Are you authorised to collect/store/process the data?
  + If yes, have you checked that the data is accurate?
  + Are you sure that the data is secure?
* If you do not have the data subject’s consent to process, are you satisfied that it is in the best interests of the staff member to collect and retain the data?
* Is processing necessary to fulfil or prepare a contract for the individual?
* Do we have a legal obligation to process the data (excluding a contract)?
* Is processing the data is necessary to protect person’s life or in a medical condition (vital interest)?
* Is processing necessary to carry out a public function, a task of public interest or the function has a clear basis for law?
* Is processing necessary to carry out our legitimate interests? This condition does not apply if there is a good reason to protect the individual’s personal data which overrides the legitimate interest.
* Have you reported the fact of the data collection to the Data Protection Officer?
* No processing of data should result in an automated decision or profiling being made. In order to provide safeguards for individuals against the risk that a potentially damaging decision is automatically taken, all decisions will be confirmed by human intervention.
* **All reports leaving the organisation (email attachments) containing personal information (assessment reports, notes etc,) should be password protected. The password should be sent to the recipient using a different communication method (e.g. text message, phone call etc).**

## Data Subject (clients and staff) Rights

1. the right to access;
2. the right to rectification;
3. the right to erasure;
4. the right to restrict processing;
5. the right to object to processing;
6. the right to data portability.
7. the right to withdraw consent.
8. Right to object to automated processing (making a decision without human involvement e.g. refusal of online credit application)
9. the right to complain to a supervisory authority

## Data Request: Access to their data.

Under the terms of the UK GDPR, **staff, customers and other users** of Microlink systems have the right of access to personal data relating to themselves that is held by Microlink in paper based or electronic format which is part of a ‘relevant filing system’.

The organisation has a duty of care to maintain the confidentiality of the personal records it holds, and an obligation to release this information only to the persons to whom it relates (or a third party in exceptional circumstances).

If individuals formally wish to access their personal information, they should complete a Data Access Request from the Data protection officer.

When a data subject requests information or action under the UK GDPR, the request details are to be logged and given to the Data Protection Officer. The DPO will collect any additional information required to complete the request, then assess the request, approve its validity taking into account the risk to any other data subjects involved, and task the relevant departments to complete the request, they will monitor and manage this process through to its completion. Microlink should complete the data request within 30 days of receiving the request with the valid proof ID documents.

These procedures relate to the collection, processing, storage and access to personal data. Requests for more general information, or for personal data relating to third parties, should be dealt with under the Freedom of Information Guidelines, available at: <https://ico.org.uk/for-organisations/guide-to-freedom-of-information/>

**Data portability**: Where the Data subject has asked for an electronic version of the data in a portal format this is to be given as a commonly machine-readable format such as a comma separated value (.CSV) file.

## Collecting Data

It is important that all data subject **(customers and staff)** know why we are collecting personal data and how we are processing the personal data. Our procedures do not infringe the rights of the data subjects as specified in the UK GDPR.

### Consent

It is important that when collecting personal data, the data subject **(customer)** gives explicit consent; for collecting, storing and processing the personal data (see the section on Privacy Notice).

A record is to be kept of:

* The consent (how it was given)
* The date consent was given
* Referee to the privacy notice at the time of consent

### Privacy Notice

All forms of data collection (electronic and paper) must explicitly tell the data subject in the privacy notice:

* Why we are collecting the data (justification)
* How we will process that data
* That they have a right to object “at the point of first communication” and in your privacy notice.
* How they can object

The data privacy notice shall be explicit, easily identifiable and separate from any other notices to ensure it is brought to the attention of the data subject.

### Storage of personal data

All personal data should be identified as data we control (but processed elsewhere) or data we both control and process. For example, Payroll we may control and process elsewhere. Whereas Door access records we will both control and process.

### Data Subject request for Rectification

When a data subject **(customer)** requests rectification or information under the UK GDPR, the request to be actioned first by the relevant member of staff. The staff member should follow the procedure provided by Corporate and DSA departments. All rectifications except name changes should be provided via email by the data subject. Any changes to the names should have proof of name change document. These procedure guidelines can be found on Microlink Intranet. If there is a problem with rectifying the data, then the request must be logged and passed onto the Data Protection Officer. Once the action has been completed the date and the nature of the corrective action are logged.

### Data Subject withdraws consent.

When a data subject **(customer)** withdraws consent under the UK GDPR, the request is logged by the client using the form provided and passed onto the Data Protection Officer.

The DPO must assess the request and review where removal of consent must result in cessation of processing. For example, some processing cannot be stopped due to legal reasons. Once approval for cessation of processing is granted all data relating about the data subject, is to be removed from processing. As per the relevant process documents for each system in question.

Once the action has been completed the date and the nature of the corrective action are logged.

### Data Subject’s request for erasure

When a data subject **(customer)** requests to be erasure of personal data under the UK GDPR, the request is logged (form) and passed onto the Data Protection Officer.

The DPO will then assess the request and see if it can be legally acted upon. If there is another legal ground for processing other than consent and continued processing poses no risk to the rights and freedoms of the data subject, then the data subject will be informed where and how processing will continue. E.g. an ongoing criminal case, legal obligation to process etc.

Once the right to erasure has been confirmed then all applicable data relating about the data subject, is to be removed from processing.

All data necessary to maintain the erasure recorded is to be moved to a non-processing part of the data storage area.

Once the action has been completed the date and the nature of the corrective action is logged and the data subject informed that their details have been removed.

### Data Subject’s request to restrict processing

When a data subject **(customer**) request to restrict processing under the UK GDPR, the requested is logged and passed onto the Data Protection Officer.

The DPO will then assess the request and see if it can be legally acted upon. If there is another legal ground for processing other than consent and continued processing poses no risk to the rights and freedoms of the data subject, then the data subject will be informed where and how processing will continue. E.g. an ongoing criminal case, legal obligation to process etc.

Once the right to restrict has been confirmed then all applicable data relating about the data subject, is to be restricted from processing.

The records for this data subject are to be marked “not for processing” and moved to a not for processing area of the data storage area

The size of the record is sufficient just to contain enough information about the data subject to ensure that the restriction is respected in future.

Once the action has been completed the date and the nature of the corrective action are logged and the data subject informed of the outcome and its effects.

### Data Subject’s request to object

When a data subject objects to the processing of their data under the UK GDPR, the requested is logged and passed onto the data Protections Officer.

Once the action has been completed the date and the nature of the corrective action are logged.

Note the data subject cannot object if we are processing data for

* processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
* processing for purposes of scientific/historical research and statistics.

## Disclosing Personal Data to Suppliers.

During the course of business, it may be necessary for Microlink to share personal data of the customers and the staff of Microlink with suppliers and 3rd party contractors for example assessors, workplace Adjustment team, Payroll etc,., in such cases:

* Contractual agreements should be provided to the suppliers. A Data Protection Impact Assessment be undertaken
* The supplier must maintain technical and organisational measures as described in the UK GDPR to protect personal data.
* **All reports leaving the organisation (email attachments) containing personal information (assessment reports, MI reports etc,) should be password protected. The password should be sent to the recipient using a different communication method (e.g. text message, phone call etc).**

## Using third party controllers and processors

As a data controller or data processor, we must have written contracts in place with any third-party data controllers or data processors that we use. The contract must contain specific clauses which set out our and their liabilities, obligations and responsibilities.

**As a data controller**, we must only appoint processors who can provide sufficient guarantees under UK GDPR and that the rights of data subjects will be respected and protected.

**As a data processor**, we must only act on the documented instructions of a controller. We acknowledge our responsibilities as a data processor under UK GDPR and we will protect and respect the rights of data subjects.

### Contracts

Our contracts must comply with the standards set out by the ICO and, where possible, follow the standard contractual clauses which are available. Our contracts with data controllers (and/or) data processors must set out the subject matter and duration of the processing, the nature and stated purpose of the processing activities, the types of personal data and categories of data subject, and the obligations and rights of the controller.

At a minimum, our contracts must include terms that specify:

* Acting only on written instructions
* Those involved in processing the data are subject to a duty of confidence
* Appropriate measures will be taken to ensure the security of the processing
* Sub-processors will only be engaged with the prior consent of the controller and under a written contract
* The controller will assist the processor in dealing with subject access requests and allowing data subjects to exercise their rights under GDPR
* The processor will assist the controller in meeting its GDPR obligations in relation to the security of processing, notification of data breaches and implementation of Data Protection Impact Assessments
* Delete or return all personal data at the end of the contract
* Submit to regular audits and inspections and provide the relevant information necessary for the controller and processor to meet their legal obligations.
* Nothing will be done by either the controller or processor to infringe on GDPR.

## Conducting a Data Protection Impact Assessment

The organisation will carry out a DPIA when

* using new technologies
* New types of data are being collected.
* The processing is likely to result in a high risk to the rights and freedoms of individuals.

The DPIA will be conducted by the relevant staff member and the data protection officer will provide advice and guidance when needed.

## Suspect loss or exposure of data

If there is a suspected loss or exposure of personal data, the Data Protection Officer is to be informed immediately.

Note the Information Commissioner’s office should be informed within 72 Hours of a suspected breach that is likely to have high risk to the rights and freedoms of a data subject.

## Criminal offence data

### Criminal record checks

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject. All data relating to criminal offences is considered to be a special category of personal data and must be treated as such.

## Audits, monitoring and training

### Data audits

Regular data audits to manage and mitigate risks will in the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant. You must conduct a regular data audit as defined by the DPO and normal procedures.

### Monitoring

Everyone must observe this policy. The DPO has overall responsibility for this policy. Microlink will keep this policy under review and amend or change it as required. You must notify the DPO of any breaches of this policy. You must comply with this policy fully and at all times.

If you require additional training on data protection matters, contact the DPO.

## Reporting breaches

Any breach of this policy or of data protection laws must be reported as soon as practically possible. This means as soon as you have become aware of a breach. Microlink has a legal obligation to report any data breaches to ICO within 72 hours.

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

* Investigate the failure and take remedial steps if necessary
* Maintain a register of compliance failures
* Notify the DPO of any compliance failures that are material either in their own right or as part of a pattern of failures.

Any member of staff who fails to notify of a breach or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures will be liable to disciplinary action.

Please refer to our Data Breach and Incident Management Reporting procedure for more information

### Failure to comply

We take compliance with this policy seriously. Failure to comply puts both you and the organisation at risk.

The importance of this policy means that failure to comply with the policy may result in disciplinary action.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the DPO.