DATA PROTECTION

INFORMATION SECURITY POLICY

AUTHOR: Ken Russell

ROLE: Information Security Manager

ISSUED: December 2025
DOCUMENT ID: IPLICIT-IMS-POLICY-005
VERSION: 2.2
REVIEW DATE: December 2026

Contents

Copyright iplicit, 2025

1. Purpose

The personal data that iplicit processes to provide services relates to its clients and other individuals as necessary, including staff and suppliers' staff.

This policy sets out iplicit's commitment to ensuring that all personal data is processed in compliance with applicable data protection laws and ISO 42001 AI governance standards. We ensure that data used in AI training, validation, and production is handled ethically, maintaining both the Trustworthiness of our AI systems and the privacy of interested parties. iplicit processes the personal data of staff from all over the world, including the personal data of many non-EU citizens, but is committed to ensuring that all the personal data that it processes is done in accordance with data protection law. iplicit ensures that good data protection practice is imbedded in the culture of our staff and our organisation.

iplicit's other data protection policies and procedures are (these should be considered, and may not all be necessary):

- record of processing activities
- privacy notices (website, clients, employees)
- personal data breach reporting process and a breach register
- data retention policy
- data subject rights procedure
- data protection impact assessment process
- IT security policies

'Data Protection Law' includes the General Data Protection Regulation 2016/679; the UK Data Protection Act 2018 and all relevant EU and UK data protection legislation.

2. Scope

The scope of this policy includes all individuals working for and on behalf of iplicit, this includes temporary staff and contingent workers, contractors, and sub-contractors at onshore and offshore locations.

iplicit's network infrastructure is deemed to include infrastructure services and hardware provided to iplicit by its service providers and 3rd party suppliers.

Copyright iplicit, 2025

3. Policy

3.1. Data protection principles

iplicit complies with the data protection principles set out below. When processing personal data, it ensures that:

- it is processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency').
- it is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation').
- it is all adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').
- Data Quality & Accuracy: Personal data must be accurate and kept up to date. In the context of AI, this includes ensuring that training datasets are representative and free from algorithmic bias. We monitor data quality to ensure that AI-driven outcomes do not lead to discriminatory or unfair treatment of data subjects.
- it is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ('storage limitation').
- it is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

iplicit will facilitate any request from a data subject who wishes to exercise their rights under data protection law as appropriate, always communicating in a concise, transparent, intelligible, and easily accessible form and without undue delay.

3.2. Process/procedures/guidance

iplicit will:

- ensure that the legal basis for processing personal data is identified in advance and that all processing complies with the law.

Copyright iplicit, 2025

- not do anything with your data that you would not expect given the content of this policy and the fair processing or privacy notice.

- ensure that appropriate privacy notices are in place advising staff and others how and why their data is being processed and advising data subjects of their rights.

- only collect and process the personal data that it needs for purposes it has identified in advance.

- ensure that, as far as possible, the personal data it holds is accurate, or a system is in place for ensuring that it is kept up to date as far as possible.

- only hold onto your personal data for as long as it is needed, after which time iplicit will securely erase or delete the personal data – iplicit's data retention policy sets out the appropriate period.

- ensure that appropriate security measures are in place to ensure that personal data can only be accessed by those who need to access it and that it is held and transferred securely.

iplicit will ensure that all staff who handle personal data on its behalf are aware of their responsibilities under this policy and other relevant data protection and information security policies, and that they are adequately trained and supervised.

Breaching this policy may result in disciplinary action for misconduct, including dismissal. Obtaining (including accessing) or disclosing personal data in breach of iplicit's data protection policies may also be a criminal offence.

3.3. Data Subject Rights

iplicit has processes in place to ensure that it can facilitate any request made by an individual to exercise their rights under data protection law. All staff have received training and are aware of the rights of data subjects. Staff can identify such a request and know who to send it to.

All requests will be considered without undue delay and within one month of receipt as far as possible.

Subject access: the right to request information about how personal data is being processed, including whether personal data is being processed and the right to be

allowed access to that data and to be provided with a copy of that data along with the right to obtain the following information:

- the purpose of the processing.
- the categories of personal data.
- the recipients to whom data has been disclosed or which will be disclosed.
- the retention period.
- the right to lodge a complaint with the Information Commissioner's Office.
- the source of the information if not collected direct from the subject.
- the existence of any automated decision-making and, crucially, the right to explainability. Data subjects have the right to receive meaningful information about the logic, significance, and envisaged consequences of AI-driven processing, ensuring that our AI operations are transparent and contestable.

Rectification: the right to allow a data subject to rectify inaccurate personal data concerning them.

Erasure: the right to have data erased and to have confirmation of erasure, but only where:

- the data is no longer necessary in relation to the purpose for which it was collected, or
- where consent is withdrawn, or
- where there is no legal basis for the processing, or
- there is a legal obligation to delete data.

Copyright iplicit, 2025

Restriction of processing: the right to ask for certain processing to be restricted in the following circumstances:

- if the accuracy of the personal data is being contested, or
- if our processing is unlawful but the data subject does not want it erased, or
- if the data is no longer needed for the purpose of the processing but it is required by the data subject for the establishment, exercise, or defence of legal claims, or
- if the data subject has objected to the processing, pending verification of that objection.

Data portability: the right to receive a copy of personal data which has been provided by the data subject and which is processed by automated means in a format which will allow the individual to transfer the data to another data controller. This would only apply if iplicit was processing the data using consent or based on a contract.

Object to processing: the right to object to the processing of personal data relying on the legitimate interests processing condition unless iplicit can demonstrate compelling legitimate grounds for the processing which override the interests of the data subject or for the establishment, exercise, or defence of legal claims.

Copyright iplicit, 2025

3.4. Special category personal data

This includes the following personal data revealing:

- racial or ethnic origin.
- political opinions.
- religious or philosophical beliefs.
- trade union membership.
- the processing of genetic data, biometric data, or inferred special category data derived from AI profiling. iplicit prohibits the use of AI systems to 'guess' or infer sensitive traits (such as health status or political leanings) from neutral datasets without a specific, documented legal basis and impact assessment.
- an individual's health.
- a natural person's sex life or sexual orientation.
- criminal convictions or offences.

iplicit processes special category data of clients, and third parties as is necessary to provide legal services for the establishment, exercise or defence of legal claims.

iplicit processes special category data of employees as is necessary to comply with employment and social security law. This policy sets out the safeguards we believe are appropriate to ensure that we comply with the data protection principles set out above. iplicit also has a data retention policy which sets out how long special category data will be held onto.

3.5. Responsibility for the processing of personal data

The iplicit Board of Directors takes ultimate responsibility for data protection and AI Ethics. The Information Security Manager is designated as the AI Risk Lead, responsible for ensuring that Data Protection Impact Assessments (DPIAs) and AI Impact Assessments (AIIAs) are conducted in tandem to address both privacy and algorithmic risks.

If you have any concerns or wish to exercise any of your rights under the UK Data Protection Act 2018, EU General Data Protection Regulations or California Consumer Privacy Act, then you can contact the Compliance Manager during office hours.

5. Compliance & Enforcement

Employees are required to accept responsibility for the actions taken and the things they do and say within their work environment. Information Security is the responsibility of each member of staff. You accept that iplicit always monitors all systems and usage of those systems. Where policy breaches may be detected, this may lead to further investigations being undertaken and/or disciplinary procedures being taken in accordance with HR process and policy.

Copyright iplicit, 2025

6. Document Management

5.1. Document Ownership and Review Cycle

This document is owned by the Information Security Manager. This policy shall be subject to review on an annual basis, in line with the associated Information Security Management System (ISMS).

5.2. Reviewers

Name	Title	Date Reviewed
Ken Russell	Information Security Manager	December 2025

5.3. Authorisation

Name	Title
Lyndon Stickley	CEO
Ed Gairdner	COO
Rob Steele	CFO

Copyright iplicit, 2025

5.4. Document History

Version	Date	Change
2.0	December 2024	Remastered for ISO 27001:2022 Standard
2.1	August 2025	IMS Created Document
2.2	December 2025	Adapted for ISO 42001

Copyright iplicit, 2025