Data Protection Policy

Hypori Ltd (UK)

Version 1.0
15/11/2025

[Policy Owner Name]

Document Revision History

Date	Version	Description	Author	Approval
15/11/2025	1.0	Creation of formal data protection policy.	Claire Robinson	

Hypori

Table of Contents

1. Introduction

This Data Protection Policy is the overarching policy for data security and protection for Hypori Ltd (hereafter referred to as "we", "us", or "our").

2. Purpose

The purpose of this policy is to ensure compliance with applicable data protection legislation, including the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and any other relevant legislation or guidance issued by the Information Commissioner's Office (ICO).

Hypori Ltd recognises that data protection is a fundamental right. We are committed to upholding data protection principles, promoting transparency, and implementing "data protection by design and by default" in all areas of our operations.

3. Scope

This policy applies to all Hypori Ltd employees, contractors, temporary staff, and third parties who process personal data on behalf of Hypori Ltd.

It covers all personal data handled in both electronic and physical formats, including special category data. The policy applies to all business activities, systems, applications, and environments where personal data is created, stored, accessed, shared, or destroyed.

4. Key Terms

Data Controller: The organisation that determines the purpose and means of processing personal data.

Data Processor: A person, company, or organisation that processes personal data on behalf of the data controller, following its documented instructions.

Data Protection Officer (DPO): The individual appointed to oversee data protection strategy and compliance, ensuring personal data is processed legally, securely, and transparently.

Data Subject: Any identifiable living individual whose personal data is processed.

Personal Data: Any information relating to an identified or identifiable individual, including names, contact details, identification numbers, location data, or online identifiers.

Processing: Any operation performed on personal data, including collection, storage, modification, access, sharing, or deletion.

Special Category Data: Personal data that is more sensitive, such as data revealing racial or ethnic origin, political opinions, religious beliefs, health data, or biometric data.

5. Data Protection Principles

Hypori Ltd will ensure that personal data is:

- Processed lawfully, fairly, and transparently
- Collected for specified, explicit, and legitimate purposes and not further processed incompatibly with those purposes
- Adequate, relevant, and limited to what is necessary (“data minimisation”)
- Accurate and, where necessary, kept up to date
- Retained only for as long as necessary for the purpose for which it is processed (“storage limitation”)
- Processed securely, using appropriate technical and organisational measures to protect against unauthorised or unlawful processing, accidental loss, destruction, or damage

We also uphold the personal data rights established under the UK GDPR, including

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure (“right to be forgotten”)
- The right to restrict processing
- The right to data portability
- The right to object
- Rights related to automated decision-making and profiling

Consent for processing will be obtained where required, in clear and accessible language, and individuals will have the right to withdraw consent as easily as it was given.

6. Underpinning Policies and Procedures

This policy is supported by the following documents and procedures:

- Data Quality Policy – Ensures data accuracy and integrity
- Record Keeping Policy – Defines data retention, disposal, and subject rights procedures
- Data Security Policy – Outlines security controls and incident reporting processes
- Business Continuity and Disaster Recovery Plan – Defines how systems and data are recovered following an incident
- Staff Code of Conduct / Information Governance Handbook – Provides clear guidance for employees handling personal data

7. Data Protection by Design and by Default

Hypori Ltd integrates data protection considerations into all new systems, projects, and processes from the outset.

- Data protection risks are assessed using Data Protection Impact Assessments (DPIAs) where processing may present a high risk to individuals.
- Systems used for processing personal data must be designed to include appropriate security and privacy controls.
- The Record of Processing Activities (ROPA) is maintained and reviewed annually.
- By default, personal data will only be processed when necessary for specific lawful purposes.
- Where possible, pseudonymisation or anonymisation will be used to minimise risk to individuals.

8. Policy Leadership

The [Policy Owner Name] is responsible for maintain and upholding data protection standards.

Responsibilities include:

- Ensuring the rights of individuals are upheld and that personal data is processed lawfully and securely
- Overseeing data protection strategy, compliance, and training
- Monitoring compliance with UK GDPR and the Data Protection Act 2018
- Managing Data Protection Impact Assessments (DPIAs)

- Reporting on compliance to senior management
- Liaising with the Information Commissioner's Office (ICO) when necessary

9. Review and Maintenance

Policy Review

This policy will be reviewed annually or following significant organisational, legal, or technological change.

The [Policy Owner Name] is responsible for ensuring that reviews are conducted, documented, and approved by senior leadership.

Non-Compliance

Any breaches or non-compliance identified under this policy must be reported immediately to the [Policy Owner Name] or senior management.

Appropriate remedial action must be taken to address any gaps or risks identified.

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or contract.

10. References (updated October 2025)

External Standards and Frameworks

- ISO/IEC 27001:2022 – Information Security Management Systems – Requirements
- ISO/IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection – Information Security Controls
- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Data (Use and Access) Act 2025 (if applicable)
- Human Rights Act 1998
- NIST SP 800-63B-4 – Digital Identity Guidelines – Authentication and Lifecycle Management
- Cyber Essentials Plus Scheme – Requirements for IT Infrastructure (latest version)

ISO/IEC 27001:2022 Control Mapping

Primary Control

- Information Deletion (A.8.10)

Secondary Controls

- Policies for Information Security (A.5.1)
- Roles and Responsibilities (A.5.2)
- Acceptable Use of Information and Associated Assets (A.5.10)
- Information Transfer (A.5.14)
- Data Masking (A.8.11)
- Data Leakage Prevention (A.8.12)
- Secure Communication (A.8.25)

Related Company Policies and Procedures

- Access Control Policy
- Acceptable Use Policy
- Information Classification and Handling Policy
- Record Keeping Policy
- Data Quality Policy
- Data Security Policy
- Backup Policy
- Secure Destruction of Client Data Process
- Subject Access Request Procedure
- Incident Response Plan
- Business Continuity and Disaster Recovery Plan

- Clear Desk and Clear Screen Policy