

Intuition Publishing Ltd. Data Protection Policy

Table of Contents

Introduction.....	3
Purpose.....	3
Scope	3
General Data Protection Regulation	3
Data Protection and Processing Principles.....	4
Data Subject Rights	4
Legal Basis for Data Processing	5
Consent	5
Performance of a Contract.....	5
Legal Obligations	5
Vital Interests of a Data Subject.....	5
Public Interest Tasks.....	6
Legitimate Interests.....	6
Privacy by Design.....	6
Contracts for Processing of Personal Data	6
International Transfers of Personal Data	6
Data Protection Officer	7
Data Breach Notification	7
Roles and Responsibilities	7
GDPR Compliance.....	8
Policy Implementation	8
Glossary of Definitions	9

Introduction

Intuition Publishing Ltd (“Intuition”) is a leading provider of technology-enabled eLearning and Knowledge Management services and solutions to a broad range of commercial sectors including the financial markets, the pharmaceutical and life sciences industries as well as public sector and healthcare organizations. We are committed to protecting your privacy and recognise our responsibilities to hold your information securely and confidentially.

Purpose

The purpose of this Data Protection Policy is to describe the steps that enable Intuition to follow and comply with the provisions of the European Union’s General Data Protection Regulation (GDPR) and subsequent amendments and related legislation with respect to all personal data collected, processed and held by the company. This includes data on:

- Current, Former and Prospective Employees
- Clients and their Users
- Website Visitors and Users
- Subscribers
- Other Stakeholders

The following policies and procedures are relevant to this Data Protection Policy:

- Privacy Notice for Employees
- Privacy Notice for Customers
- Data Subject Access Request Policy and Response Workflow
- Information Security Incident Response Procedure
- Data Retention Policy
- Data Protection Impact Assessment (DPIA)
- Legitimate Interest Assessment Procedure

Scope

This policy is based on the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (“General Data Protection Regulation” or “GDPR”). The GDPR emphasises transparency, security and accountability by data controllers and processors, while also providing a robust framework for standardising and strengthening the rights of European citizens to data privacy.

This policy applies to all company staff (including directors, employees, contractors, suppliers and any other third parties) who have access to any of our systems or information assets that contain personal data collected, processed and held in either electronic or paper form by Intuition on behalf of our employees, clients, suppliers and service providers.

Please note that Intuition acts as a Data Controller in respect of personal data processed for our employees and acts as a Data Processor for personal data processed on behalf of our clients.

General Data Protection Regulation

The GDPR is one of the most important pieces of data protection legislation that affects how Intuition conducts its various information processing activities. Significant fines apply if a personal data breach is deemed to have occurred under the GDPR, which is designed to protect the personal data of EU citizens. It is the policy of Intuition to ensure full, clear and demonstrable compliance with the GDPR at all times.

Data Protection and Processing Principles

Intuition has adopted the following core principles to govern its collection, processing and storage of personal data under the relevant GDPR provisions.

These principles state that personal data must:

1. Be processed lawfully, fairly and in a transparent manner in relation to the data subjects ('lawfulness, fairness and transparency').
2. Be collected for specified, explicit and legitimate purposes and shall not be further processed in a manner that is incompatible with those purposes; ("purpose limitation").
3. Be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed ("data minimisation").
4. Be accurate and where necessary kept up to date; every reasonable step must be taken to ensure that inaccurate personal data is corrected or deleted without delay, having regard to the purposes for which it is processed ("data accuracy").
5. Be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which it is processed.
6. Be processed in a manner that ensures appropriate security of the personal data using appropriate technical and organisational controls against unauthorised or unlawful processing and against accidental loss, destruction or damage ("data integrity and confidentiality").
7. Not be transferred to a country or territory outside the European Union except when in compliance with conditions for transfer specified under the relevant GDPR provisions.

Intuition will ensure that it complies with all of these principles for both its current data processing activities and as part of any new processing methods such as the introduction of new IT systems.

Data Subject Rights

Each data subject has the following rights under the GDPR with respect to the processing of their personal data:

1. The right to be informed.
2. The right to access.
3. The right to rectification.
4. The right to deletion.
5. The right to restrict processing.
6. The right to data portability.
7. The right to object.
8. Automated decision making and profiling rights.

Intuition supports each of these data subject's rights with appropriate procedures that allow the required action to be taken within the GDPR mandatory timescales indicated below:

Data Subject Request	Timescale
The right to be informed	When data is collected (if provided by data subject) or within one month (if not provided by data subject)
The right to access	Without undue delay and in any event within one month (may be extended by two further months where necessary due to complexity and number of requests)
The right to rectification	Without undue delay and in any event within one month (may be extended by two further months where necessary due to complexity and number of requests)

The right to deletion	Without undue delay and in any event within one month (may be extended by two further months where necessary due to complexity and number of requests)
The right to restrict processing	Without undue delay and in any event within one month (may be extended by two further months where necessary due to complexity and number of requests)
The right to data portability	Without undue delay and in any event within one month (may be extended by two further months where necessary due to complexity and number of requests)
The right to object	Without undue delay and in any event within one month (may be extended by two further months where necessary due to complexity and number of requests)
Automated decision making and profiling rights	Without undue delay and in any event within one month (may be extended by two further months where necessary due to complexity and number of requests)

Legal Basis for Data Processing

Under GDPR, there are six different legal bases under which a data subject's personal data can be processed. It is Intuition's policy to identify the appropriate legal basis for data processing and document it in accordance with the GDPR. Each option is described briefly in the following sections.

Consent

Intuition will always obtain explicit consent from a data subject to collect and process their personal data for one or more specific purposes unless the processing falls under one of the other five permitted legal bases for processing under the GDPR.

For children below the age of 16 years (a lower age may be permitted in certain EU member states), we will obtain parental consent in all such cases. Intuition will provide transparent information to data subjects regarding our usage of their personal data and their rights at the time that their consent is obtained including the right to withdraw their consent. We will provide this information in an accessible form, written in clear language and free of charge.

If the personal data is not obtained directly from the data subject, then Intuition will provide this information to the data subject within one month after the data was obtained.

Performance of a Contract

Where personal data collected and processed is required to fulfil a legal contract with the data subject, then explicit consent is not required from the data subjects. This applies where Intuition has signed a legal contract with a client for the provision of our eLearning software, Knowledge Management and Consultancy services and solutions and the data subjects' personal data is necessary for completion of the contract. Note that where the client is not an individual, or where the client is not the same person as the data subject, the client will be required to confirm that it has a legal basis for providing the information on the data subject to Intuition.

Legal Obligations

Where Intuition acting as a Data Controller is required to collect and process a data subject's personal data to comply with a legal obligation such as an EU member state's employment or taxation legislation, then explicit consent is not required from the data subjects to process the data required.

Vital Interests of a Data Subject

Where personal data is required to be processed to protect the vital interests of the data subject or of another natural person, then such processing is regarded as lawful under the GDPR. Intuition will retain reasonable documented evidence to cover this case whenever this reason is used as the lawful basis for this type of processing

of personal data.

Public Interest Tasks

Where Intuition is required to perform a task that we believe is in the public interest as laid down by law or as part of an official duty, then explicit consent is not required from the data subjects. The assessment of the public interest task or official duty will be documented by Intuition.

Legitimate Interests

If the processing of specific personal data is in the legitimate interests of Intuition and a proportionality assessment is carried out that determines that Intuition's legitimate interests are not overridden by the interests or fundamental rights and freedoms of the data subject, then this may be defined as the lawful basis for processing. The legitimate interests assessment will be documented by Intuition. Note that where Intuition is working with public authorities in the performance of their tasks, legitimate interests may not be an adequate lawful basis for processing.

Privacy by Design

Intuition has adopted the principle of privacy by design and will ensure that the definition and planning of all new or significantly updated software and IT systems that collect or process personal data will be subject to due consideration of data privacy risks, including the completion of data protection impact assessments where necessary.

The data protection impact assessment will include:

- Consideration of how personal data will be processed and for what purpose(s).
- Assessment of whether the proposed processing of personal data is both necessary and proportionate to the purpose(s).
- Assessment of the risks to data subjects in processing their personal data.
- Determination of what controls are necessary to address the identified risks and demonstrate compliance with the GDPR.

Intuition will consider the use of data minimisation and pseudonymisation technologies where applicable and appropriate.

Contracts for Processing of Personal Data

Intuition will ensure that all business agreements that it enters into with our clients, service providers or third parties that involve the processing of personal data are subject to a documented legal contract that includes specific provisions and terms as required by the GDPR.

International Transfers of Personal Data

As a global organisation with offices in various countries, where legally permissible, Intuition may store, use, transfer, and otherwise process employees and customers personal data in countries outside of the country of their residence, which may have different data protection rules.

Intuition may transfer and/or disclose employees and customers personal data to any company within the Intuition group of companies and to specific third parties acting on Intuition's behalf. Such intra-group international data transfers will be subject to legally binding agreements known as Binding Corporate Rules (BCR), which provide enforceable rights for data subjects.

This also includes data transfers to servers and databases located outside the country where employees or clients provided Intuition with their personal data. Such data transfers may include transfers and/or disclosures outside the European Economic Area (EEA) and in the United States of America.

Intuition will not transfer personal information outside the EEA to a third country or international organisation that does not provide an adequate level of data protection, without explicit consent.

Data Protection Officer

Intuition is not required to appoint a Data Protection Officer (DPO) as it does not meet the GDPR requirements or criteria for such an appointment. However, Derek Doran, General Manager of Operations has been assigned responsibility to oversee compliance with Data Protection Policy. If you have any questions about this Data Protection Policy or how we handle your personal information, please contact gdpr@intuition.com. You also have the right to make a complaint at any time to the Office of the Data Protection Commissioner, the Irish supervisory authority for data protection issues.

Data Breach Notification

It is the policy of Intuition to be fair and proportionate when considering the reporting actions required when notifying affected parties regarding any breaches of their personal data. In accordance with the GDPR, where a data breach is known to have occurred that is likely to result in a risk to the rights and freedoms of individuals, Intuition will notify the relevant Supervisory Authority with 72 hours. For more information, please refer to the company's *Information Security Incident Response Procedure*, which sets out the overall process for handling and managing any information security incidents and data breaches.

Roles and Responsibilities

Each staff member (including both employees and contractors) at Intuition is responsible for ensuring that personal data is collected, handled and stored appropriately. Each Intuition team that handles personal data must ensure that it is handled and processed in accordance with this Data Protection Policy and the GDPR's Data Protection Principles. However, the following Intuition staff have key additional responsibilities under the GDPR:

- The **Management** team and the **Board of Directors** has ultimate responsibility for ensuring that Intuition meets its legal obligations.
- The **Information Security** team is responsible for:
 - Keeping the Management team informed about data protection responsibilities, risks and issues and changes to existing or new data privacy legislation.
 - Reviewing all data protection procedures and related policies in accordance with an agreed schedule.
 - Arranging information security training and advice for all company staff covered by this Data Protection Policy.
 - Handling all data protection queries and data subject access requests from all company staff covered by this Data Protection Policy.
 - Handling all data protection queries and data subject access requests from the company's clients.
 - Handling all correspondence, enquiries and audit notifications from the Supervisory Authority.
 - Reviewing and approving any contracts or agreements with any third parties that may handle the company's sensitive data or our employees' personal data.
- The **Intuition Technical Support (ITS)** team is responsible for:
 - Ensuring that all systems, services and equipment used for collecting, processing and storing personal data meets acceptable security standards and controls.
 - Conducting regular checks and scans to ensure that IT security hardware and software is operating correctly.
 - Evaluating any third-party services and IT systems that the company is considering using to process and store personal data.

- The **Marketing Team** is responsible for:
 - Approving any data protection statements attached to any marketing collateral such as emails, corporate website forms and cookies statement.
 - Working with other company staff to ensure any existing or new marketing campaigns and initiatives comply with the GDPR data protection principles.
 - Handling any data protection queries from media outlets in the event of a company data breach.

GDPR Compliance

The following actions are undertaken by Intuition to ensure that the company complies at all times with the GDPR accountability principle:

- The legal basis for processing personal data is documented, clear and unambiguous.
- All company staff involved in handling personal data understand their responsibilities with respect to best practices for data protection.
- All company staff receive mandatory information security training on at least an annual basis.
- All GDPR rules regarding obtaining a data subject's consent are correctly applied.
- Various options are available to data subjects who wish to exercise their rights regarding personal data and such access requests and enquiries are effectively handled.
- Regular reviews of procedures for handling personal data are conducted by qualified company staff.
- Privacy by design is adopted for all new or significantly updated software and IT systems that process personal data.
- Periodic reviews are carried out to determine that any personal data collected is not excessive.

These actions are reviewed on a regular basis as part of company's data protection management program.

Policy Implementation

This Data Protection Policy is made available to all company staff through the corporate ISO 9001:2015 certified Quality Management System (QMS) Intranet. Intuition reserves the right to update this policy at any time to comply with any new data protection legislation including amendments and updates to the GDPR. Notice of significant revisions of this policy will be provided to company staff through the company's QMS Intranet.

Glossary of Definitions

Consent means any freely given, specific, unambiguous and informed affirmative act by which the data subject signifies agreement to their personal data being processed.

Data Controller means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

Data Processor means a person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Data Subject means an individual about whom the personal data relates. Data subjects can include customers and website users, individuals on contact/emailing lists or marketing databases, employees, contractors and suppliers.

Personal Data means data related to a living person who can be directly or indirectly identified from that data or from that data and other information in the possession of a data controller or data processor. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way that organisations collect information about people.

Processing Data covers a wide variety of operations relating to data, including obtaining, recording or holding data or carrying out any operation or set of operations on data, including:

- Hosting, storing or viewing
- Organisation, adaptation, or alteration
- Disclosure by transmission, dissemination, or otherwise
- Alignment, combination, blocking, erasure, or destruction.

Sensitive Data means personal data containing information as to the data subject's:

- Race or ethnic origin;
- Religious beliefs or other beliefs of a similar nature;
- Political opinions;
- Physical or mental health or condition;
- Sexual history or orientation;
- Trade union membership;
- Commission or alleged commission of any offense and any related court proceedings.