



Privacy and Data Protection **Policy**

General Data Protection Regulation (GDPR)

LET'S MAKE THE WORLD BETTER WITH OUR TECHNOLOGIES!

	Privacy and Data Protection Policy	POL.RRH.02 Rev.00
		Date: 16/06/2026

Document Information:

Title:
Data Protection Policy

Edition:
Human Resources Department

Publication Date:
June 2026

	Privacy and Data Protection Policy	POL.RRH.02 Rev.00
		Date: 16/06/2026

TABLE OF CONTENTS

- 1. Purpose
- 2. Data Protection Principles
- 3. Collection and Processing of Personal Data
 - 3.1. Scope
 - 3.2. Data Collected
 - 3.3. Purposes and Legal Basis for Processing
 - 3.4. Consent
 - 3.5. Video Surveillance
- 4. Disclosure, Transfers, Retention, Deletion and Security of Personal Data
 - 4.1. Disclosure
 - 4.2. International Transfers of Personal Data
 - 4.3. Retention and Deletion
 - 4.4. Security
 - 4.5. Personal Data Breaches
- 5. Data Subjects' Rights
 - 5.1. Processes and Procedures for Requesting Access to Personal Data Processed or for Lodging a Privacy Complaint with the Supervisory Authority
- 6. Updates to the Privacy Policy

	Privacy and Data Protection Policy	POL.RRH.02 Rev.00
		Date: 16/06/2026

1. Purpose

The purpose of this Privacy and Data Protection Policy is to provide clear, transparent, and concise information to data subjects, including website users, customers, suppliers, service providers, and business partners, regarding the processing of their personal data by **Ultimate Technology to Industrial Savings, S.A. (UTIS)**.

UTIS, with its registered office at **Estrada Nacional 249-4, Km 4, São Domingos de Rana, 2785-035 Cascais, Portugal**, recognises the importance of privacy and the protection of personal data and is committed to ensuring that such data is processed in accordance with the principles and requirements established by **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation – GDPR)**, as well as all applicable national legislation.

This Policy also defines the rights of data subjects and describes the mechanisms available for exercising those rights, thereby promoting trust and transparency in UTIS's relationships with all stakeholders.

2. Data Protection Principles

UTIS respects the privacy and protection of the personal data it processes in the course of its business activities, ensuring compliance with the **GDPR** and applicable national legislation.

UTIS is committed to ensuring that personal data is:

- Processed lawfully, fairly, and transparently;
- Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed;
- Accurate and, where necessary, kept up to date;
- Retained only for as long as necessary to fulfil the purposes of the processing;
- Processed in a manner that ensures appropriate security and confidentiality.

	Privacy and Data Protection Policy	POL.RRH.02 Rev.00 Date: 16/06/2026

3. Collection and Processing of Personal Data

3.1. Scope

This Policy applies to the processing of personal data carried out by UTIS in its capacity as Data Controller, including personal data collected through the website www.utis.pt, as well as data obtained in the context of contractual, commercial, and institutional relationships with customers, suppliers, service providers, business partners, and other data subjects.

3.2. Data Collected

UTIS may collect, among others, the following categories of personal data:

- Identification data (name, image, job title, tax identification number (TIN));
- Professional data (company, job title, employee number);
- Contact details (email address, telephone number, postal address);
- Technical data (IP address, website access logs);
- Data required for the performance of contracts, invoicing, or technical support;
- Recruitment and job application data (name, telephone number, email address, CV/résumé).

3.3. Purposes and Legal Basis for Processing

UTIS processes personal data for the following purposes and on the following legal bases:

- **Managing enquiries and information requests submitted through the website** – legal basis: UTIS's **legitimate interest** in responding to enquiries and managing its business activities (Article 6(1)(f) of the GDPR);
- **Managing customers and suppliers**, including the conclusion and performance of contracts, invoicing, and communications necessary for the contractual relationship – legal basis: **performance of a contract** and **compliance with legal obligations** (Article 6(1)(b) and (c) of the GDPR);
- **Institutional and technical communications** within the framework of the contractual relationship – legal basis: UTIS's **legitimate interest** in ensuring the effective management and continuity of its relationships with customers and suppliers (Article 6(1)(f) of the GDPR);
- **Compliance with legal and tax obligations** – legal basis: **compliance with a legal**

	Privacy and Data Protection Policy	POL.RRH.02 Rev.00
		Date: 16/06/2026

obligation to which UTIS is subject (Article 6(1)(c) of the GDPR);

- **Sending commercial communications**, where applicable – legal basis: the **data subject's consent** (Article 6(1)(a) of the GDPR);
- **Managing recruitment processes and job applications** – legal basis: **pre-contractual steps** taken at the request of the data subject and, where applicable, **consent** (Article 6(1)(b) and (a) of the GDPR);
- **Protecting people and property**, including the use of video surveillance at UTIS premises – legal basis: UTIS's **legitimate interest** in ensuring the security of its premises (Article 6(1)(f) of the GDPR), in accordance with the applicable legislation.

Personal data is processed by both manual and automated means. UTIS implements appropriate technical and organisational measures to ensure the security, integrity, and confidentiality of personal data.

3.4. Consent

Where the processing of personal data is based on the data subject's consent, such consent shall be obtained freely, specifically, informedly, and unambiguously through a statement or a clear affirmative action, following the provision of appropriate information regarding the purposes of the processing.

The data subject may withdraw their consent at any time, easily and free of charge, without affecting the lawfulness of any processing carried out based on the consent provided prior to its withdrawal.

3.5. Video Surveillance

UTIS operates video surveillance systems at its premises for the purposes of protecting people and property, preventing unlawful activities, enhancing the physical security of its facilities, and supporting the investigation of security incidents.

The processing of images captured by these video surveillance systems is based on UTIS's legitimate interest in protecting its premises, employees, customers, suppliers, and other visitors, in accordance with Article 6(1)(f) of the GDPR, without prejudice to compliance with applicable national legislation.

	Privacy and Data Protection Policy	POL.RRH.02 Rev.00 Date: 16/06/2026

The video surveillance systems are appropriately signposted by means of information notices displayed in clearly visible locations before entry into the monitored areas.

The images collected are used exclusively for the security purposes described above and shall not be used for the continuous monitoring of employees' work performance or for any purpose incompatible with those for which they were originally collected.

Access to recorded images is restricted to persons expressly authorized by UTIS and, where legally required, to the competent judicial, law enforcement, or administrative authorities.

Recordings shall be retained for the maximum period permitted by law, currently 30 days, after which they are automatically deleted unless a longer retention period is required for the purposes of a criminal investigation, judicial proceedings, or compliance with a legal obligation.

UTIS implements appropriate technical and organisational measures to ensure the security, integrity, confidentiality, and traceability of access to the recorded images.

Data subjects retain all rights granted to them under the applicable data protection legislation, including the rights of access, restriction of processing, and the right to lodge a complaint with the Portuguese Data Protection Authority (Comissão Nacional de Proteção de Dados – CNPD), without prejudice to any legal restrictions where the exercise of such rights may adversely affect the rights of third parties, ongoing investigations, or public security interests.

The processing of personal data through video surveillance systems is carried out in accordance with Regulation (EU) 2016/679 (GDPR), Law No. 58/2019 of 8 August, and all other applicable legislation governing data protection and private security.

	Privacy and Data Protection Policy	POL.RRH.02 Rev.00
		Date: 16/06/2026

4. Disclosure, Transfers, Retention, Deletion and Security of Personal Data

4.1 Disclosure

UTIS does not disclose personal data to third parties except where such disclosure is necessary for:

- Compliance with legal obligations;
- The performance of a contract to which the data subject is a party;
- The protection of the vital interests of the data subject;
- Situations where the data subject has given their explicit consent.

Where personal data is shared, any third party processing personal data on behalf of UTIS acts as a data processor and is bound by a written agreement ensuring the confidentiality and security of the personal data.

Personal data may be disclosed only to the following categories of recipients, strictly to the extent necessary to fulfil the purposes described in this Policy:

- Hosting and IT infrastructure service providers;
- IT support and maintenance service providers;
- Legal, accounting, and tax advisers;
- Financial institutions and payment service providers;
- Insurance companies;
- Administrative, regulatory, or judicial authorities, where disclosure is required by law;
- Public authorities with statutory supervisory or enforcement powers.

All data processors are bound by written agreements that ensure compliance with the obligations set out in Article 28 of the GDPR.

4.2 International Transfers of Personal Data

As a general rule, UTIS does not transfer personal data to third countries or international organisations located outside the European Economic Area (EEA).

However, where such transfers become necessary in the course of its business activities, including through the use of external service providers or when accessing customers' premises, UTIS will ensure that any international transfer is carried out in full compliance with Articles 44 to 50 of the GDPR, implementing the appropriate technical, organisational, and legal safeguards to ensure a level of data protection equivalent to that required within the

	Privacy and Data Protection Policy	POL.RRH.02 Rev.00
		Date: 16/06/2026

European Union.

International transfers may be based on one or more of the following legal mechanisms:

- a) Adequacy Decisions adopted by the European Commission pursuant to Article 45 of the GDPR, where the destination country has been formally recognised as providing an adequate level of data protection;
- b) Standard Contractual Clauses (SCCs) approved by the European Commission pursuant to Article 46 of the GDPR, entered into between UTIS and the recipient of the personal data;
- c) Binding Corporate Rules (BCRs), where applicable;
- d) Any other appropriate safeguards expressly provided for under applicable data protection legislation.

Where necessary, and particularly in light of the case law of the Court of Justice of the European Union (CJEU), UTIS will assess the risks associated with the transfer and implement supplementary technical, organisational, and contractual measures to ensure the effective protection of the transferred personal data, including, where appropriate:

- Encryption of personal data in transit and at rest;
- Pseudonymisation of personal data;
- Strict access controls;
- Enhanced monitoring and auditing measures;
- Limitation of the volume of personal data transferred.

Data subjects may request additional information regarding any international transfers of personal data and the safeguards implemented by contacting UTIS using the contact details provided in this Policy.

4.3 Retention and Deletion

Personal data shall be retained only for the period necessary to fulfil the purposes for which it was collected and in accordance with the applicable legal retention periods.

Retention periods:

Customers / contractual relationship: 10 years' retention;

Invoicing: 10 years' retention;

Recruitment (where no employment relationship is established): 12 months;

Video surveillance: 30 days;

Contact requests: 2 years;

	Privacy and Data Protection Policy	POL.RRH.02 Rev.00
		Date: 16/06/2026

Security logs: 12 months' retention.

After the expiry of these periods, the personal data shall be securely deleted or irreversibly anonymised, without prejudice to its retention for additional periods where necessary for the purposes of complying with legal obligations or for the establishment, exercise, or defence of legal claims in judicial proceedings.

4.4 Security

UTIS implements appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or unauthorised access, including:

- Restricted access to authorised personnel;
- Secure cloud servers located within the European Union;
- Encryption and authentication protocols;
- Monitoring of security incidents.

Users are also responsible for ensuring that their devices and access credentials are used securely.

4.5. Personal Data Breaches

UTIS has established internal procedures for the detection, assessment, containment, and management of security incidents that may compromise the confidentiality, integrity, or availability of the personal data it processes.

Where a personal data breach is likely to result in a risk to the rights and freedoms of data subjects, UTIS shall notify the Portuguese Data Protection Authority (Comissão Nacional de Proteção de Dados – CNPD) without undue delay and, where feasible, within 72 hours of becoming aware of the breach, in accordance with Article 33 of the GDPR.

Where the personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, UTIS shall also communicate the breach to the affected data subjects without undue delay, in accordance with Article 34 of the GDPR.

	Privacy and Data Protection Policy	POL.RRH.02 Rev.00
		Date: 16/06/2026

5. Data Subjects' Rights

In accordance with the applicable legislation, data subjects have the following rights:

- **The right to access** their personal data;
- **The right to rectify inaccurate or incomplete** personal data;
- **The right to erasure** ("right to be forgotten");
- **The right to restriction of processing**;
- **The right to data portability**, where applicable;
- **The right to object to the processing** of their personal data;
- **The right to withdraw any consent** previously given.

The exercise of these rights is free of charge, except where a request is manifestly unfounded or excessive. UTIS is committed to responding to all requests within a maximum period of **30 days** from the date of receipt.

5.1. Processes and Procedures for Requesting Access to Personal Data Processed or for Lodging a Privacy Complaint with the Supervisory Authority

Data subjects may exercise their rights or request any additional information by contacting:

The **Data Controller** is Ultimate Technology to Industrial Savings, S.A. (UTIS), with its registered office at Estrada Nacional 249-4, Km 4, São Domingos de Rana, 2785-035 Cascais, Portugal. UTIS may be contacted regarding any matters relating to data protection by email at hr@utis.pt.

Data Protection Contact: Human Resources Manager, Patrícia Ferreira Raimundo.

Following an assessment of the nature, scope, context, and purposes of its processing activities, UTIS has concluded that it is not legally required to appoint a Data Protection Officer (DPO) pursuant to Article 37 of the GDPR. Notwithstanding the above, any queries relating to the processing of personal data may be addressed to hr@utis.pt. If a data subject considers that UTIS has infringed their rights or failed to comply with its legal obligations concerning data protection, they have the right to lodge a complaint with the competent supervisory **authority, the Portuguese Data Protection Authority (Comissão Nacional de Proteção de Dados – CNPD)**, via its website: www.cnpd.pt.

	Privacy and Data Protection Policy	POL.RRH.02 Rev.00
		Date: 16/06/2026

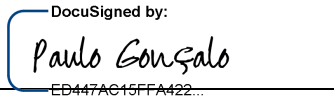
6. Updates to the Privacy Policy

UTIS reserves the right to amend or update this Privacy Policy whenever necessary to ensure its compliance with legal or organisational changes.

The most up-to-date version of this Policy will always be made available at www.utis.pt, together with the date of the latest revision.

São domingos de Rana, 15 june 2026

Executive Committee

Paulo Gonalo (CEO) 

Luís Nabais (CFO) 