INTEGER CONSULTING

Privacy and Personal Data Protection Policy

Code:	PS.19
Version:	02
Version Date:	25/07/2025
Author:	IMS
Approved by:	IMS Manager
Classification:	Public

* ISO 9001:2015, ISO/IEC 27001:2022 and ISO/IEC 27701:2019

Change History

Date	Version	Author	Description of Change
18/02/2022	01	IMS	Initial Version
25/07/2025	02	IMS	New template, inclusion of paragraphs: 1. Objective, 2. Scope, 3. Recipients, 5. Associated Documents, 6. Reference Documents, 7. Definitions and Acronyms, 8. Review and Validation, and 9. Conclusion.

Table of Contents

1. Objective

The objective of this policy is to establish the principles, rules and practices of Integer Consulting S.A., hereinafter referred to as INTEGER, for the processing of personal data, ensuring its compliance with the General Data Protection Regulation (GDPR), ISO/IEC 27001 and ISO/IEC 27701 standards, as well as applicable national legislation and regulations, ensuring the rights of data subjects and the trust of its partners, customers and employees.

2. Scope

This policy applies to all INTEGER activities involving the processing of personal data, regardless of the medium or form, including processing carried out by computer, on paper or by other automated or manual means. It applies to all employees, service providers, partners, customers, subcontractors and any third parties who, in the course of their duties, access or process personal data on behalf of INTEGER.

3. Recipient

This policy is intended for all INTEGER employees, service providers, suppliers, partners, customers and any third parties with whom personal data is shared or processed in the context of the organisation's activities.

4. Process

This policy explains the fundamental information and rules regarding the processing of personal data in our activities. To facilitate understanding, we present this policy in the form of questions and answers:

4.1 Who is responsible for processing?

Integer, headquartered at Rua Julieta Ferrão nº 10 8º Piso 1600-131 Lisbon, taxpayer no. 507969332, is responsible for the processing of personal data. You can contact them through the contact details available on the website or by email at rgpd@integer.pt.

4.2 What is personal data?

Personal data is 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.

4.3 What is sensitive personal data?

Sensitive personal data is information relating to a natural person concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data that allows a person to be identified unambiguously, data concerning health, data concerning sex life or sexual orientation.

4.4 What principles do we follow when processing personal data?

When processing personal data, we respect the following principles:

- Principle of lawfulness: personal data may only be processed under the conditions provided for by law;
- Principle of fairness and transparency: the processing of personal data must always be carried out in a fair and transparent manner towards the data subjects;
- Principle of purpose limitation: personal data must be collected for specific, explicit and legitimate purposes and may not be further processed in a manner incompatible with the purposes of collection;
- Principle of minimisation: Only personal data that is adequate, relevant and necessary for the purposes of processing should be collected and processed;
- Principle of accuracy: Data must be accurate and up to date. Inaccurate data must be rectified without delay;
- Principle of storage limitation: Personal data must be stored in a way that allows the identification of data subjects only for the period strictly necessary for the purposes for which they are processed;
- Principle of integrity and confidentiality: Personal data must be processed in a manner that ensures its security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures;
- Principle of accountability: the controller must comply with all the principles set out and be able to demonstrate such compliance.

4.5 When can we process personal data?

Whenever any of the following circumstances apply:

- Consent: by 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;
- Contracts: Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- Legal obligation: processing is necessary for compliance with a legal obligation to which the controller is subject (legal powers and duties);
- Legitimate interest: Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

4.6 When can we process sensitive personal data?

Whenever any of the following circumstances apply:

- Consent: by 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;
- Compliance with obligations and the exercise of specific rights: Processing necessary for compliance with obligations and the exercise of specific rights of the controller or data subject in the field of labour law, social security and social protection;
- Processing necessary for preventive or occupational medicine: for the assessment of the employee's working capacity, medical diagnosis, the provision of health care or treatment.

4.7 What are the rights of personal data subjects?

We will facilitate the exercise of the following rights by data subjects:

- Confirmation that personal data is being processed: the right to obtain information about whether and which data is being processed;
- Right of access to personal data: to consult and obtain a copy of the data processed;
- Right to rectify data: rectify and update the data processed;
- Right to restriction of processing: under certain conditions, the right to restrict the processing of your personal data;
- Right to lodge a complaint: You have the right to lodge a complaint with the competent supervisory authority, the National Data Protection Commission (CNPD), if you consider that the processing of your personal data violates your rights and/or the applicable data protection laws. You can do so via the website www.cnpd.pt.
- Right to erasure of data ("right to be forgotten"): under certain conditions, request the erasure of your personal data. To do so, you must send an email to rgpd@integer.pt.
- Right to data portability: obtain and transmit personal data in a structured, commonly used and machine-readable format;
- Right to object to processing: to object at any time, on grounds relating to your particular situation, to the processing of personal data;
- Right to withdraw consent: in the same way that you gave your consent, you can withdraw it without compromising the lawfulness of the processing already carried out;

The exercise of these rights, under the terms and conditions provided for in the legislation, may vary depending on the grounds for data processing.
For assistance in exercising these rights, simply contact us using the contact details provided above.

4.8 When do we process personal data and for what purposes?

We process personal data when:

- Data subjects submit applications for job opportunities, unsolicited applications or applications for professional internships;
- Data subjects submit CVs to us in selection and recruitment processes, including for the development of projects with our clients;
- Data subjects submit proposals to us or request other pre-contractual negotiations for service provision contracts;
- With the prior consent of the data subjects, the data may be shared with clients with a view to approving the professional profile for the placement of outsourced professionals;
- Contracts are entered into, including employment contracts with employees, service contracts with service providers, contracts with suppliers, and contracts with clients;
- In contracts with service providers, suppliers, and clients, we may process personal data of natural persons who are sole traders, or of legal representatives and employees of legal persons for the purposes of performing the contract;
- The law requires or allows the processing of personal data, namely labour, social security, tax and occupational health legislation and for the purposes set out in that legislation;
- Personal data may be transmitted to third parties, public and private entities in compliance with legal obligations or the execution of contracts;
- Data subjects give their consent to the processing of personal data, namely in the collection of images or other data, at events promoted by Integer;
- In the case of sensitive data, it will be processed in a limited manner and only when provided for in the legislation and for the purposes provided for therein;
- Data subjects establish contact via electronic communication, telephone or the website;

- When data subjects access our website, very limited and reduced cookies may be registered, which do not require consent.

4.9 How do we comply with transparency obligations?

Whenever we collect personal data, we provide the following information:

- Identity and contact details of the data controller;
- The purposes and grounds for processing;
- The recipients or categories of recipients;
- Whether there will be any transfer to third countries and the respective conditions;
- The period or criteria used to determine the retention period;
- The rights of the data subjects referred to above;
- Whether the communication of data constitutes a legal or contractual obligation or a necessary requirement for entering into a contract;
- Whether the data subject is obliged to provide the data and the possible consequences of not providing it;
- The existence of automated decisions, including profiling, the underlying logic, the significance and the consequences of such processing.

4.10 Who processes personal data?

As a rule, data is processed exclusively by Integer, which applies the appropriate and necessary technical and organisational measures to carry out the processing in accordance with the law, applying appropriate policies for the protection of personal data.

It may happen that the data is processed by Integer in conjunction with other entities, in which case both are responsible for the processing, or other entities process the data on behalf of Integer. In this case, Integer will enter into a contract with the other entities involved in the processing, whether they are joint controllers or subcontractors, setting out the conditions, responsibilities and obligations of each entity in the processing of data in order to ensure compliance with legal obligations and the rights of data subjects.

Integer enters into confidentiality and personal data protection agreements with all persons or entities that have contact with information about or process personal data.

4.11 How long do we keep the data?

Personal data will be kept for as long as necessary to fulfil the purposes of data processing, plus the legally established period for archiving the documents in which the data is recorded.

4.12 What are the security measures for personal data?

Integer adopts technical and organisational measures for the security of personal data in accordance with the following standards:

- The recommendations for the physical and electronic security of personal data published by the National Data Protection Commission;
- The requirements and reference controls for information security, including personal data, provided for in the Information Security Management System in accordance with ISO 27001;
- With regard to cybersecurity, in accordance with the National Cybersecurity Framework published by the National Cybersecurity Centre;
- The provisions on processing security in the General Personal Data Protection Regulation, Article 32, as appropriate:
  - Pseudonymisation and encryption of personal data;
  - The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

4.13 What do we do in the event of a personal data breach?

If an incident occurs accidentally or unlawfully that causes the destruction, loss, alteration, disclosure or unauthorised access to personal data:

- We will notify the supervisory authority CNPD if the data breach is likely to result in a risk to the rights, freedoms and guarantees of natural persons;
- We will document any personal data breaches, including the facts, effects and remedial measures;
- We will communicate to data subjects if the breach is likely to result in a high risk to the rights, freedoms and guarantees of natural persons.

4.14 When do we carry out data protection impact assessments and prior consultations?

If we carry out processing operations that are likely to pose a high risk to the rights and freedoms of natural persons, namely those provided for in the CNPD list, we will carry out an impact assessment of these processing operations before carrying them out. If the impact assessment indicates a high risk in the absence of measures taken, the supervisory authority will be consulted before proceeding with the processing.

4.15 How will we transfer personal data to third countries (outside the EU)?

We will only transfer personal data outside the EU if one of the following conditions is met:

- There is an adequacy decision by the European Commission;
- The transfers are subject to appropriate safeguards;
- There are binding rules applicable to companies;
- They fall within the conditions of specific derogations.

You can obtain further clarification by contacting us.

5. Related Documents

Information Security Policy
Risk Management Procedure
Security Incident Management Procedure
Access Management Policy
Privacy Impact Assessment Procedure
Acceptable Use Policy

6. Reference Documents

ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection Information security management systems
ISO 9001:2015 - Quality management systems-Requirements
ISO/IEC 27701:2019 - Security techniques
Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR - General Data Protection Regulation);

Law No. 58/2019 of 8 August - Law implementing the GDPR in Portugal;
Decree-Law No. 109-E/2021, of 9 December - General Regime for the Prevention of Corruption (RGPC);
Guides and recommendations from the National Data Protection Commission (CNPD);
National Cybersecurity Reference Framework (CNCS) - applicable whenever digital security and data processing are involved.

7. Definitions and Acronyms

Personal data: Any information relating to an identified or identifiable natural person.
Sensitive data: Special category of personal data that includes, for example, health data, sexual orientation or religious beliefs.
Data processing: Any operation performed on personal data, such as collection, recording, organisation, storage, alteration, consultation, use, communication or erasure.
Data subject: Natural person to whom the personal data relates.
Data controller: Entity that determines the purposes and means of personal data processing.
Processor: External entity that processes data on behalf of the controller.
PIA (*Privacy Impact Assessment*): Assessment of the impact on privacy.
CNPD: National Data Protection Commission.

8. Review and Validation

This policy is reviewed annually or whenever there is a relevant change in the legal, regulatory, normative or contractual framework. Responsibility for its review lies with the IMS team, with validation by Senior Management.

The recording of versions, changes and approvals is ensured through the document control established in INTEGER's Integrated Management System.

9. Conclusion

INTEGER is committed to a culture of respect for privacy and personal data protection, adopting appropriate measures to ensure its security and compliance with the applicable legal and regulatory framework. Compliance with this policy is mandatory and will be subject to periodic monitoring. Violation of this policy may result in corrective or disciplinary measures, in accordance with the organisation's internal regulations.