

# DATA PROTECTION POLICY



<b>i Introduction .....</b>	<b>3</b>
<b>ii Scope of application .....</b>	<b>3</b>
<b>iii Principles of processing .....</b>	<b>4</b>
<b>iv Rights of the Data Subject .....</b>	<b>6</b>
<b>v Security Risk Analysis and Management .....</b>	<b>7</b>
<b>vi Data protection impact assessment .....</b>	<b>8</b>
<b>vii Commissioning processing .....</b>	<b>8</b>
<b>viii Security Incidents .....</b>	<b>9</b>
<b>ix Person in charge of Data Protection .....</b>	<b>9</b>
<b>x Entry into force, control and compliance .....</b>	<b>10</b>

## i Introduction

---

At Gestamp Group we are committed to the protection of personal data.

We want to transmit security to our employees, customers, suppliers, trade partners and to society as a whole, so that they see us as a company that is worth trusting.

For this reason, we comply with prevailing personal data protection legislation and we adopt the necessary technical and organisational measures to ensure the security of personal data and prevent their unauthorised alteration, loss, processing or access, taking into account the state of technology, the nature of the stored data, and the risks to which they are exposed.

Accordingly, the Data Protection Policy is part of our commitment to the protection of the fundamental rights and freedoms of natural persons and, in particular, their right to personal data protection.

The Data Protection Policy becomes the focal point of our commitment in this area, but does not constitute comprehensive regulation. The companies of the Gestamp Group rely on a series of additional rules, instructions and procedures for the purposes of a more detailed application of the guarantees and principles set forth in this Data Protection Policy.

## ii Scope of application

---

The Data Protection Policy affects all the employees and is applicable to all the personal data processing activity undertaken by the companies of the Gestamp Group, either performed under its own responsibility as the controller, or on behalf of third parties processed pursuant to the provision of services in its capacity as the processor.

Additionally, the Data Protection Policy is applicable to all the resources supporting said processing activities, at all levels of the organisation.

For the purposes of this Data Protection Policy:

- «**personal data**» means any information relating to an identified or identifiable natural person (the «**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 on-line identifier or to one or more factors specific

to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

- «**processing**» means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- «**controller**» means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. For the purposes of this Data Protection Policy, generally it will be such company of the Gestamp Group collecting personal data of the data subject, and;
- «**processor**» means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. For the purposes of this Data Protection Policy, it might be a third party or a company of the Gestamp Group providing corporate and/or divisional services to the controller.

### iii Principles of processing

---

All the personal data processing activity undertaken by the companies of the Gestamp Group, at all levels of its organisation, either performed under its own responsibility as the controller, or on behalf of third parties processed pursuant to the provision of services in its capacity as the processor, must follow a specific procedure that ensures the respect and compliance of the guarantees and principles established in this Data Protection Policy, and more specifically:

- **Lawfulness of processing**. The processing of personal data shall be lawful when the data subject has given their consent, when it is necessary for the performance of a contract to which the data subject is party, when it is necessary for compliance with a legal obligation, or when it is necessary for the purposes of carrying out the activities or achieving the legitimate objectives of the companies of the Gestamp Group.
- **Purpose limitation**. Personal data shall be collected for specified, explicit and legitimate purposes. The purposes for which personal data can be processed shall be limited as much as possible.

- **Data Minimisation**. The quantity and type of personal data collected and processed shall be limited to what is necessary in relation to the purposes for which they are processed.
- **Accuracy of the Data**. Personal data shall be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- **Storage Limitation**. The storage of personal data shall be limited to the minimum necessary, so that they will be only retained as long as is required for the purpose for which it was collected. When its preservation is no longer required, the companies of the Gestamp Group will keep blocked such personal data which might be necessary during the period required by law to attend any questions regarding its processing. Once this period has elapsed, the personal data will be erased adopting the appropriate security measures to ensure its complete erasure.
- **Integrity and Confidentiality**. Personal data shall be 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. Access to the data for processing purposes shall be limited as much as possible, so that the personal data is not accessible to an indeterminate number of persons.
- **Accountability**. The Companies of the Gestamp Group shall be in a position to prove compliance of data protection rules, so that there will always be sufficient proof or evidence so as to be able to show said compliance.
- **Privacy by design and by default**. The companies of the Gestamp Group shall implement appropriate technical and organisational measures for ensuring that, by design and by default, there is effective application of the processing principles, and measures that ensure the security of the data, in order to comply with the requirements of data protection rules and protect the rights of the data subjects.
- **Records of processing activities**. The companies of the Gestamp Group shall keep and maintain updated Records of Processing Activities with the information relative to all the personal data processing activities undertaken by the company, at all levels of its organisation, either performed under its own responsibility as the controller, or on behalf of third parties processed pursuant to the provision of services in its capacity as the processor. For that purpose the companies of the Gestamp Group shall appoint at least one person in charge of preparing and maintaining updated its Records of Processing Activities.

- **International data transfer**. All personal data processing that entails the transfer of data, can only be carried out when said transfer provides adequate guarantees in accordance with the applicable regulations.

## iv Rights of the Data Subject

---

The companies of the Gestamp Group shall comply with the obligation to duly deal with requests to exercise rights put forth by the data subjects whose personal data it has under its responsibility, guaranteeing the data subject the following rights:

- **Access**: The right of the data subject to know what data is being processed, the purpose of the processing, as well as the origin of said data, the data already disclosed or that which will be disclosed, and the envisaged period for which the personal data will be stored or the criteria used to determine that period.
- **Rectification**: The right of the data subject to modify the data that is inaccurate or incomplete.
- **Erasure**: The right to erase the data that is unnecessary, inadequate or excessive for the purposes of processing, as well as when the data subject withdraws its consent or objects to its processing, its processing is unlawful or there exists a legal obligation, notwithstanding the blocking obligation.
- **Blocking**: Identification and reservation of the personal data with the purpose of preventing its processing, except for making the same available to the Public Administrations, Judges and Courts, to attend to potential liabilities derived from their processing, and solely within the statute of limitations applicable to said liabilities. Once this period has elapsed, it must proceed with the erasure of the data.
- **Restriction**: The right to restrict or block all processing where one of the following applies:
  - a) The accuracy of the data is contested by the data subject. During the period enabling the controller to verify the accuracy of the data and, where applicable, correct the same.
  - b) Unlawful processing of data. When the data subject opposes erasure of the data and requests the restriction of their use.
  - c) When the data may be eliminated because they are no longer necessary for the purposes of the processing, but they are required by the data subject for the filing of a claim.

d) When the data subject has objected to processing, pending the verification whether the legitimate grounds of the controller override those of the data subject.

- **Portability:** The data subject shall have the right to receive a copy of the data provided to the controller, in a commonly used and machine-readable format, and have the right to transmit those data to another controller.
- **Objection:** The right to object to a specific processing of the personal data, or that processing thereof cease.

These rights are personal, and can solely be exercised by their legitimate titleholders or their legal or voluntary representatives, always providing documentation proving their condition. Consequently, they must be refused if said documentation is not provided.

These rights are independent, so that none of them are a prior requirement for the exercising of the other.

The companies of the Gestamp Group shall provide a simple and free of charge procedure for the exercising of these rights.

The companies of the Gestamp Group shall attend requests even in those situations in which the established procedure has not been used, provided that the data subject has used a medium that serves to certify the filing and receipt of the request.

## v Security Risk Analysis and Management

---

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the companies of the Gestamp Group shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

Said security measures shall ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, as well as the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

Likewise, these security measures shall be subject to a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

## **vi Data protection impact assessment**

---

The Impact Assessment shall consist of an analysis of the viability and the risks of a new data processing project that may result in a high risk to the privacy of the data subjects. This Impact Assessment must always be undertaken prior to the development of the project, so as to be able to influence in the initial conception.

Said situation may arise as a result of the use of new technology, due to the large amount of data collected in relation with one person, or due to the large number of persons affected.

This analysis must contain, at the very least:

- The systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
- The assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- The assessment of the risks to the rights and freedoms of data subjects; and
- The measures envisaged to address the risks, including the security measures and mechanisms to ensure the protection of personal data.

In the event that the result of the Impact Assessment and the measures adopted do not considerably reduce the risk to the data protection of the data subjects, a prior consultation must be made with the competent authority, whose criterion shall be complied with and respected in any case.

## **vii Commissioning processing**

---

When the companies of the Gestamp Group undertake the contracting of services that implies the processing by third parties of personal data for which it is the controller, it shall ensure that said processor complies with the obligations of data protection rules.

In any case, an agreement must be signed with the processor that shall regulate access to the data for which the companies of the Gestamp Group are the controller, in accordance with that established in data protection rules.



These obligations shall also be applicable when a company of the Gestamp Group acting as processor provides corporate and/or divisional services to other companies of the Gestamp Group that are the controllers.

## **viii Security Incidents**

---

In the event of a personal data breach, the controller shall immediately inform Gestamp Servicios, S.A., by sending an e-mail to [dataprotection@gestamp.com](mailto:dataprotection@gestamp.com) and following the procedure for communication of security incidents. If required by the applicable regulation in the relevant territory, controller and Gestamp Servicios, S.A., shall jointly notify the competent supervisory authority of its existence, without undue delay within the period established by the applicable regulation, unless it is improbable that said breach constitutes a risk to the rights and freedoms of natural persons.

When it is probable that the personal data breach entails a high risk to the rights and freedoms of natural persons, and if required by the applicable regulation in the relevant territory, the controller and Gestamp Servicios, S.A., shall also jointly notify the data subject of its existence, without undue delay.

The controller must manage, resolve, record and document any incident that may affect the security of the personal data for which it is the controller, including the facts related thereto, their effects and the corrective measures adopted, so that the weakest aspects of the security of the companies of the Gestamp Group may be periodically assessed, and the appropriate measures adopted to reinforce said aspects.

## **ix Person in charge of Data Protection**

---

Each of the companies of the Gestamp Group shall appoint at least one person in charge of ensuring the respect and compliance of the guarantees and principles established in this Data Protection Policy, between others, to prepare and to maintain updated its Records of Processing Activities, to duly deal with requests to exercise rights put forth by the data subjects whose personal data it has under its responsibility, to carry out impact assessments, or to notify and to manage security incidents. Those persons in charge shall act as contact persons between the companies of the Gestamp Group for Data Protection issues.

If required by the applicable regulation in the relevant territory, the companies of the Gestamp Group shall appoint a Data Protection Officer or an analogous officer required by such regulation.

## **x Entry into force, control and compliance**

---

This Data Protection Policy enters into force on 25 May 2018, and shall be revised and where applicable adapted to the requirements of the prevailing legislation.

Gestamp Servicios, S.A., shall control the respect and compliance of the guarantees and principles established in this Data Protection Policy by the companies of the Gestamp Group.