Data Protection Policy

HOISTGROUP
hospitality innovations.

Contents

Version Control

Version	Date	Author	Notes
0.1	07/11/18	Åsa Holmlund	First Draft
0.2	6/12/18	Rachel Mariner and Åsa Holmlund	Second Draft
0.3	1/1/19	Rachel Mariner/ Åsa Holmlund	Published

Introduction

Policy Statement

The Board of Directors and management of Hoist Group, with Main office located at Vretenvägen 8, Solna, Sweden are committed to compliance with all relevant EU and Member State laws in respect of personal data, and the protection of the rights and freedoms of individuals whose information Hoist Group collects and processes in accordance with the General Data Protection Regulation (GDPR).

Compliance with the GDPR is described by this policy along with connected processes and procedures.

The GDPR and this policy apply to all of Hoist Group's personal data processing functions, including those performed on hotel guests', customers', employees', suppliers' and partners' personal data, and any other personal data the organisation processes from any source. Hoist Group functions in the hospitality sector and guests of our hotel clients entrust their personal data to our products.

Hoist Group aims for, and works toward, full and fair compliance with all data protection legislation

Any breach of the GDPR will be dealt with under Hoist Group's disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

Objectives

This policy is intended to integrate the principles of data protection into the operations, products and people of Hoist Group This policy is mandatory and by accessing any of the Hoist´s information/data, users are agreeing to abide by the terms of this policy

Scope

This policy is addressed to all employees and the management, suppliers, customers, hotel guests, subcontractors, resellers within Hoist Group. Hoist Group (Hoist) is legally required under the REGULATION (EU) 2016/679 to ensure the security and confidentiality of the information/data it processes on behalf of its customers and employees.

Responsibility

The Data Protection Officer (DPO) is responsible for annual review of Hoist Group's data practices and compliance in the light of any changes to Hoist Group's activities and to any additional requirements identified by means of data protection impact assessments.

The DPO is also responsible for maintaining and updating this policy.

This Policy Statement has been adopted by Hoist Group's Data Protection Officer and its board.

General provisions

Subject matter and objectives

1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

Material scope – the GDPR applies to the processing of personal data wholly or partly by automated and to the processing other than by automated means of personal data that form part of a filing system or are intended to form part of a filing system. (Article 2)

Territorial scope – the GDPR will apply to all controllers that are established in the EU (European Union) who process the personal data of data subjects, in the context of that establishment. It will also apply to controllers outside of the EU that process personal data in order to offer goods and services, or monitor the behavior of data subjects who are resident in the EU. (Article 3)

1. Responsibilities and roles under the General Data Protection Regulation

1.1 Hoist Group is sometimes data controller and sometimes data processor under the GDPR.

1.2 Top Management and all those in managerial or supervisory roles throughout Hoist Group are responsible for developing and encouraging good information handling practices within Hoist Group.

1.3 The DPO should be a member of the senior management team, is accountable to Board of Directors of Hoist Group for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes:
- 1.3.1 development and implementation of the GDPR as required by this policy; and
- 1.3.2 Security and risk management in relation to compliance with the policy.

1.4 The DPO and the local GDPR Representative has been appointed to take responsibility for Hoist Group's compliance with this policy on a day-to-day basis and have responsibility for ensuring that Hoist Group complies with the GDPR, as do other manager's in respect of data processing that takes place within their area of responsibility.

1.5 The local GDRP Representative have specific responsibilities in respect of procedures for local Subject Access Request Procedure and are the first point of call for Employees/Staff seeking clarification on any aspect of data protection compliance.

1.6 Compliance with data protection legislation is the responsibility of all Employees/Staff of Hoist Group who process personal data.

1.7 Hoist Group's GDPR Training Policy sets out specific training and awareness requirements in relation to specific roles and Employees/Staff of Hoist Group generally.

1.8 Employees/Staff of Hoist Group are responsible for ensuring that any personal data about them and supplied by them to Hoist Group is accurate and up-to-date.

2. Data protection principles

All processing of personal data must be conducted in accordance with the data protection principles. Hoist Group's policies and procedures are designed to ensure compliance with the principles in GDPR Article 5

2.1 Personal data must be processed lawfully, fairly and transparently

2.2 Personal data can only be collected for specific, explicit and legitimate purposes

2.3 Personal data must be adequate, relevant and limited to what is necessary for processing

2.4 Personal data must be accurate and kept up to date with every effort to erase or rectify without delay

2.5 Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.

2.6 Personal data must be processed in a manner that ensures the appropriate security

2.7 The controller must be able to demonstrate compliance with the GDPR's other principles (accountability)

3. Data subjects' rights (article 13-22)

3.1 Data subjects have the following rights regarding data processing, and the data that is recorded about them:

3.1.1 The right to be informed

3.1.2 The right of access
3.1.3 The right to rectification
3.1.4 The right to erasure
3.1.5 The right to restrict processing
3.1.6 Notification obligation regarding rectification or erasure of personal data or restriction of processing
3.1.7 The right to data portability
3.1.8 The right to object
3.1.9 Rights in relation to automated decision making and profiling

3.2 Hoist Group ensures that data subjects may exercise these rights:

3.2.1 Data subjects may make subject data access requests (SAR). Hoist Group will ensure that its response to the SAR complies with the requirements of the GDPR.

3.2.2 Data subjects have the right to complain to Hoist Group related to the processing of their personal data and the handling of a request

4. Consent

4.1 Hoist Group understands 'consent' to mean that it has been explicitly and freely given. The data subject can withdraw their consent at any time.

4.2 Hoist Group understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.

4.3 There must be some active communication between the parties to demonstrate active consent. Consent cannot be inferred from non-response to a communication. The Controller must be able to demonstrate that consent was obtained for the processing operation.

4.4 For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

4.5 Hoist Group chooses to rely on legal bases of processing other than consent wherever possible.

5. Security of data

5.1 All Employees/Staff are responsible for ensuring that any personal data that Hoist Group holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by Hoist Group to receive that information and has entered into a confidentiality agreement.

5.2 All personal data should be accessible only to those who need to use it, and access may only be granted in line with the IT Policy.

5.3 Care must be taken to ensure that PC screens and terminals are not visible except to authorised Employees/Staff of Hoist Group.

5.4 Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit authorisation.

6. Disclosure of data

6.1 Hoist Group must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All Employees/Staff should exercise caution when asked to disclose personal data held on another individual to a third party It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of Hoist Group's business.

6.2 All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the GDPR Owner.

7. Retention and disposal of data

7.1 Hoist Group shall not keep personal data in a form that permits identification of data subjects for longer a period than is necessary, in relation to the purpose(s) for which the data was originally collected.

7.2 Hoist Group may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

7.3 The retention period for each category of personal data will be set out along with the criteria used to determine this period including any statutory obligations Hoist Group has to retain the data.

7.4 Hoist Group's data retention and data disposal procedures will apply in all cases. Personal data must be disposed of securely in accordance with the sixth principle of the GDPR – processed in an appropriate manner to maintain security, thereby protecting the "rights and freedoms" of data subjects. Any disposal of data will be done in accordance with the disposal procedure.

8. Data transfers

8.1 All exports of data from within the European Economic Area (EEA) to non-European Economic Area countries (referred to in the GDPR as 'third countries') are unlawful unless there is an appropriate "level of protection for the fundamental rights of the data subjects".

The transfer of personal data outside of the EEA is prohibited unless one or more of the specified safeguards, or exceptions, apply:

8.2 An adequacy decision

The European Commission can and does assess third countries, a territory and/or specific sectors within third countries to assess whether there is an appropriate level of protection for the rights and freedoms of natural persons. In these instances no authorisation is required.

Countries that are members of the European Economic Area (EEA) but not of the EU are accepted as having met he conditions for an adequacy decision.

A list of countries that currently satisfy the adequacy requirements of the Commission are published in the Official Journal of the European Union.

Assesment of adequacy by the data controller

In making an assessment of adequacy, the exporting controller should take into account the following factors:

- the nature of the information being transferred;
- the country or territory of the origin, and final destination, of the information;
- how the information will be used and for how long;
- the laws and practices of the country of the transferee, including relevant codes of practice and international obligations; and
- the security measures that are to be taken as regards the data in the overseas location.

9. Information asset register/data inventory

9.1 Hoist Group is aware of any risks associated with the processing of particular types of personal data.

9.1.1 Hoist Group assesses the level of risk to individuals associated with the processing of their personal data. Data protection impact assessments (DPIAs) will be carried out from time to time in relation to the processing of personal data by Hoist Group, and in relation to processing undertaken by other organisations on behalf of Hoist Group.

9.1.2 Hoist Group shall manage any risks identified by the risk assessment in order to reduce the likelihood of a non-conformance with this policy.

9.1.3 Where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, Hoist Group shall, prior to the processing, carry out a DPIA of the impact of the envisaged processing operations on the protection of personal data.

9.1.4 Where, as a result of a DPIA it is clear that Hoist Group is about to commence processing of personal data that could cause damage and/or distress to the data subjects, the decision as to whether or not Hoist Group may proceed must be escalated for review to the DPO.

9.1.5 The DPO shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned,escalate the matter to the supervisory authority.

9.1.6 Appropriate controls will be selected and applied to reduce the level of risk associated with processing individual data to an acceptable level, by reference to the requirements of the GDPR.

10. Breach Management

10.1 The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant parties will be informed. All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of Hoist becoming aware of it.

10.2 Effective and robust breach detection, investigation and internal reporting procedures are in place at Hoist Group
Within a breach notification, the following information will be outlined:
- The nature of the personal data breach,
- The name and contact details of the DPO
- An explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects

10.3 Hoist Group will, when data processor, co-operate with the data controller take such reasonable commercial steps as are directed by the data controller to assist in the investigation, mitigation and remediation of each such incident.

10.4 Hoist Group maintains Breach Management policies and procedures.

11. Subject Access Request (SAR)

Any individual have the right to be informed by Hoist Group whether or not it is processing personal data that relates to them and, if so, to be told

11.1 What personal data it is being processed.
11.2 The purposes for which the personal data is being processed.
11.3 Who, if anyone, the personal data is disclosed to.
11.4 The extent to which it is using the personal data for the purpose of making automated decisions relating to the data subject and, if so, what logic is being used for that purpose.

The request can be made verbally or in writing and will be answered within 30 days, provided the identity of the requestor has been ascertained.

12. Definitions (Article 4)

personal data means any 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;

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;

restriction of processing means the marking of stored personal data with the aim of limiting their processing in the future;

profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural persons performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

filing system means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

controller means entity that determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

recipient [1] means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not;

third party means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subjects 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;

personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

establishment

a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;

b) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;

representative means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation;

enterprise means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;

group of undertakings means a controlling undertaking and its controlled undertakings;

binding corporate rules means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;

supervisory authority means an independent public authority which is established by a Member State pursuant to Article 51;

supervisory authority concerned means a supervisory authority which is concerned by the processing of personal data because:

a) the controller or processor is established on the territory of the Member State of that supervisory authority;

b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or

1. a complaint has been lodged with that supervisory authority;
2. cross-border processing means either:
3. processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or

4. processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

relevant and reasoned objection means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union;

information society service means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council ([1]);

international organisation means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

[1] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p. 1).

References

https://gdpr-info.eu

https://ec.europa.eu/commission/index_en

Breach Management Policy

Contact the DPO