Data Protection Policy

This document is intended for internal use only. Copying and dissemination of this document in whole or in part and in any manner whatsoever is prohibited unless prior authorization of the owner of the document is provided.

Revision history

Date	Rev. No.	Description of Revision	Revision Author	Approved by
25.05.2018	0	New document	Name Surname	Name Surname

Summary

This document describes the policy for the protection of personal data, including special categories of personal data, data on criminal convictions/offences and compliance with the current regulatory requirements.

Scope

All group companies, employees, and contractors, including data processors and third parties.

Related Documents

Data Retention and Disposal Policy

Data Subject Requests Handling Process

Data Protection by Design and Impact Assessment Methodology

Personal Data Breach Handling Process

This document is intended for internal use only. Copying and dissemination of this document in whole or in part and in any manner whatsoever is prohibited unless prior authorization of the owner of the document is provided.

Contents

This document is intended for internal use only. Copying and dissemination of this document in whole or in part and in any manner whatsoever is prohibited unless prior authorization of the owner of the document is provided.

Definitions

For the implementation of this policy the below terms must be clarified:

Personal data means any information which relate to a living individual who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, online identifiers or one or more factors specific to the physical, physiological, economic, cultural or social identity of that living individual.

Special categories of personal data means personal data consisting of information as to (a) the racial or ethnic origin of the data subject, (b) his/her political opinions, (c) his/her religious beliefs or other beliefs of a similar nature, (d) whether he/she is a member of a trade union, (e) his/her physical or mental health or condition, (f) his/her sexual life, (g) the commission or alleged commission by him/her of any offence, or (h) any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any court in such proceedings.

Data Processing, in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including (a) organization, adaptation or alteration of the information or data, (b) retrieval, consultation or use of the information or data, (c) disclosure of the information or data by transmission, dissemination or otherwise making available, or (d) alignment, combination, blocking, erasure or destruction of the information or data.

Data subject means an individual who is the subject of personal data.

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

Data processor, in relation to personal data, means any person (natural or legal other than the data controller) who processes the data on behalf of the data controller.

Third party, in relation to personal data, means any person other than – (a) the data subject, (b) the data controller, or (c) any data processor or other person authorized to process data for the data controller or processor.

This document is intended for internal use only. Copying and dissemination of this document in whole or in part and in any manner whatsoever is prohibited unless prior authorization of the owner of the document is provided.

Data Protection Principles

We ensure full compliance with the applicable Data Protection Legal Framework, including the General Data Protection Regulation (GDPR) and process personal data in accordance with the applicable main principles. In this context, we ensure that personal data is:

a) **Processed lawfully, fairly and in a transparent manner in relation to individuals;**

The lawful bases for processing are described below. We ensure that one of these applies whenever we process personal data:

- **Consent**: the individual has provided clear and unambiguous consent, allowing us to process their personal data for a specific purpose.
- **Contract**: the processing is necessary for a contract between us and the individual, or because we have been asked to take specific steps before entering into a contract.
- **Legal obligation**: the processing is necessary for us to comply with the law (not including contractual obligations).
- **Vital interests**: the processing is necessary to protect someone's life or other vital interests.
- **Public Interest**: the processing is necessary in order to perform a task in the public interest.
- **Legitimate interests**: the processing is necessary in order to pursue our legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

b) **Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;** further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) **Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;** Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed. Specifically for retention periods please see Data Retention and Disposal Policy.

d) **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;

e) **Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;** personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organizational measures required by the applicable data protection framework, in order to safeguard the rights and freedoms of individuals;

This document is intended for internal use only. Copying and dissemination of this document in whole or in part and in any manner whatsoever is prohibited unless prior authorization of the owner of the document is provided.

f) **Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.** Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data; and

g) **Personal data shall not be transferred to a country or territory outside the European Economic Area** unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Special categories of personal data

Processing Special Categories of Personal Data

Special Categories of Personal Data, as described in the above definitions, could create more significant risks to a person's fundamental rights and freedoms, if not lawfully processed and/or inadequately protected. For instance, unauthorised use of such data could result to a risk of unlawful discrimination. There are certain conditions that have to be fulfilled in order for processing of special categories of personal data to be allowed, for example:

a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes;

b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of Frigoglass in the field of employment and social security and social protection law, so far as it is authorized by law or collective agreement, which also provides for appropriate safeguards;

c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

d) processing relates to personal data which are manifestly made public by the data subject;

e) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

f) processing is necessary for reasons of substantial public interest;

g) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment;

h) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices;

This document is intended for internal use only. Copying and dissemination of this document in whole or in part and in any manner whatsoever is prohibited unless prior authorization of the owner of the document is provided.

Criminal offence data

Processing of personal data relating to criminal convictions and offences or related security measures shall be carried out only under the control of official authority or when the processing is properly authorized by law, providing for appropriate safeguards for the rights and freedoms of data subjects.

Children

Children need particular protection when collecting and processing their personal data because they may be less aware of the risks involved. Compliance with the data protection principles and in particular fairness should be central to all processing of children's personal data.

Children have the same rights as adults over their personal data. These include the rights to access their personal data; request rectification; object to processing and have their personal data erased.

An individual's right to erasure is particularly relevant if they gave their consent to processing when they were a child.

When Frigoglass processes personal data of children based on consent, it must be ensured that either (a) children who provide their consent are at least 16 years old or (b) consent is given or authorised by the holder of parental responsibility.

Individual rights

Data Subject Rights	
Right to be informed	The Data Subject has the right to be informed about the collection and use of their personal data.
Right of Access	The Data Subject has the right to obtain from the controller confirmation as to whether or not Personal Data concerning him are being processed, and, where that is the case, access to the Personal Data in a concise, intelligible, transparent, and easily accessible form.
Right to Rectification	The Data Subject may request, and Frigoglass will ensure that without undue delay it will proceed to rectification of inaccurate or incomplete Personal Data, including by means of providing supplementary statement.
Right to Erasure	The Data Subject has the right to request by Frigoglass the erasure of Personal Data concerning him or her, without undue delay and Frigoglass shall comply, subject to the conditions set by law.
Right to Restriction	The Data Subject shall have the right to request Frigoglass to restrict its processing activities only to specific purposes, subject to the conditions set by law.
Right to Object	The Data Subject shall have the right to object on grounds relating to his or her particular situation, at any time to processing of Personal Data concerning him

This document is intended for internal use only. Copying and dissemination of this document in whole or in part and in any manner whatsoever is prohibited unless prior authorization of the owner of the document is provided.

	or her. Frigoglass shall then no longer process the Personal Data unless the controller demonstrates compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the Data Subject or for the establishment, exercise or defense of legal claims.
Right to Portability	The Data Subject shall have the right to receive the Personal Data concerning him or her, which he or she has provided to Frigoglass, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from Frigoglass.
Right to Obtain Human Intervention	The Data Subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

Frigoglass respects the above rights and facilitates the Data Subjects to exercise them, by submitting relevant requests. For details on handling data subjects requests please see **Data Subject Requests Handling Process**.

Accountability and governance

In line with the principle of accountability, Frigoglass has adopted policies and measures in order to achieve compliance with all applicable data protection obligations, but also to ensure that compliance can be adequately demonstrated. To this end, Frigoglass:

- Implements appropriate technical and organizational measures to ensure and demonstrate compliance.
- Has adopted and implemented a Data Protection Framework, including this Data Protection Policy, Processes on handling Data Subject Requests and managing any actual or suspected Data Breaches, Information Security Policies, staff training, internal audits of processing activities, and regular reviews of internal policies and procedures that include processing of personal data;
- Maintains relevant documentation on processing activities in an organized and continuously updated Record of Processing Activities;
- Has appointed a Data Protection Officer;
- Implements measures and policies that meet the principles of data protection by design and data protection by default;
- Ensures data minimization and where appropriate applies measures such as pseudonymisation or encryption, creating and improving security features on an ongoing basis.
- Performs Data Protection Impact Assessments where appropriate.

This document is intended for internal use only. Copying and dissemination of this document in whole or in part and in any manner whatsoever is prohibited unless prior authorization of the owner of the document is provided.

Contracts

Any third party acting as a personal data Processor is required to execute a written contract with Frigoglass. The contract is important so that both parties understand their responsibilities and liabilities. Frigoglass, when acting as a personal data Controller, is liable for its compliance with the applicable personal data protection legal framework and must only appoint processors who can provide 'sufficient guarantees' that the requirements of the applicable legal framework will be met and the rights of data subjects protected. Using a processor which adheres to an approved code of conduct or certification scheme may help in the future to satisfy this requirement – though currently, no such schemes are available to certify compliance with Data Protection Legal Framework (e.g. GDPR compliance). However, certificates verifying compliance with specific technical or information security requirements will be taken into account and are important for the assessment of a Processor's organisational and technical measures aiming to ensure security of personal data they process.

Processors must only act on the documented instructions of Frigoglass. However, they remain directly responsible towards authorities for a series of obligations and may be subject to fines or other sanctions if they don't comply.

International transfers

The applicable personal data protection legal framework imposes restrictions on the transfer of personal data outside the European Economic Area (E.E.A.), to third countries or international organisations. These restrictions are in place to ensure that the level of protection of individuals afforded by the European and local framework is not undermined. Personal data may be transferred outside the E.E.A., where the organisation receiving the personal data has provided adequate safeguards. Individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer.

When a processing activity or agreement with a third party includes transfer of personal data, the business owner shall seek advice on such transfers and on the required safeguards by the Data Protection Officer of Frigoglass.

Data protection by design and default

Data Protection by Design means that any action Frigoglass undertakes that involves processing of personal data must be done with data protection and privacy in mind at every step. This includes internal projects, product development, software development, IT systems, and much more. In practice, this means that the IT department, or any department that processes personal data, must ensure that privacy is built in to a system during the whole life cycle of the system or process.

For details on how Data Protection by Design is implemented by Frigoglass please see Data Protection by Design and Impact Assessment Methodology.

Data Protection by Default means that once a product or service has been released, the strictest privacy settings should apply by default, without any manual input from the end user. In addition, any personal data provided by the user to enable a product's optimal use should only be kept for the amount

This document is intended for internal use only. Copying and dissemination of this document in whole or in part and in any manner whatsoever is prohibited unless prior authorization of the owner of the document is provided.

of time necessary to provide the product or service. If more information than necessary to provide the service is disclosed, then "privacy by default" has been breached.

Under the GDPR, there is a general obligation to implement technical and organisational measures to show that data protection has been considered and integrated into every processing activity.

Data protection impact assessments (DPIA)

A Data Protection Impact Assessment (DPIA) is a process to help Frigoglass identify and minimise the data protection risks of a project. A DPIA must be performed for certain listed types of processing, or any other processing that is likely to result in a high risk to individuals' rights and freedoms. The Data Protection Officer should always be consulted in order to assess likely impact and level of risk involved in new or modified personal data processing activities.

As a good practice, Frigoglass may also choose to perform a DPIA for any major project which requires the processing of personal data.

The DPIA shall be properly documented and carried out with the assistance of the Data Protection Officer (DPO). Where the DPIA's results indicate that there is a high residual risk for data subjects, the supervisory authority must be notified and its view on adequate measures to reduce the risks must be obtained.

For details on performing DPIA please see Data Protection by Design and Impact Assessment Methodology.

Personal data breaches

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. This includes incidents that are the result of both accidental and deliberate actions or omissions. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or unlawfully disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

If the data breach may result to a risk for the rights and freedoms of data subjects, Frigoglass shall report it to the relevant supervisory authority **within 72 hours of becoming aware** of the breach, where feasible. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, those individuals must also be informed without undue delay. A record of any personal data breaches reported is maintained by Frigoglass, regardless of whether notification to the DPA and/or to data subjects was eventually required.

Details on handing data breaches are available in Personal Data Breach Handling Process.

Data Privacy Organization

For successfully protecting individual's data, additional roles and responsibilities must be defined. The roles and their responsibilities are described below.

This document is intended for internal use only. Copying and dissemination of this document in whole or in part and in any manner whatsoever is prohibited unless prior authorization of the owner of the document is provided.

Data controller

The data controller, as stated previously, defines the purpose and means of processing and is responsible for the appropriate processing of personal data and compliance with data protection and data security requirements. The data controller is responsible for:

- Implementing the current policy;
- implementing appropriate technical and organizational security measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access;
- implementing "privacy by design" and "privacy by default" principles i.e. considering the above measures both in the planning phase of processing activities and the implementation phase of any new product or service;
- providing processors and sub-processors act only act on the controller's documented instructions;
- notify the supervisory authority and the data subject (if applicable) for a personal data breach according to relevant process;
- provide all the necessary means for data subjects to effectively exercise their rights; and
- conduct DPIA's along with the assistance of the data protection officer.

Data Processor

The data processor is responsible to:

- only act on the controller's documented instructions;
- impose confidentiality obligations on all personnel who process the relevant data;
- must ensure the security of the personal data that it processes;
- abide by the rules regarding appointment of sub-processors;
- implement measures to assist the controller in complying with the rights of data subjects;
- assist the controller in obtaining approval from DPAs where required;
- at the controller's election, either return or destroy the personal data at the end of the relationship (except as required by EU or Member State law); and
- provide the controller with all information necessary to demonstrate compliance with the GDPR.

Data protection officers (DPO)

The Data Protection Officer (DPO) is independent, an expert in data protection, adequately resourced, and reports to the highest management level.

This document is intended for internal use only. Copying and dissemination of this document in whole or in part and in any manner whatsoever is prohibited unless prior authorization of the owner of the document is provided.

The DPO's is responsible:

- to inform and advise Frigoglass and its employees about the obligations to comply with the applicable EU and national Data Protection Legal Framework;
- to monitor compliance with the applicable data protection legal framework, and with Frigoglass data protection polices, including managing internal data protection activities; raising awareness of data protection issues, training staff and conducting internal audits;
- to advise on, and to monitor, data protection impact assessments; to cooperate with the supervisory authority; and
- to be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc.).

When carrying out his/hers tasks the DPO is required to take into account the risk associated with the processing undertaken, the nature, scope, context and purposes of the processing. The DPO should prioritize and focus on the more risky activities, for example where special categories of personal data are being processed, or where the potential impact on individuals could be damaging.

Frigoglass ensures that the DPO:

- is involved, closely and in a timely manner, in all data protection matters; the DPO has access to the highest authority in the company, operates independently and is not dismissed or penalized for performing their tasks;
- is provided with adequate resources (sufficient time, financial, infrastructure, and, where appropriate, staff) to meet the obligations of the applicable data protection legal framework, and to maintain the necessary expert level of knowledge;
- is given appropriate access to personal data and processing activities;
- provides advice when carrying out a DPIA;

Finally, the DPO isn't personally liable for data protection compliance. As the controller or processor it remains in Frigoglass responsibility to comply with the applicable data protection legal framework. Nevertheless, the DPO clearly plays a crucial role in helping fulfilling Frigoglass data protection obligations.

Monitoring compliance

As stated above one of the DPO tasks is to monitor compliance with the applicable data protection legal framework and internal policies.

For this, **all personnel has the responsibility to notify the DPO**, **or seek advice when necessary**, for any changes or introduction of new personal data processing activities (including those performed by processors) to ensure proper evaluation and update of the Record of Processing Activities.

This document is intended for internal use only. Copying and dissemination of this document in whole or in part and in any manner whatsoever is prohibited unless prior authorization of the owner of the document is provided.

Also the following periodic tasks should be performed:

Task	Review Period
Processing activities recorded in the registry. This means that workshops with data owners and related Units should take place in order to validate current status or update when needed.	2 year
Revision of Data Protection Impact Assessments (DPIA's) performed	2-3 years or upon changed of the related processing activities
Audit compliance of third-party processors, on high risk activities	2 year
Audit compliance of third-party processors, on non-high risk activities	2-3 years
Policies, Consent forms, Privacy Notices, Procedures, Methodologies and all other relevant documentation used to comply with the GDPR requirements	2 year or upon occurrence of major changes
Perform Privacy pen-test	3 year
Perform Data Breach Response Simulation	3 year

Failure to comply with the data protection policy may result in disciplinary action up to and including dismissal. Violations of legal or regulatory obligations may be reported to external authorities, and may result in criminal, civil or regulatory penalties.

Document Revision

This document, and all documents related to this policy, is periodically reviewed and revised where appropriate by the Data Protection Officer according to Data Protection Policy.

This document is intended for internal use only. Copying and dissemination of this document in whole or in part and in any manner whatsoever is prohibited unless prior authorization of the owner of the document is provided.