Data Protection Policy

Policy Owner:	Head of Legal
Approval:	Froneri International PLC Board
Policy Audience:	All colleagues
Effective date:	29 May 2018
Next review date:	29 May 2019

1.1 Change Control

Version	Author of Change	Date	Details of Change
1.0	Chontelle Wright	25 May 2018	Creation of Policy

1.2 Record of Approvals

Approver	Date
Froneri International PLC Board	29 May 2018

2.1 Purpose and Objective

This Policy sets out how the Froneri Group handles the personal data of our customers, suppliers, employees, workers and other third parties.

Compliance with this Policy is mandatory for all Froneri Group businesses and colleagues. Related policies and guidelines as well as template documents referenced in this Policy are available from the Group Head of Legal to help you interpret and act in accordance with this Policy.

This Policy is an internal document and cannot be shared without prior authorisation from the Group Head of Legal.

We reserve the right to change this Policy at any time and the updated Policy will be published to Country Managers and made available on the Froneri intranet.

2.2 Policy Requirements

We recognise that the correct and lawful treatment of personal data will maintain confidence in Froneri and will provide for successful business operations. Protecting the confidentiality and integrity of personal data is a critical responsibility that we take seriously. Froneri is exposed to potential fines of up to **€20 million or 4% of total worldwide annual turnover**, whichever is higher and depending on the breach, for failure to comply with the provisions of the General Data Protection Regulation ((EU) 2016/679) ("**GDPR**").

All Country Managers, Heads of Finance, departments and managers are responsible for implementing appropriate practices, processes, controls and training to ensure all Froneri business and colleagues comply with this Policy.

Please contact the Group Head of Legal with any questions about the operation of this Policy or the GDPR or if you have any concerns that this Policy is not being or has not been followed.

2.2.1 Data Protection Principles

The GDPR requires us to protect personal data when we process it.

What is 'personal data'?
'Personal data' means any information identifying an individual or information relating to an individual that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal data includes Sensitive Personal Data (which is data revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and personal data relating to criminal offences and convictions) and Pseudonymised personal data (which means replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure). Personal data does not include anonymous data or data that has had the identity of an

individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.
What is data processing?
When we talk about 'processing' personal data this means any activity that involves the use of personal data, including: obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties.

We adhere to the 8 principles relating to processing personal data set out in the GDPR. The 8 principles require personal data to be:

1. Processed lawfully, fairly and in a transparent manner (**Lawfulness, Fairness and Transparency**).
2. Collected only for specified, explicit and legitimate purposes (**Purpose Limitation**).
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (**Data Minimisation**).
4. Accurate and where necessary kept up to date (**Accuracy**).
5. Not kept in a form which permits identification of individuals for longer than is necessary for the purposes for which the data is processed (**Storage Limitation**).
6. Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (**Security, Integrity and Confidentiality**).
7. Not transferred to another country without appropriate safeguards being in place (**Transfer Limitation**).
8. Made available to individuals (known as 'Data Subjects') and individuals allowed to exercise certain rights in relation to their Personal Data (**Data Subject's Rights and Requests**).

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (**Accountability**).

Further detail on what each of these Principles means in practice and what you must do to comply is set out below.

2.2.2 Lawfulness, fairness, transparency

You must process personal data lawfully, fairly and in a transparent manner in relation to the individual. This means you may only collect, process and share personal data fairly and lawfully and for specified purposes. The GDPR allows processing for specific purposes, some of the most relevant ones for Froneri are set out below:

- the individual has given his or her consent (this will be most relevant when undertaking marketing);

- the processing is necessary for the performance of a contract with the individual (this is likely to be relevant when you are processing employee personal data such as their payroll information in order to pay them as agreed);
- to meet our legal compliance obligations (this is likely to be relevant when you are processing employee personal data such as immigration and right to work documentation to meet your employment law obligations, or when processing disability information to ensure the work place is safe for an employee);
- to protect the individual's vital interests (this is likely to be relevant when you process medical information to protect an individual's health); or
- to pursue our legitimate interests for purposes where they are not overridden because the processing prejudices the interests or fundamental rights and freedoms of individuals. If we rely on 'legitimate interests' to process personal data we must explain clearly what this interest is in the applicable Privacy Notice (see section 2.2.4 (below)).

If you do not have a specific and lawful purpose for processing the personal data, you cannot process it, so it's important you understand what lawful basis you are relying on to process the personal data. The grounds may be different for different types of personal data.

You must identify the ground being relied on for each processing activity before you undertake it and you must document this in a Data Processing Register which must be maintained by each Froneri business. Guidelines on how to identify the lawful basis for processing personal data and a *Froneri Template Data Processing Register* is available from the Group Head of Legal. Your Data Processing Register must be available on request.

2.2.3 Consent

Consent is one way to lawfully process data. However, consent should not be relied on as the preferred legal basis for processing personal data because consent can be difficult to obtain lawfully and can always be withdrawn.

Consent should not be used in Froneri for processing employee data and local Froneri businesses should ensure their employment contracts and associated documentation reflect this position. In most cases, Froneri will have another lawful basis for processing the personal data it holds, such as to perform a contract (e.g. with an employee, customer or a supplier), to meet legal obligations (e.g. when processing certain employee data), or for our legitimate business interests (e.g. processing customer contact information when customers make a complaint).

Consent should only be used in limited circumstances (e.g. when we collect personal data for direct marketing purposes on the basis of the individual's consent). If you do need to rely on consent, you must ensure the consent is valid under GDPR.

What is valid consent?
• *Consent must be freely given, specific, informed and be an unambiguous indication of the individual's wishes. This means you must use very clear language, telling the individual why we want the data and what we're going to do with it and giving them a genuine free choice to*

consent or not. You should give separate distinct ('granular') options to consent separately to different purposes and types of processing, where relevant.

- *Consent must be indicated either by a statement or positive action (such as ticking a box or clicking a button). Silence, pre-ticked boxes or inactivity are not sufficient.*
- *If consent is given in a document which deals with other matters, then the consent must be kept separate from those other matters.*
- *You should inform the individual that consent can be withdrawn at any time and any withdrawal must be promptly honoured.*

A *Froneri Template Marketing Consent Form* which can be used when collecting consent for marketing purposes is available from the Group Head of Legal.

Consents are generally only valid for a reasonable period of time before they need to be refreshed; there is no set time limit for consent. How long it lasts will depend on the context. Consent may also (in some circumstances) need to be refreshed if you intend to process personal data for a different and incompatible purpose which was not disclosed when the individual first consented. You should review and refresh consent as appropriate.

Unless you can rely on another legal basis of processing, explicit consent (consent which requires a very clear and specific statement (not just a positive action)) is usually required for processing sensitive personal data (see the definition of sensitive personal data in section 2.2.1), for Automated Decision-Making (see section 2.2.17) and for cross border data transfers (see section 2.2.11). Usually you will be relying on another legal basis (and not require explicit consent) to process most types of sensitive data at Froneri. Where explicit consent is required, you must issue a Privacy Notice (see section 2.2.4 below) to the individual to capture their explicit consent.

You must evidence consent captured and keep records of all consents you are relying on (including when and how you got the consent from the individual and what they were told at the time) so that Froneri can demonstrate compliance with GDPR requirements. A *Froneri Template Consent Register* is available for recording this information.

2.2.4 Transparency (notifying individuals)

The GDPR requires Froneri to provide detailed, specific information to individuals depending on whether the information was collected directly from them or from elsewhere. Such information must be provided through appropriate privacy notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that an individual can easily understand them.

What is a privacy notice or a privacy policy?

A notice setting out information that must be provided to individuals when Froneri collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one-time privacy statements covering processing related to a specific purpose.

Whenever you collect personal data directly from individuals, including for HR or employment purposes, you must provide the individual with all the information required by the GDPR including:

- the identity of the Data Controller (this is the person/organisation responsible for making decisions about the management of the personal data and in our case, will be the relevant local Froneri business who is the Data Controller of personal data relating to its colleagues and personal data used in its business for its own commercial purposes) and Data Protection Officer (DPO) if there is one, or if not, someone with responsibility for overseeing data protection compliance within the local Froneri business; and
- how and why you will use, process, disclose, protect and retain that personal data.

This information should be provided through a privacy notice which must be presented when the individual first provides the personal data.

What is a Data Protection Officer or a DPO?
A DPO is the person required to be appointed in specific circumstances under the GDPR to oversee data protection compliance. There is no Group DPO at Froneri as we are not legally required to have one; however, you must check whether your local Froneri business needs a DPO under local law. If it does not, you should still ensure a suitable person in your organisation has responsibility for overseeing data protection compliance and can act as a key contact in your business. Where a mandatory DPO has not been appointed, this term means a data protection manager or other person in the business who has responsibility for data protection compliance.

External facing privacy notices (relating to how you process data about customers, suppliers and others) should be published on the local Froneri website. *Froneri Template Privacy Notices* are available from the Group Head of Legal.

When personal data is collected indirectly (for example, from a third party or publically available source), you must provide the individual with all the information required by the GDPR (explained above) as soon as possible after collecting/receiving the data. You must also check that the personal data was collected by the third party in accordance with the GDPR and on a basis which contemplates your proposed processing of that personal data; this will require you to ask for certain information from the third party about how they collected the data, what information was provided to that individual and obtain records to verify this, where possible. Please contact the Group Head of Legal for further guidance.

2.2.5 Purpose limitation

Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes. This means that you cannot use personal data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the individual of the new purposes and they have consented where necessary. For example, if you collect personal data to recruit an individual, you cannot then use that personal data for a different purpose which is incompatible with the recruitment of that individual, such as sending them marketing about third party products.

Keeping a record of your processing using the *Froneri Template Data Processing Register* (as required under section 2.2.2 above) will help you to check the purpose of processing and identify whether a new purpose is incompatible or not.

2.2.6 Data minimisation

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

You may only process personal data when performing your job duties requires it. You cannot process personal data for any reason unrelated to your job duties.

You may only collect personal data that you require for your job duties: do not collect excessive data. Ensure any personal data collected is adequate and relevant for the intended purposes. Remember, the more you collect, the more you have to manage and protect, so please collect only the minimum data required.

You must ensure that when personal data is no longer needed for specified purposes, it is deleted or anonymised in accordance with Froneri's data retention guidelines.

2.2.7 Accuracy

Personal data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

You must ensure that the personal data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any personal data at the point of collection and at regular intervals afterwards (for example, on an annual basis). You must take all reasonable steps to destroy or amend inaccurate or out-of-date personal data within a reasonable time after becoming aware of the inaccuracy (e.g. within 72 hours of notification of inaccuracy by a customer or employee).

2.2.8 Storage limitation

Personal data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

You must not keep personal data in a form which permits the identification of the individual for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for satisfying any legal, accounting or reporting requirements.

Each Froneri business must maintain retention policies and procedures to ensure personal data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time. Such retention policies and procedures must comply with local law.

You will take all reasonable steps to destroy or erase from your systems all personal data that is no longer required in accordance with all Froneri's applicable retention policies and procedures. This includes requiring third parties to delete such data where applicable.

You will ensure individuals are informed of the period for which data is stored and how that period is determined in the applicable Froneri Privacy Notice.

2.2.9 Security integrity and confidentiality

We must secure personal data using appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

What are 'technical and organisational measures'?
This term is used in GDPR to describe all measures an organisation uses to protect personal data. A 'technical measure' includes measures involving technology such as password protection, encryption, intrusion detection systems and firewalls. An 'organisational' measure is anything used within an organisation to protect personal data other than technology and includes policies, procedures and training. It is important we can clearly identify what measures we use and what measures third parties use when they process personal data on our behalf. We should regularly assess our measures to ensure they remain appropriate based on the nature of the personal data we process and market standards.

Froneri will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of personal data that we own or maintain on behalf of others and identified risks (including use of encryption where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our processing of personal data.

Each Froneri business is responsible for protecting the personal data it holds and must implement reasonable and appropriate security measures against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. Particular care must be exercised in protecting sensitive personal data from loss and unauthorised access, use or disclosure.

You must follow all procedures and technologies we put in place to maintain the security of all personal data from the point of collection to the point of destruction. You may only transfer personal data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

- *Confidentiality* means that only people who have a need to know and are authorised to use the Personal Data can access it.
- *Integrity* means that Personal Data is accurate and suitable for the purpose for which it is processed.

- *Availability* means that authorised users (and in some cases, individuals themselves) are able to access the Personal Data when they need it for authorised purposes.

You must comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the GDPR and relevant standards to protect Personal Data. This includes Froneri Information Security Policies.

Each Froneri business is responsible for maintaining an up to date description of its technical and organisational measures and documenting them in it Data Processing Register (see section 2.2.14 (below)) to demonstrate compliance with this principle.

Each Froneri business must, on implementation of this Policy, and on regular basis thereafter undertake an assessment of the adequacy of its technical and organisational measures to ensure they are protecting the personal data appropriately. In some cases, Froneri Group will conduct and/or engage third parties to conduct such assessments on its behalf and Froneri businesses must co-operate with these assessments.

2.2.10 Reporting a Personal Data Breach

The GDPR requires Froneri to notify any Personal Data Breach to the applicable Regulator and, in certain instances, the individual. This must be done in certain timescales (often within 72 hours of the breach).

What is a personal data breach?
A Personal Data Breach is anything that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. This includes loss (such as the loss of a laptop containing personal data), or unauthorised access (such as hacking), disclosure (such as accidental disclosure to a third party) or acquisition, of Personal Data.

Froneri Group has created a Data Breach Procedure that will be followed in the case of a personal data breach affecting personal data at a Group level i.e. involving a Group managed IT system, database or service or which involves individuals in more than one Froneri territory (a copy of the Procedure is available from the Group Head of Legal).

Each Froneri business must put in place a local Data Breach Procedure to deal with any suspected local territory personal data breach and notify individuals or their local Regulator where they are legally required to do so. Any personal data breach which results in a notification to a local Regulator must be first notified to the Group Head of Legal.

2.2.11 Transfer limitation

The GDPR restricts data transfers to countries outside the European Economic Area (being the 28 countries in the EU, and Iceland, Liechtenstein and Norway) ("EEA") to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. Personal data originating in one

country is transferred across borders when you transmit, send, view or access that data in or to a different country. For example, if you access a global HR system hosted in Germany from Australia.

You may only transfer Personal Data outside the EEA if one of the following conditions applies:

- the European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the individuals' rights and freedoms;
- appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO;
- the individual has provided explicit consent to the proposed transfer after being informed of any potential risks; or
- the transfer is necessary for one of the other reasons set out in the GDPR including the performance of a contract between us and the individual, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the individual where the individual is physically or legally incapable of giving consent and, in some limited cases, for our legitimate interest.

Remember if the cross-border data transfer happens when working with a third party (such as using a third-party IT system hosted outside the EEA), you must comply with section 2.2.19 which sets out minimum requirements for engaging third parties who process personal data on Froneri's behalf.

You can obtain further guidance on cross border data transfers and model contractual clauses which can be used to help protect the data being transferred from the Group Head of Legal.

2.2.12 Individual's rights and requests

Individuals have rights when it comes to how we handle their personal data including the right to make a Data Subject Request exercising one of their rights. Each Froneri business must have a GDPR compliant Data Subject Request Procedure in place within their business to appropriately assess and respond to requests in accordance with GDPR. An example procedure can be obtained from the Group Head of Legal.

What are the Data Subject Rights that individuals have?
These include rights to: • *withdraw consent to processing at any time;* • *receive certain information about Froneri's processing activities;* • *request access to their Personal Data that we hold;* • *prevent our use of their Personal Data for direct marketing purposes;* • *ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;*

- *restrict processing in specific circumstances;*
- *challenge processing which has been justified based on our legitimate interests or in the public interest;*
- *request a copy of an agreement under which Personal Data is transferred outside of the EEA;*
- *object to decisions based solely on Automated Processing, including profiling (ADM);*
- *prevent processing that is likely to cause damage or distress to the individual or anyone else;*
- *be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;*
- *make a complaint to the local data protection authority; and*
- *in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format.*

2.2.13 Accountability

We are responsible for, and must be able to demonstrate, compliance with the data protection principles.

Froneri must have adequate resources and controls in place to ensure and to document GDPR compliance including:

- appointing a suitably qualified DPO (where necessary) and an executive accountable for data privacy (if a local Froneri business does not appoint a DPO, it should record the reason for its decision not to do so and instead ensure it has a local contact responsible for data protection compliance – see section 2.2.14);
- implementing Privacy by Design when processing personal data and completing DPIAs where processing presents a high risk to rights and freedoms of individuals (see section 2.2.16);
- integrating data protection into internal documents including this Policy;
- regularly training Froneri colleagues on the GDPR, this Policy and data protection matters (se section 2.2.15); and
- regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

2.2.14 Record keeping

The GDPR requires us to keep full and accurate records of all our data processing activities.

Each Froneri business must keep and maintain accurate corporate records reflecting the data processing it undertakes. These records should include, at a minimum, the name and contact details of the Froneri Data Controller and the DPO (if there is one), clear descriptions of the personal data types, individual types, processing activities, processing purposes, third-party recipients of the

personal data, personal data storage locations, personal data transfers, the personal data's retention period and a description of the security measures in place.

The 5 Registers that must, as a minimum, be created and maintained as up to date and accurate are:

1. Data Processing Register (see the *Froneri Template Data Processing Register*);
2. Consent Register (see the *Froneri Template Consent Register*);
3. Data Subject Access Request Register (see the *Froneri Template DSAR Register*);
4. DPIA Register (see the *Froneri Template DPIA Register*); and
5. Personal Data Breach Register (see the *Froneri Template Personal Data Breach Register*),

as well as a record of the contact details of your local DPO or, if none, your rationale for why a local DPO is not needed under applicable local law. Contact the Group Head of Legal for support in this assessment. These Registers must be available for inspection by the Group Head of Legal and any relevant Regulator at any time.

2.2.15 Training and audit

We are required to ensure all Froneri colleagues have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

You must regularly review all the systems and processes under your control to ensure they comply with this Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of personal data.

As a minimum you must ensure all Froneri staff are trained on the requirements of this Policy and GDPR, and that targeted training is provided to those colleagues whose role requires them to process personal data (such as Management, HR, Marketing and Sales) on an annual basis. Records should be kept to evidence who received training and when. *Froneri Template Training Materials* are available from the Group Head of Legal.

From time to time the Group Head of Legal supported by the Group Head of Internal Audit will assess your country's compliance with the requirements of this Policy.

2.2.16 Privacy by Design and Data Protection Impact Assessment (DPIA)

We are required to implement Privacy by Design measures when processing personal data by implementing appropriate technical and organisational measures (see section 2.2.9) in an effective manner, to ensure compliance with data privacy principles.

Each Froneri business must assess what Privacy by Design measures can be implemented on all programs, systems or processes that process personal data by considering the following:

- the state of the art;
- the cost of implementation;
- the nature, scope, context and purposes of processing; and

- the risks of varying likelihood and severity for rights and freedoms of individuals posed by the processing.

For example, this might involve ensuring that sensitive employee data relating to racial or ethnic origin used for equal opportunities monitoring is pseudonymised before it is input into a HR database to minimise the ability for individuals accessing that data to identify the individuals concerned where this is irrelevant for the purpose of equal opportunities monitoring. This is about designing systems and processes with privacy as one of the guiding principles before we implement that system or process.

We must also conduct a 'Data Privacy Impact Assessment' (DPIA) (which is a tool used to identify and reduce risks of a data processing activity) in respect to high risk processing.

What is 'high risk processing'?
High risk processing is anything that could pose a higher than normal risk to an individual because of how we process their personal data or the nature or scale of the processing we want to undertake. This could include where we want to start tracking / monitoring individuals for marketing purposes or where we want to move a large amount of data from one system to another system.

You should conduct a DPIA (and discuss your findings with your DPO (or if none, the Group Head of Legal) when implementing any major system or business change programs involving the processing of personal data. For Froneri, this is likely to be relevant when you want to:

- use new technologies (such as a new IT system or process);
- use Automated Processing including profiling and ADM (see section 2.2.17 (below));
- conduct large scale processing of sensitive data (such as for employment purposes) (see the definition of personal data in section 2.2.1).

DPIAs should be conducted using the *Froneri Template DPIA* and copies of the DPIAs submitted to the Group Head of Legal and any relevant Group Function Head (such as the Head of IT or the Head of HR) for review before the relevant activity is undertaken. A Register of all DPIAs undertaken should also be maintained in accordance with section 2.2.14 (Record Keeping).

2.2.17 Automated Decision-Making and Automated Processing

What is Automated Decision-Making (ADM) and Automated Processing?
Automated Decision-Making (ADM) is when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. *Automated Processing means any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.*

Generally, ADM is prohibited under GDPR when a decision has a legal or similar significant effect on an individual unless certain conditions are met.

Froneri does not generally use Automated Processing or ADM within its business. If you identify a need for Automated Processing or ADM, please contact the Group Head of Legal for further guidance.

2.2.18 Direct marketing

We are subject to certain rules and privacy laws when marketing to our customers.

For example, an individual's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing must be explicitly offered to the individual in an intelligible manner so that it is clearly distinguishable from other information.

An individual's objection to direct marketing must be promptly honoured. If an individual opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future (i.e. it does not mean deleting the data, but keeping a record to ensure the details cannot be marketed to again).

You must comply with Froneri's guidelines on direct marketing and use the *Froneri Template Marketing Consent Form* when collecting personal data for marketing purposes (available from the Group Head of Legal).

2.2.19 Sharing Personal Data

Generally, we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

You may only share the personal data we hold with another employee, agent or representative of the Froneri Group if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

You may only share the personal data we hold with third parties, such as our service providers if:

- they have a need to know the information for the purposes of providing the contracted services;
- sharing the personal data complies with the privacy notice provided to the individual and, if required, the individual's consent has been obtained;
- the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;

- the transfer complies with any applicable cross border transfer restrictions (see section 2.2.11 above); and
- a fully executed written contract that contains GDPR approved third party clauses has been obtained (see below).

When you engage a third party to process data on Froneri's behalf (known as a 'data processor') (e.g. you engage an IT provider or a marketing agency or another supplier who you want to provide with employee or customer personal data), you must first undertake due diligence on that third party to ensure that they will process the personal data in accordance with applicable law. As a minimum you must ensure you understand what they will use the data for, who will have access to it, where it will be located / transferred to and what technical and organisational security measures the third party will use to protect the data. The *Froneri Template Data Processor Questionnaire* is available from the Group Head of Legal for this purpose.

Once you have completed the due diligence and you are happy that the third party is able to meet the requirements of applicable law, you must enter into a written contract with that third party which requires them to protect the data in accordance with GDPR. There are certain contractual clauses that you must include in the contract to ensure it meets applicable legal requirements; failure to do so is a breach of the law. *Froneri Template Data Processor Contractual Clauses* are available from the Group Head of Legal for this purpose.

At the end of the engagement with the third party, you should ensure that they securely and permanently delete any personal data they held on our behalf so they cannot access or use it again in future. You should obtain written confirmation from the third party that they have undertaken this deletion.

You should maintain appropriate records to identify any third-party data processor appointed, keep a copy of the due diligence undertaken and dates when they were appointed and when their appointment ended including confirmation that deletion of any personal data has occurred. Such records must be available for inspection on request.

2.3 Scope and Exceptions

This Policy applies to all Froneri businesses and colleagues, both inside and outside Europe.

This Policy does not override any applicable national data privacy laws and regulations in countries where Froneri operates. If a local Froneri business is subject to more stringent local laws, the higher standard will apply.

Any local variations to or derogations from this Policy are only permitted with the prior written approval of the Group Head of Legal.

2.4 Roles and Responsibilities

Country Managers and Heads of Finance are responsible for ensuring local business compliance with this Policy.

Local business colleagues who process personal data are responsible for complying with any Froneri policies and procedures implemented to protect that personal data and comply with applicable laws.

The Group Head of Legal is responsible for providing advice and guidance on compliance with this Policy and applicable laws.

2.5 Froneri Delegation of Authority (DOA) References

N/A

2.6 Consequences for non-compliance

Consequences to Froneri

Data Protection laws carry potentially significant civil and criminal liability. Where Data Protection Laws are breached Froneri is also likely to face loss of customers, damage to reputation, financial penalties and it might also place Froneri in breach of contractual undertakings that it has given to third parties.

Consequences to colleagues

Colleagues should also ensure that they personally do not undertake any activity in breach of Data Protection laws as in some cases, this can attract personal liability for the individual.

Given the potential consequences outlined above, failure to comply with this Policy may result in disciplinary action.

2.7 Contacts

Should you have any questions about the content of this Policy, please contact the Group Head of Legal.

2.8 Appendix

Other relevant Policies / Templates:

- Froneri Template Registers:
  - Froneri Template Data Processing Register
  - Froneri Template Consent Register
  - Froneri Template Personal Data Breach Register
  - Froneri Template DPIA Register
  - Froneri Template DSAR Register
- Froneri Template Employee Privacy Notice
- Froneri Template Candidate Privacy Notice
- Froneri Template Privacy Policy (and guidance notes on minimum requirements)
- Froneri Template Marketing Consent Form
- Froneri Template Data Subject Request Procedure
- Froneri Template DPIA (Data Privacy Impact Assessment)
- Froneri Template Data Protection Training Materials
- Froneri Template Data Processor Questionnaire
- Froneri Template Data Processor Contractual Clauses
- Froneri Template Training Materials
- Froneri Group Data Breach Procedure
- Froneri Guidelines on Lawful Processing
- Froneri Guidelines on Data Retention