SAINT-GOBAIN UK & IRELAND

DATA PROTECTION POLICY

Internal company policy, not intended for circulation outside of the business.

External requests should be directed towards our Privacy Statement available with other external facing policies on our ***Saint-Gobain Policies*** *page.*

Contents

PART 1 - POLICY STATEMENT 3
INTRODUCTION 3
SCOPE 4
PART 2 - DATA PROTECTION PRINCIPLES UNDER THE GDPR 5
1. Principles 5
PART 3 - KEY REQUIREMENTS AND SPECIFIC PROCEDURES 6
1 LAWFULNESS, FAIRNESS, TRANSPARENCY 6
1. Lawfulness and Fairness 6
2. Consent 6
3. Performance of a Contract 7
4. Legal Compliance 7
5. Pursue Our Legitimate Interests 7
6. Transparency (Notifying Data Subjects) 7
2 PURPOSE LIMITATION 7
3 DATA MINIMISATION 8
4 ACCURACY 8
5 STORAGE LIMITATION 8
6 SECURITY INTEGRITY AND CONFIDENTIALITY 8
6.1 Protecting Personal Data 8
6.2 Reporting a Personal Data Breach 9
7 TRANSFER LIMITATION 10
8 DATA SUBJECT'S RIGHTS AND REQUESTS 10
9 ACCOUNTABILITY 11
9.1 Compliance 11
9.2 Resources and Controls 11
9.3 Record Keeping 12
9.4 Training and Audit 12
9.5 Privacy by Design and Data Protection Impact Assessment (DPIA) 12
9.6 Automated Processing (Including Profiling) and Automated Decision- Making 13
9.7 Direct Marketing 13
9.8 Sharing Personal Data 14
PART 4 - DEFINITIONS AND INTERPRETATION 15

PART 1 - POLICY STATEMENT

INTRODUCTION

1.1 Saint-Gobain is committed to respecting privacy and ensures the security and confidentiality of the Personal Data of the users of its services.

1.2 Any Processing of Personal Data must be legal and fall within one of the authorised cases (consent of the individual, performance of a contract, compliance with a legal obligation or justified by a legitimate interest).

1.3 The definitions set out in Part 4 of this Data Protection Policy ("**Policy**") shall apply to this Policy.

1.4 This Policy sets out the roles and responsibilities of and how every Saint-Gobain company/business in the UK and Ireland and all employees ("**we**", "**our**", "**us**", "**the Company**") handle the Personal Data of our customers, suppliers, employees, workers and other third parties.

1.5 This Policy consists of the following sections:

1.5.1 **Part 1** - this sets out the **policy statement** and employees' responsibilities when Processing Personal Data;

1.5.2 **Part 2** - this sets out the **data protection principles** under the (i) retained EU law version of the General Data Protection Regulation (EU 2016/679) ("UK GDPR") (ii) and, in (i) the UK, the UK Data Protection Act 2018, (ii) Ireland, the Irish Data Protection Act 2018 (iii) Jersey, the Data Protection (Jersey) Law 2018, (iv) Guernsey, the Data Protection (Bailiwick of Guernsey) Law 2017 and (v) the Isle of Man, the Data Protection Act 2018 (together the "DPA") (iii) any laws and regulations ratifying, implementing, adopting, supplementing or replacing the DPA and UK GDPR.

1.5.3 **Part 3** - this sets out **key requirements and specific procedures** which must be followed by employees when Processing Personal Data; and

1.5.4 **Part 4** - this sets out the **definitions** used throughout this Policy.

1.6 This Policy applies to all Personal Data we Process regardless of the media on which the data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other Data Subject.

1.7 This Policy applies to all Company Personnel ("**you**", "**your**"). You must read, understand and comply with this Policy when Processing Personal Data on our behalf and attend training on its requirements. This Policy sets out what we expect from you in order for the Company to comply with applicable law.

1.8 Your compliance with this Policy, and the Related Policies, is mandatory. Related Policies are available to help you interpret and act in accordance with thisPolicy. **Any breach of this Policy and/or Related Policies may result in disciplinary action**.

1.9 This Policy must be read in conjunction with the Related Policies, all of which are **internal documents** and must not be shared with third parties, clients or regulators without prior authorisation from the Privacy Advisor whose contact details are set out in 2.3 below.

1.10 We reserve the right to change this Policy at any time without notice to you, so **please check back regularly** to obtain the latest copy of this Policy. We last revised this Policy on 1st September 2021. We will endeavour to provide you with a new version of this Policy when we make any substantial updates. However, it is your responsibility to ensure you are aware of any changes.

1.11 This Policy does not override any applicable national data privacy laws and regulations in countries where the Company operates. Certain countries may have localised variances to this Policy which may be available upon request to the Privacy Advisor.

SCOPE

2.1 The correct and lawful treatment of Personal Data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility to be taken seriously at all times. The Saint- Gobain Group is exposed to **potential fines of up to €20m** (approximately £18m) or **4% of total worldwide group annual turnover**, whichever is higher and depending on the breach, for failure to comply with the provisions of the GDPR.

2.2 All employees, consultants and agents are responsible for ensuring they are fully aware of and comply with this Policy. Every company/business, with support from their Privacy Correspondent and Privacy Advisor, must implement appropriate practices, processes, controls and training to ensure such compliance.

2.3 The Privacy Advisor is responsible for overseeing this Policy and, as applicable, developing Related Policies. The post is held by Rosie Prabhakar, Solicitor, who is contactable at rosie.prabhakar@saint-gobain.com

2.4 Please contact your Company's Privacy Correspondent with any questions about the operation of this Policy or the UK GDPR or if you have any concerns this Policy is not being or has not been followed. In particular, **you must always** contact your Company's Privacy Correspondent in the following circumstances:

a) if you are **unsure of the lawful basis** which you are relying on to process Personal Data (including the legitimate interests used by the Company) (see Section 1.1 of Part 3);

b) if you **need to rely on Consent** and/or need to **capture Explicit Consent** (see Section 1.2 of Part 3);

c) if you need to **draft Privacy Notices** or **Fair Processing Notices** (see Section 1.3 of Part 3);

d) if you are **unsure about the retention period** for the Personal Data being Processed (see Section 5 of Part 3);

e) if you are **unsure about what security** or other measures you need to implement to protect Personal Data (see Section 6.1 of Part 3);

f) if there has been a **Personal Data Breach** (Section 6.2 of Part 3);

g) if you are unsure on **what basis to transfer** Personal Data outside the EEA (see Section 7 of Part 3);

h) if you need any assistance **dealing with any rights** invoked by a Data Subject (see Section 8);

i) whenever you are engaging in a significant new, or change in, **Processing activity** which is likely to require a DPIA (see Section 9.5 of Part 3) or plan to use Personal Data for **other purposes** than what it was collected for;

j) If you plan to undertake any activities involving **Automated Processing** including profiling or **Automated Decision-Making** (see Section 9.6 of Part 3);

k) If you need help complying with applicable law when carrying out **direct marketing activities** (see Section 9.7 of Part 3); or

l) if you need help with any contracts or other areas in relation to sharing Personal Datawith third parties (see Section 9.8 of Part 3).

2.5 Details of the Privacy Correspondent for your Company can be found on the UK Governance and Compliance intranet page.

PART 2 - DATA PROTECTION PRINCIPLES UNDER THE GDPR

1. Principles

1.1. We adhere to the principles relating to Processing of Personal Data set out in the UK GDPR which require Personal Data to be:

a. Processed **lawfully**, **fairly** and in a **transparent** manner (Lawfulness, Fairness and Transparency).

b. Collected only for specified, explicit and legitimate purposes (Purpose Limitation).

c. **Adequate, relevant and limited to what is necessary** in relation to the purposes forwhich it is Processed (Data Minimisation).

d. Accurate and where necessary **kept up to date** (Accuracy).

e. Not kept in a form which permits identification of Data Subjects for l**onger than is necessary for the purposes** for which the data is Processed (Storage Limitation).

f. Processed in a manner **ensuring 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).

1.2. We will **not transfer personal data to another country** without appropriate safeguards being in place in accordance with the UK GDPR.

1.3. We will make personal data available to Data Subjects and enable Data Subjects to **exercise certain rights** in relation to their Personal Data (Data Subject's Rights and Requests) in accordance with the UK GDPR.

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

PART 3 - KEY REQUIREMENTS AND SPECIFIC PROCEDURES

1 LAWFULNESS, FAIRNESS, TRANSPARENCY

1. Lawfulness and Fairness

1.1. Personal Data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

1.2. Examples of Personal Data include (but is not limited to): employment records, names and addresses.

1.3. You may only collect, process and share Personal Data fairly and lawfully and for specified purposes. The UK GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing, but ensure we Process Personal Data fairly and without adversely affecting the Data Subject.

1.4. A Data Controller must only process Personal Data on the basis of one or more of the lawful bases set out in the UK GDPR, which include Consent.

1.5. The UK GDPR allows Processing for specific purposes, some of which are set out below:

a. the Data Subject has given his or her Consent;

b. the Processing is necessary for the performance of a contract with the Data Subject;

c. to meet our legal compliance obligations;

d. to protect the Data Subject's vital interests; or

e. to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices or Fair Processing Notices.

1.6. You must identify and document the legal ground being relied on for each Processing activity, and seek supervisor approval before Processing Personal Data.

1.7. ICO guidance entitled "Collecting Personal Data" is available for further details on how to ensure Personal Data is collected and handled fairly and lawfully.

2. Consent

2.1. A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action; so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

2.2. Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

2.3. Unless we can rely on another legal basis of Processing, Explicit Consent is usually required for Processing Special Categories of Personal Data, for Automated Decision-Making and for cross border data transfers. Usually we will be relying on another legal basis (and not require Explicit Consent) to Process most types of Special Categories of Data. Where Explicit Consent is required, you must issue a FairProcessing Notice to the Data Subject to capture Explicit Consent.

2.4. You will need to evidence Consent captured and keep records of all Consents so the Company can demonstrate compliance with Consent requirements.

3. Performance of a Contract

3.1. We can rely on this lawful basis when we need to process an individual's data:
   a. in order to fulfil a contract with the individual;
   b. because they have asked us to do something before entering a contract with them (preparatory steps).

4. Legal Compliance

4.1. We can rely on this lawful basis where we are required to process data due to legal obligations imposed upon us.

4.2. This basis does not apply to contractual obligations: we can process personal data where it is necessary to do so due to an identifiable, specific legal obligation to which we are subject. Examples of the use of this basis may be where we need to processdata in order to disclose details to HMRC, or due to a court order.

5. Pursue Our Legitimate Interests

5.1. We can rely on this basis for process where:
   a. we believe we have a legitimate interest in processing the data of the individual; and
   b. we have analysed those interests, as against the likely impact on the rights, interests, and freedoms of the individuals affected, and have determined our own interests outweigh the impact on the individual.

5.2. We must:
   a. identify a legitimate interest (the 'purpose test');
   b. show the processing is necessary to achieve its interest (the 'necessity test'); and
   c. balance the interest against the individual's rights, interests and freedoms (the 'balancing test').

5.3. We must keep a record of all of our legitimate interests' assessments in order to demonstrate our compliance with the GDPR

6. Transparency (Notifying Data Subjects)

6.1. The UK GDPR requires Data Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate **Privacy Notices or Fair Processing Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language** so a Data Subject can easily understand them.

6.2. Whenever we collect Personal Data directly from Data Subjects, including for human resources or employment UK purposes, we must provide the Data Subject with all the information required by the GDPR including the **identity of the Data Controller,** howand why we will use, process, disclose, protect and retain Personal Data througha Fair Processing Notice which must be presented when the Data Subject first provides the Personal Data.

6.3. When Personal Data is collected indirectly (for example, from a third party or publically available source), you must provide the Data Subject with all the information required by the UK GDPR as soon as possible after collecting/receiving the data and in any event within 30 days. You must also check the Personal Data was collected by the third party in accordance with the UK GDPR and on a basis which contemplates our proposed Processing of the Personal Data.

2 PURPOSE LIMITATION

2.1 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.

2.2 You cannot use Personal Data for new, different or incompatible purposes from any disclosure when it was first obtained unless you have informed the Data Subject of the new purposes and they have Consented where necessary.

3 DATA MINIMISATION

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

3.2 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.

3.3 You may only collect Personal Data you require for your job duties: **do not collect excessive data**. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

3.4 You must ensure when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Company's data retention guidelines.

4 ACCURACY

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

4.2 You will ensure the Personal Data we use and hold is accurate, complete, kept up to dateand 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. **You must take all reasonable steps to destroy or amend inaccurate or out of date Personal Data**.

5 STORAGE LIMITATION

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

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

5.3 Each Company shall maintain adequate and appropriate 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. **You must comply with the Company's guidelines on Data Retention**.

5.4 **You will take all reasonable steps to destroy or erase from our systems all Personal Data we no longer require** in accordance with all the Company's applicable records retention schedules and policies. This includes requiring third parties to delete such data where applicable.

5.5 You will ensure Data Subjects are informed of the period for which data is stored and how this period is determined in any applicable Privacy Notice or Fair Processing Notice.

6 SECURITY INTEGRITY AND CONFIDENTIALITY

6.1 Protecting Personal Data

6.1.1 Personal Data must be **secured by appropriate technical and organisational measures** against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

6.1.2 The Company will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data we own or maintain on behalf of others and identified risks (including use of encryption and

Pseudonymisation where applicable). We will **regularly evaluate and test the effectiveness of those safeguards** to ensure security of our Processing of Personal Data. You are responsible for protecting the Personal Data we hold. **You 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. For more information also see IT User Charter. You must **exercise particular care in protecting specialcategories of Personal Data** and data concerning criminal convictions from loss andunauthorised access, use or disclosure.

6.1.3 You must **follow all procedures and/or technologies** 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.

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

a) **Confidentiality** means only those people who have a **need to know and are authorised** to use the Personal Data can access it.

b) Integrity means Personal Data is accurate and suitable for the purpose for which it is processed.

c) **Availability** means authorised users are able to access the Personal Data **when they need it** for authorised purposes.

6.1.5 You must ensure Personal Data is stored in a manner which enables it to be Processed in accordance with the UK GDPR. For example:

a) Manual records must be kept secure by the use of **locked cabinets**. Access to such records must be restricted. Where a manual record is in constant use, appropriate security measures must be taken. These include securing such records during lunch breaks and outside office hours.

b) **Passwords and physical security measures** must be in place to guard against unauthorised disclosures. Company computer systems (and computer files, as far as it is reasonable) must be **password protected and use adequate encryption**.

c) Particular care must be taken of **Special Categories of Personal Data** and security measures must **reflect the importance** of keeping such Special Categories of Personal Data secure and preventing unauthorised disclosure. This includes the use of **lockable cabinets and password protection** of automated data. When sending attachments containing Special Categories of Personal Data or large volumes of Personal Data (whether internally or externally), these files must be sent using the **OneDrive facility** available for such purposes and extra care must be taken where Personal Datais being sent externally (including to other companies within the Saint-Gobain group).

d) Access **controls and passwords** must be applied to **employment records**, and paying particular attention to the use of e-mail, to prevent unauthorised access.

6.2 Reporting a Personal Data Breach

6.2.1 The UK GDPR requires Data Controllers to **notify any Personal Data Breach** to the applicable Regulator within 72 hours (including weekends and bank holidays) and, in certain instances, the Data Subject.

6.2.2 The Company has put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

6.2.3 If you know or suspect a Personal Data Breach has occurred, **do not attempt to investigate the matter yourself**. Immediately contact your line manager and your Privacy Correspondent. You must **preserve all evidence** relating to the potential Personal Data Breach.

6.2.4 Even if the incident is not reportable to ICO and/or the data subjects affected, you must still involve your Privacy Correspondent and the Privacy Advisor at the earliest opportunity to document our decision making process, corrective actions or learnings and complete a OneTrust incident record. These smaller, less obvious breaches are those which are most likely to result in complaints to ICO therefore we must follow the correct procedure, not least because it may be scrutinised later by the authorities.

7 TRANSFER LIMITATION

7.1 The UK GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access data in or to a different country.

7.2 Before making a restricted transfer you must consider whether you can achieve your aims without actually sending personal data. If you make the data anonymous so it is never possible to identify individuals (even when combined with other information which is available to receiver), it is not personal data.

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

7.3.1 if the receiver is located in a third country or territory or is an international organisation, covered by UK "adequacy regulations";

7.3.2 **appropriate safeguards are in place** such as binding corporate rules (BCR). The concept of using BCRs to provide adequate safeguards for making restricted transfers was developed under EU law and continues to be part of UK law under the UK GDPR,

7.3.3 **Standard contractual clauses (SCCs)** - You can make a restricted transfer if you and the receiver have entered into a contract incorporating standard data protection clauses recognised or issued in accordance with the UK data protection regime. These are known as 'standard contractual clauses' ('SCCs' or 'model clauses'). The SCCs contain contractual obligations on you (the data exporter) and the receiver (the data importer), and rights for the individuals whose personal data is transferred. Individuals can directly enforce those rights against the data importer and the data exporter.

7.3.4 the Data Subject has provided **Explicit Consent to the proposed transfer** after being informed of any potential risks; or

7.3.5 the **transfer is necessary** for one of the other reasons set out in the UK GDPR including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests ofthe Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

8 DATA SUBJECT'S RIGHTS AND REQUESTS

8.1 Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

8.1.1 **withdraw Consent** to Processing at any time;

8.1.2 **receive certain information** about the Data Controller's Processing activities;

8.1.3 **request access** to their Personal Data we hold;

8.1.4 prevent our use of their Personal Data for direct marketing purposes;

8.1.5 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;

8.1.6 restrict Processing in specific circumstances;

8.1.7 challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;

8.1.8 **request a copy of an agreement** under which Personal Data is transferred outside of the EEA.;

8.1.9 **object to decisions** based solely on Automated Processing, including Automated Decision-Making;

8.1.10 **prevent Processing** likely to cause damage or distress to the Data Subject or anyone else;

8.1.11 **be notified of a Personal Data Breach** which is likely to result in high risk to their rights and freedoms;

8.1.12 **make a complaint** to the supervisory authority; and

8.1.13 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.

8.2 You must **verify the identity** of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

8.3 You **must immediately** forward any Data Subject request you receive to your Privacy Correspondent. Please also see ICO guidance note entitled "Right of access/subject access requests and other rights" for further information on this subject.

8.4 You must respond to a **request for erasure** without undue delay and at the latest within one month, letting the individual know whether you have erased the data in question, or you have refused their request, and if so and explanation of why data cannot be erased.

9 ACCOUNTABILITY

9.1 Compliance

9.1.1 The Data Controller must implement appropriate technical and organisational measures in aneffective manner, to ensure compliance with data protection principles.

9.1.2 The Data Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

9.2 Resources and Controls

The Company must have **adequate resources and controls in place** to ensure and to document UK GDPR compliance including:

9.2.1 **appointing Privacy Correspondents** accountable for data privacy (under the UK GDPR we are not required to appoint a Data Protection Officer);

9.2.2 **implementing Privacy by Design** when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;

9.2.3 **integrating data protection into internal documents** including this Policy, Related

Policies, Privacy Notices or Fair Processing Notices;

9.2.4 **regularly training** Company Personnel on the UK GDPR, this Policy, Related Policies and data protection matters including, for example, Data Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches. The Company must **maintain a record of training** attendance by Company Personnel; and

9.2.5 **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.

9.3 Record Keeping

9.3.1 The UK GDPR requires us to **keep full and accurate records** of all our data Processing activities.

9.3.2 You must keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents in accordance with the Company's record keeping guidelines.

9.3.3 These records must include, at a minimum, the **name and contact** details of the Data Controller, **clear descriptions** of the Personal Data types, Data Subject **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. In order to create such records, data maps should be created which include the detail set out above together with appropriate data flows.

9.4 Training and Audit

9.4.1 We are required to ensure all Company Personnel 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.

9.4.2 You must undergo all mandatory data privacy related training and ensure your team undergo similar mandatory training.

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

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

9.5.1 We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

9.5.2 You must assess what Privacy by Design measures can be implemented on all programs/systems/processes which Process Personal Data by taking into account the following:

a) the state of the art;

b) the cost of implementation;

c) the nature, scope, context and purposes of Processing; and

d) the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

9.5.3 Data Controllers must also conduct DPIAs in respect to high risk Processing.

9.5.4 You must **conduct a DPIA** (and discuss your findings with your Privacy Correspondent) when implementing major system or business change programs involving the Processing of Personal Data including:

a) use of **new technologies** (programs, systems or processes), or changing technologies (programs, systems or processes);

b) **Automated Processing** including profiling and ADM;

c) **large scale Processing** of Special Categories of Data; and

d) large scale, systematic monitoring of a publicly accessible area.

9.5.5 A DPIA must include:

a) a **description** of the Processing, its purposes and the Data Controller's legitimate interests if appropriate;

b) an **assessment of the necessity and proportionality** of the Processing in relation to its purpose;

c) an assessment of the risk to individuals; and

d) the **risk mitigation measures** in place and demonstration of compliance.

9.6 Automated Processing (Including Profiling) and Automated Decision Making

9.6.1 Generally, Automated Decision Making (ADM) is prohibited when a decision has a legal or similar significant effect on an individual unless:

a) a Data Subject has Explicitly Consented;

b) the Processing is authorised by law; or

c) the Processing is necessary for the performance of or entering into a contract.

9.6.2 If certain types of Special Categories of Data are being processed, then grounds (b) or (c) will not be allowed but such Special Categories of Personal Data can be Processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

9.6.3 If a decision is to be based solely on Automated Processing (including profiling), then Data Subjects must be informed when you first communicate with them of their right to object. This right must be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the Data Subject's rights and freedoms and legitimate interests.

9.6.4 We must also inform the Data Subject of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the Data Subject the right to request human intervention, express their point of view or challenge the decision.

9.6.5 A DPIA must be carried out before any Automated Processing (including profiling) or ADM activities are undertaken.

9.7 Direct Marketing

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

9.7.2 For example, a Data Subject'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 the same 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.

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

9.7.4 A Data Subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details are to be **suppressed as soon as possible**. Suppression involves retaining just enough information to ensure marketing preferences are respected in the future.

9.8 Sharing Personal Data

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

9.8.2 You may only share the Personal Data we hold with another employee, agent or representative of our group (which includes our subsidiaries and our ultimate holding company along with its subsidiaries) if the recipient has a **job-related need to know** the information and the transfer complies with any applicable cross-border transfer restrictions.

9.8.3 You may only share the Personal Data we hold with third parties, such as our service providers if:

a) they have a **need to know** or have access to the information for the purposes of providing the contracted services;

b) sharing the Personal Data **complies with the Privacy Notice** provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;

c) the third party has **agreed to comply** with the required data security standards, policies and procedures and put adequate security measures in place;

d) the transfer complies with any applicable cross border **transfer restrictions**; and

e) a fully executed written contract containing UK GDPR **approved third party clauses** has been obtained.

PART 4 - DEFINITIONS AND INTERPRETATION

"Automated Decision-Making" or "ADM"	when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The UK GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing;
"Automated Processing"	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 the individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing;
"Company Personnel"	all employees, workers, contractors, agency workers, consultants, directors, members and others;
"Consent"	agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them;
"Data Controller"	the person or organisation determining when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the UK GDPR. We are the Data Controller of all Personal Data relating to our Company Personnel and Personal Data used in our business for our own commercial purposes;
"Data Subject"	a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data;
"Data Privacy Impact Assessment" or "DPIA"	tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and must be conducted for all major system or business change programs involving the Processing of Personal Data;
"Data Protection Officer" or "DPO"	the person required to be appointed in specific circumstances under the UK GDPR. Where a mandatory DPO has not been appointed, this term means a data protection manager or other voluntary appointment of a DPO or refers to the Company data privacy team with responsibility for data protection compliance;
"EEA"	the 27 member states of the EU, plus Iceland, Liechtenstein and Norway;
"Explicit Consent"	means consent which requires a very clear and specific statement (not just action) and must be expressly confirmed in words;
"GDPR"	the General Data Protection Regulation ((EU) 2016/679) and any other directly applicable European Union regulation relating to data protection (for so long as and to the extent that the law of the European Union has legal effect in the UK)
"ICO"	The Information Commissioner's Office www.ico.org.uk
"Personal Data"	any information identifying a Data Subject or information relating to a Data Subject we can identify (directly or indirectly) from the data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Categories of Personal Data and Pseudonymised Personal Data but excludes anonymous data or data where the identity of an individual is permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about the person's actions or behaviour;

"Personal Data Breach"	any act or omission compromising the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards we or our third- party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach;
"Privacy Advisor"	Privacy Advisors represent the Privacy Network's legal advisors within the Saint-Gobain group for any question concerning Data Protection.
"Privacy Correspondent"	Privacy Correspondents represent the very structure of the Privacy Network within the Saint-Gobain group. They capture and coordinate Data Protection subjects within their scope. Every legal entity subject to GDPR must appoint one, but one person can take charge of these duties on behalf of several entities.
"Privacy by Design"	implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the UK GDPR;
"Privacy Notices", "Fair Processing Notices" or "Privacy Policies"	separate notices setting out information may be provided to Data Subjects when the Company 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;
"Processing" or "Process"	any activity involving the use of Personal Data. It includes 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;
"Pseudonymisation" or "Pseudonymised"	replacing information which directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so 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;
"Related Policies"	the Company's policies, operating procedures or processes related to this Policy and designed to protect Personal Data, available here: https://portal.saint-gobain.com/web/gbr/gdpr
"Special Categories of Personal Data"	information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric data for the purpose of uniquely identifying a natural person or genetic data, and Personal Data relating to criminal offences and convictions
"Secure File Transfer Service"	the Company's secure file transfer service in place from time to time, available here: https://portal.saint-gobain.com/web/sgts-uk-and-ireland/o365-one-drive
"UK GDPR"	the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019.