DATA PROTECTION POLICY

INTRODUCTION

Unity Doors Limited ("**we**", "**us**" or "**our**") needs to gather and use certain information about individuals. These can include customers, suppliers, business contacts, employees and other people that the organisation has a relationship with or may need to contact. They expect that we adopt adequate safeguards to ensure that information about them is kept confidential and is accessed only by authorised personnel and used for proper purposes.

This policy describes how this personal information must be collected, processed and stored to meet our data protection standards.

1 PURPOSE

1.1 The purpose of this policy is to ensure that we have an appropriate and consistent approach to protecting personal data used within our business activities, in accordance with the General Data Protection Regulation and, when enacted, the Data Protection Act 2018 (together referred to as the "**GDPR**").

1.2 Everyone who works for us has a duty to respect the confidentiality and integrity of any information and data that they access, and is personally accountable for safeguarding assets in line with this policy. This policy sets out the behaviours that are expected of our employees and third parties in relation to the collection, use, retention, transfer, disclosure and destruction of any personal data belonging to our customers and/or clients.

1.3 Non-compliance with this policy may expose us to complaints, regulatory action, fines, claims and/or significant reputational damage.

2 SCOPE

2.1 This policy applies to all of our staff, including consultants, agents and any third party ("**you**" or "**your**") who has access to personal data which is created or processed by us or on our behalf in order for us to deliver services and conduct business, including information received from or exchanged with external partners.

2.2 "**Personal data**" is any information about a living individual from which they can be identified such as name, ID number, location data, any online identifier, or any factor specific to the physical, physiological, genetic, mental, economic or social identity of that person. It does not include data where any potential identifiers have been removed (anonymous data) or data held in an unstructured file. Personal data may take a number of forms, including (but not limited to):

2.2.1 hard copy data held on paper;
2.2.2 data stored electronically in computer systems and mobile devices (e.g. smart phones);
2.2.3 communications sent by physical post or using email;
2.2.4 data stored using electronic media such as USB drives, disks and tapes; and
2.2.5 data stored in the cloud (e.g. file sharing sites) and social media.

2.3 There are "**special categories**" of more sensitive personal data which are more private in nature and therefore require a higher level of protection, such as genetic data, biometric data, sexual orientation, race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and health. For the purposes of this policy, special categories data will include any personal data collected about criminal convictions.

2.4 When we refer to "**processing**", this means anything from collecting, using, storing, transferring, disclosing, altering or destroying personal data.

3 YOUR RESPONSIBILITY TO COMPLY WITH THIS POLICY

3.1 You have a personal responsibility to comply with the GDPR and have a duty to familiarise yourself with the relevant policies and procedures to ensure that no individual or corporate breach can occur. Failure to comply with the GDPR could result in us facing huge financial penalties of up to €20m or 4% of our global group turnover (whichever the greater). In addition, we could face claims from people affected by a breach and significant reputational damage as a result of our breach of the GDPR. Any breach of this policy and/or related policies may result in disciplinary action.

4 GOVERNANCE

4.1 Our Data Protection Champion ("**DPC**") is responsible for overseeing this policy and may be able to assist you with any questions that you may have about the operation of this policy, the GDPR or if you have any concerns that this policy is not being followed. That post is held by Oliver Townsend, Director.

4.2 This policy must be read in conjunction with all of our other policies related to data protection, all of which are internal documents and cannot be shared with third parties, clients or regulators without prior authorisation from the DPC.

4.3 We may supplement or amend this policy by additional policies and guidelines from time to time. You will be notified by us of any changes to this policy.

4.4 Our management team will ensure that all of our staff who are responsible for the processing of personal data are aware of and comply with the contents of this policy. In addition, we will make sure that all third parties who are engaged to process personal data on our behalf are aware of and comply with the contents of this policy. Assurance of such compliance must be obtained from all third parties, whether companies or individuals, prior to granting them access to personal data controlled by us or otherwise permitting them to process any personal data on our behalf.

4.5 You must always contact the DPC in the following circumstances:

4.5.1 if you are **unsure of the lawful basis** which you are relying on to process personal data (including the legitimate interests that we rely on);

4.5.2 if you **need to rely on Consent** and/or **need to capture Explicit Consent**;

4.5.3 if you need to **draft Privacy Notices**;

4.5.4 if you are **unsure about the retention period** for the personal data being processed;

4.5.5 if you are **unsure about what security** or other measures you need to implement to protect personal data;

4.5.6 if there has been a **personal data breach;**

4.5.7 if you are **unsure on what basis to transfer personal data outside the European Economic Area** ("**EEA**");

4.5.8 if you need any assistance **dealing with any rights** invoked by a data subject;

4.5.9 whenever you are engaging in a significant **new, or change in, processing activity** which is likely to require a data protection impact assessment ("**DPIA**") or **plan to use personal data for other purposes** than what it was collected for;

4.5.10 if you plan to undertake any activities involving **automated processing** including profiling or automated decision-making;

4.5.11 if you need assistance for carrying out **direct marketing activities**; or

4.5.12 if you need **help with any contracts** or other areas in relation to sharing personal data with third parties.

5 DATA PROTECTION BY DESIGN

5.1 When designing new systems or processes and/or when reviewing or expanding existing systems or processes, you must ensure that they go through an approval process before continuing to ensure that all data protection requirements are identified and addressed.

5.2 In accordance with the GDPR, you must ensure that a DPIA has been carried out on any "high risk" processing activity for all new and/or revised systems or processes before it starts. High risk processing may involve: (i) large-scale processing of special categories of personal data, (ii) use of new or invasive technologies, or (iii) carrying out profiling activities.

5.3 We will endeavor to consult with a data protection subject matter expert during the course of completing any DPIA. Where applicable, our IT provider - ACS, as part of the IT system and application design review process, will cooperate with the data protection subject matter expert to assess the impact of any new technology uses on the security of personal data.

6 DATA PROTECTION PRINCIPLES

6.1 The GDPR is underpinned by the following data protection principles, which help to drive compliance:

Fairness and transparency	We must tell the customer, client or employee what we intend to do with their personal data (transparency) and must process that personal data in accordance with the description given to them (fairness). The description will be contained within a privacy policy, and one of the lawful grounds set out in the GDPR must apply (lawfulness).
Purpose limitation	We must specify exactly what the collected personal data will be used for, and limit the processing of it to only what is necessary to meet the specified purpose.
Data minimisation	We must not collect or store any personal data beyond what is strictly required.
Accuracy	We must have in place processes for identifying and addressing out-of-date, incorrect, incomplete and redundant personal data.
Storage limitation	We must, wherever possible, store personal data in a way that limits or prevents identification of any customer, client or employee. Personal data should not be retained for longer than necessary in relation to the purposes for which they were collected.
Security, integrity and confidentiality	We must use appropriate technical and organisational measures to ensure the integrity and confidentiality of personal data is maintained at all times.
Transfer limitation	We must not transfer personal data to another country without appropriate safeguards being in place.
Data Subject's rights and requests	We must make personal data available to data subjects, who are allowed to exercise certain rights in relation to their own personal data.
Accountability	We are responsible for and must be able to demonstrate compliance with the data protection principles listed above.

7 ACCOUNTABILITY

7.1 As detailed above, we must be able to demonstrate that all of the data protection principles (outlined above) are met for all personal data for which we are responsible.

7.2 It is the responsibility of all of our staff to implement appropriate measures to reduce the risk of them breaching the GDPR and to show that they take data governance seriously.

7.3 We have also put in place the following processes in order to demonstrate accountability:

7.3.1 operation of a data privacy governance structure through the appointment of a DPC;
7.3.2 maintaining an inventory of data processing activities;
7.3.3 implementing appropriate privacy notices;
7.3.4 obtaining appropriate consents;
7.3.5 applying appropriate organisational and technical measures to ensure compliance with the data protection principles;
7.3.6 carrying out DPIAs; and
7.3.7 creating a breach reporting mechanism.

8 HOW WE USE PERSONAL DATA

8.1 We use the personal data of our customers for a number of broad purposes. This may include:

8.1.1 the general running and business administration;
8.1.2 to provide goods or services to our customers; and/or
8.1.3 the ongoing administration and management of customer services.

8.2 The use of customer information should always be considered from their perspective and whether the use will be within their expectations or if they are likely to object. For example, it would clearly be within a customer's expectations that their details will be used by us to respond to a customer's request for information about the products and services on offer. However, it might not be within their reasonable expectations that we would then provide their details to third parties for marketing purposes without their consent.

8.3 We will process personal data in accordance with all applicable laws and applicable contractual obligations. More specifically, we will not process personal data unless at least one of the following requirements are met:

8.3.1 where **consent** has been given in respect of specific processing;
8.3.2 where processing is necessary for the **performance of a contract** to which the customer is a party;
8.3.3 to comply with our **legal obligations** (e.g. to prevent or detect a crime or fraud);
8.3.4 where it is in your **vital interests** (e.g. in a life or death situation, or disclosing pertinent information to emergency services in relation to a unconscious member of staff);
8.3.5 where it is necessary for the **performance of a task carried out in the public interest** or in the exercise of official authority vested in us (e.g. notifying the recipients of defective devices to relevant authorities); or
8.3.6 To pursue our (or a third party's) **legitimate interests** as a business, except where such interests are overridden by the interests or fundamental rights and freedoms of the customer.

8.4 There are some legitimate circumstances in which personal data may be further processed for purposes that go beyond the original purpose for which the personal data was collected.

9 HOW WE USE YOUR SPECIAL CATEGORIES OF PERSONAL DATA

9.1 In most cases where we process special categories of personal data, we will require the data subject's **explicit consent** to do so unless exceptional circumstances apply or to enable us to **perform our legal obligations** (e.g. to comply with health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

9.2 More specifically, we will only process special categories of personal data in accordance with the GDPR, including (but not limited to) where:

9.2.1 **explicit consent** has been given in respect of specific processing;
9.2.2 the personal data has been made public by the customer or employee;
9.2.3 it is required to establish, defend or exercise legal claims;
9.2.4 it is required to enable us to perform our legal obligations;
9.2.5 it is necessary for historical research or statistical purposes, and safeguards have been put in place to protect customers and/or employees; or
9.2.6 it is in your **vital interests**, or where the data subject is physically or legally incapable of giving their consent.

9.3 Where special categories of personal data are being processed, we will adopt additional measures to protect the data (e.g. encryption).

10 CONSENT

10.1 The GDPR sets a higher standard for consent. All staff must adhere to the rules on consent outlined in this section when relying this legal ground to process personal data. Guidance as to what constitutes 'lawful' consent is set out below.

10.2 "**Consent**" means offering people genuine choice and control over how you use their personal data. The personal data that we collect after receiving consent is subject to a data subject's continuing active consent (which means that consent can be revoked at any time).

10.3 Consent must satisfy the following criteria:

Unbundled	Requests for consent must be separate from other terms and conditions. Consent should not be a precondition of signing up to a service unless necessary for that service;
Active opt-in	Consent must be expressed by a statement or clear affirmative action. Silence, pre-ticked boxes or inactivity should therefore not constitute consent;
Granular	Granular options must be provided allowing data subjects to consent separately to different types of processing wherever appropriate;
Named	Anyone who will be recipients of the customer or employee's personal data (whether us or any third party) must be named;
Documented	It is necessary to keep records to demonstrate what the data subject has consented to, including what they were told, and when and how they consented (e.g. timestamp) and if and when they withdrew consent at any point. Documenting the date, method and content of the disclosures made, as well as the validity, scope, and volition of the consents given;
Easy to withdraw	Data subjects have the right to withdraw their consent at any time and it must be as easy for them to withdraw as it is to give consent at any time. This means simple and effective withdrawal mechanisms must be in place (e.g. unsubscribe link or contact number);

No imbalance in the relationship	Consent will not be freely given if there is imbalance in the relationship between the data subject and us. Consent from an employee will except in rare cases be invalid due to such imbalance; and
Plain Language	The language used to obtain consent must be intelligible, clear and simple.

11 DIRECT MARKETING

11.1 We are subject to certain rules and privacy laws when marketing to our customers. For example, a data subject's prior consent is required for electronic direct marketing (such as emails, text or automated calls). The limited exception for existing customers known as "soft opt in" allows organisations to send marketing communications 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.

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

11.3 A data subject's objection to direct marketing must be promptly honored. If a customer 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.

12 RIGHTS OF DATA SUBJECTS

12.1 Individuals have certain rights under the GDPR, including the right to request access to any data held about them by us. These rights, summarised in the table below, can be exercised at any time by a data subject (which includes customers or employees). Data subjects are not required to provide an explanation for engaging their right under GDPR.

Information access	Data subjects have a right to request a copy of their personal data being processed by us, together with supplementary information which includes information on the likely external recipients of the data, the retention periods in place (i.e. how long the information will be held for), the source of the data (where it has not originated from the data subject), the existence of other rights detailed in this section and the right to complain to the ICO;
Objection to Processing	Data subjects have the right to object, on grounds relating to their particular situation, to the processing of their personal data unless we can demonstrate that it either has compelling grounds for continuing the processing, or that the processing is necessary in connection with our legal rights;
Objection to automated decision making (including Profiling)	Data subjects have the right not to be subject to a decision based solely on automated processing (e.g., in connection with offers of employment; discounts; insurance premiums) which significantly affect them (including profiling). Such processing is permitted where it is necessary for entering into or performing a contract with the data subject provided that appropriate safeguards are in place, it is authorised by law or the data subject has explicitly consented and appropriate safeguards are in place. A common example of automated decision making would be the automatic refusal of an on-line credit application although this would be permitted in the context of a purchase (which constitutes entering into a contract for the sale of goods or a service);

Restriction of Processing	Data subjects have the right to restrict the processing of personal data (meaning that the data may only be held by us, and may only be used for limited purposes) if the accuracy of the data is contested (and only for as long as it takes to verify that accuracy), the processing is unlawful and the data subject requests restriction (as opposed to exercising the right to erasure), the data is no longer needed for its original purpose, but the data is still required by us to establish, exercise or defend our legal rights;
Data portability	A data subject has the right to receive a copy of their personal data in a common, structured electronic and reusable format. A data subject may also request that their data is transferred directly to another organisation;
Data rectification	We must ensure that inaccurate or incomplete personal data is erased or rectified; and
Right to be forgotten	A data subject may request that any personal data held on them is deleted or removed (except in limited circumstances, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

12.2 Requests (whether verbal or in writing) from customers should be forwarded as soon as possible to Dave Symonds in the HR Department.

12.3 Requests (whether verbal or in writing) from staff members should be forwarded as soon as possible to Dave Symonds in the HR Department.

12.4 In most cases you cannot charge a fee for complying with such a request. However, we may charge a reasonable fee for "repetitive requests", "manifestly unfounded or excessive requests" or "further copies". Guidance should be sought from the DPC in advance of charging such a fee to ensure it is justified accordingly and ensure a consistent approach.

12.5 You must ask data subjects to provide proof of identity before giving effect to their rights. This helps to limit the risk that third parties gain unlawful access to personal data.

12.6 You must fulfil a response to each request within 30 days of the receipt of the request from the data subject. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests.

12.7 Data subjects' requests may be subject to a series of exemptions which may result in a legal requirement to refuse to comply with a request. The only exception is the right to object to receiving direct marketing, which is an absolute right (meaning no exemption applies). You should seek advice from the DPC where you are unsure whether an exemption applies.

12.8 In certain circumstances, we are permitted to share information about data subjects with the police or agencies responsible for the investigation of crimes or fraud (e.g. HM Customs & Revenue). This can be done without the knowledge or consent of a data subject. This is the case where the disclosure of the personal data is necessary for any of the following purposes:

12.8.1 the prevention or detection of crime;
12.8.2 the apprehension or prosecution of offenders;
12.8.3 the assessment or collection of a tax or duty; or
12.8.4 by the order of a court or by any rule of law.

13 DATA QUALITY

13.1 You must ensure that the personal data you collect is complete and accurate in the first instance, and is updated to reflect the current situation of the data subject. All staff must take care when entering personal details onto any of our systems. Personal data (e.g. contact details) should be validated and/or updated wherever possible.

13.2 Personal data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if provided by the data subject (or known by them to be inaccurate) must be corrected.

14 DATA RETENTION

14.1 You should ensure that personal data relating to all data subjects is deleted or destroyed where there is no longer a reason to retain it.

14.2 The length of time for which we need to retain personal data is set out in our Data Retention Policy, which is available on request from the HR Department. This takes into account the legal and contractual requirements, both minimum and maximum, that influence the retention periods set forth in the schedule to that policy.

15 STORING DATA SECURELY

15.1 You must ensure that personal data is protected against undesired destruction or loss. You must ensure you have read, understood and comply with our policies relating to information security.

15.2 A summary of the personal data related security measures which you (including temporary workers) must abide by is provided below:

15.2.1 where personal data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it (e.g. locked cabinet or restricted rooms). Keys to such cabinets used to store such data must also be kept secure when not in use (e.g. key safe);

15.2.2 printed documents that contain personal data should be shredded or disposed of in a confidential waste bin or destroyed using an office shredder when it is no longer needed;

15.2.3 data stored on computers should be adequately password protected. Passwords must not be shared and should be kept confidential;

15.2.4 all computers, workstations, mobile devices, CDs and/or media storage devices (USBs) must always be securely locked (where appropriate) or locked away when left unattended and not in use;

15.2.5 data must be accessed only by those who are authorised to do so. You must only access personal data (in whatever form) strictly on a need-to-know basis and in the course of your normal business duties. User access logs will be maintained on all databases in accordance with pre-agreed retention periods. Inappropriately accessing customer or staff records or other personal data will not be tolerated and may result in disciplinary action;

15.2.6 you must accept and install all legitimate software and app updates on your computer or mobile device as soon as they are available. If you believe that your anti-virus software is not up to date, then you must promptly notify the IT helpdesk;

15.2.7 you must not open email attachments or click on web links embedded in suspicious emails or emails from unfamiliar senders. It is important that you check the email address. For example, if you receive an e-mail from Apple and the sender's address is AppleSupport765@hotmail.com, this is clearly not really from Apple. If you do click on a suspicious attachment then you must disconnect your device from the internet by switching off Wi-Fi and/or removing the Ethernet cable and report the incident immediately to the IT helpdesk;

15.2.8 any data relating to or owned by us (including personal data) must not be stored on a personal device unless expressly permitted to do so;

15.2.9 servers containing personal data must be kept in a secure location, away from general office space;

15.2.10 The DPC along with the IT provider must approve any cloud used to store any personal data.

15.3 Encrypting data whilst it is being stored (e.g. on a laptop, mobile, USB or back-up media, databases and file servers) provides effective protection against unauthorised or unlawful

processing. Personal data of any kind relating to our business should never be saved to mobile devices such as laptops, tablets or smartphones without appropriate and adequate encryption (such encryption should be enabled by default). Where possible, our data (including any personal data) should only be stored temporarily on these devices and transferred to our network as soon as possible. This is to ensure the on-going availability of information in the event of damage or loss of a laptop.

15.4 You must use appropriate measures (such as encryption) when sending emails containing any personal data. Any email containing special categories of personal data (which could be included in the title, body or within an attachment) sent to any third party should be sent as with adequate encryption. You must exercise care when sending emails containing personal data and must promptly report incidents when an email containing personal data is sent to an incorrect recipient in error.

16 BREACH REPORTING

16.1 All members of staff (including temporary workers) have an obligation to promptly report actual or potential data protection breaches or compliance failures. Any individual who suspects that a personal data breach has occurred must immediately notify their line manager or the DPC.

16.2 A personal data breach may be caused by a number of events, including (but not limited to):

16.2.1 theft of a laptop;
16.2.2 loss of a USB;
16.2.3 emailing incorrect recipients or “Cc’ing” to unauthorised recipients;
16.2.4 failing to collect printed documents straight away, which may contain personal data;
16.2.5 phishing or vishing attack allowing a third party to access company systems or records;
16.2.6 malicious hacking; and/or
16.2.7 accessing HR records without having the authority to do so.

16.3 All companies which process personal data are subject to a formal data breach notification process under the GDPR. This is summarised as follows:

16.3.1 if we are processing personal data on behalf of a third party company as a data processor, all personal data breaches must be reported to the DPC and that third party, without undue delay, regardless of the severity of the breach and regardless of whether or not we have sufficient information to determine the severity of the breach; and

16.3.2 where we are the data controller of personal data, any personal data breach must be reported to the DPC without delay. The DPC in consultation with the key stakeholders (e.g. senior management team, IT provider) will evaluate the severity of the breach and determine whether the breach should be reported to the ICO within 72 hours of becoming aware of the breach. In some cases, affected data subjects will also need to be advised of the personal data breach.

17 OUTSOURCING/SUPPLIERS

17.1 **Suppliers.** Any of our suppliers who have access to personal data must guarantee in writing that they comply with the GDPR. We will only transfer personal data or allow access to third parties when it is assured that any such personal data will be processed legitimately and protected appropriately by the third party recipient.

17.2 **Contracts.** We will enter into an appropriate agreement with a third party to clarify each party’s responsibilities in respect to the personal data transferred and/or otherwise processed. The agreement must require the third party to protect the personal data, promptly

report data breaches to us and to only process personal data in compliance with our instructions.

17.3 **Transfers of data outside the European Economic Area ("EEA").** You must not allow personal data to be transferred to any individual or company located outside the EEA without the prior written approval of the DPC. This also applies where a company uses equipment, resources or a subcontractor located outside the EEA to process personal data. The DPC may require certain conditions to be met or safeguards to be in place before any personal data can be transferred outside of the EEA.

17.4 **Audits.** Regular audits of third parties handling our data (including any personal data), especially in respect of information security measures they have in place, must be undertaken. Any major deficiencies identified will be reported to and monitored by our DPC.

18 DATA PROTECTION TRAINING

All appropriate staff will receive training on this policy, and new joiners will receive IT security and Data Protection policy information as part of the induction process.

19 COMPLAINTS HANDLING

19.1 Any individual with a complaint about the processing of their personal data should put their complaint in writing to us. An investigation of the complaint will be carried out by the DPC in consultation with the relevant business owner to the extent that is appropriate based on the merits of the specific case. We will inform the complainant of the progress and the outcome of the complaint within a reasonable period.

19.2 If the issue cannot be resolved through consultation with the complainant, then the complainant should be advised that they may, at their discretion, complain to the Information Commissioner's Office (ICO).

20 DEROGATIONS

20.1 Any derogations from the requirements of this policy shall require prior written approval from the DPC.