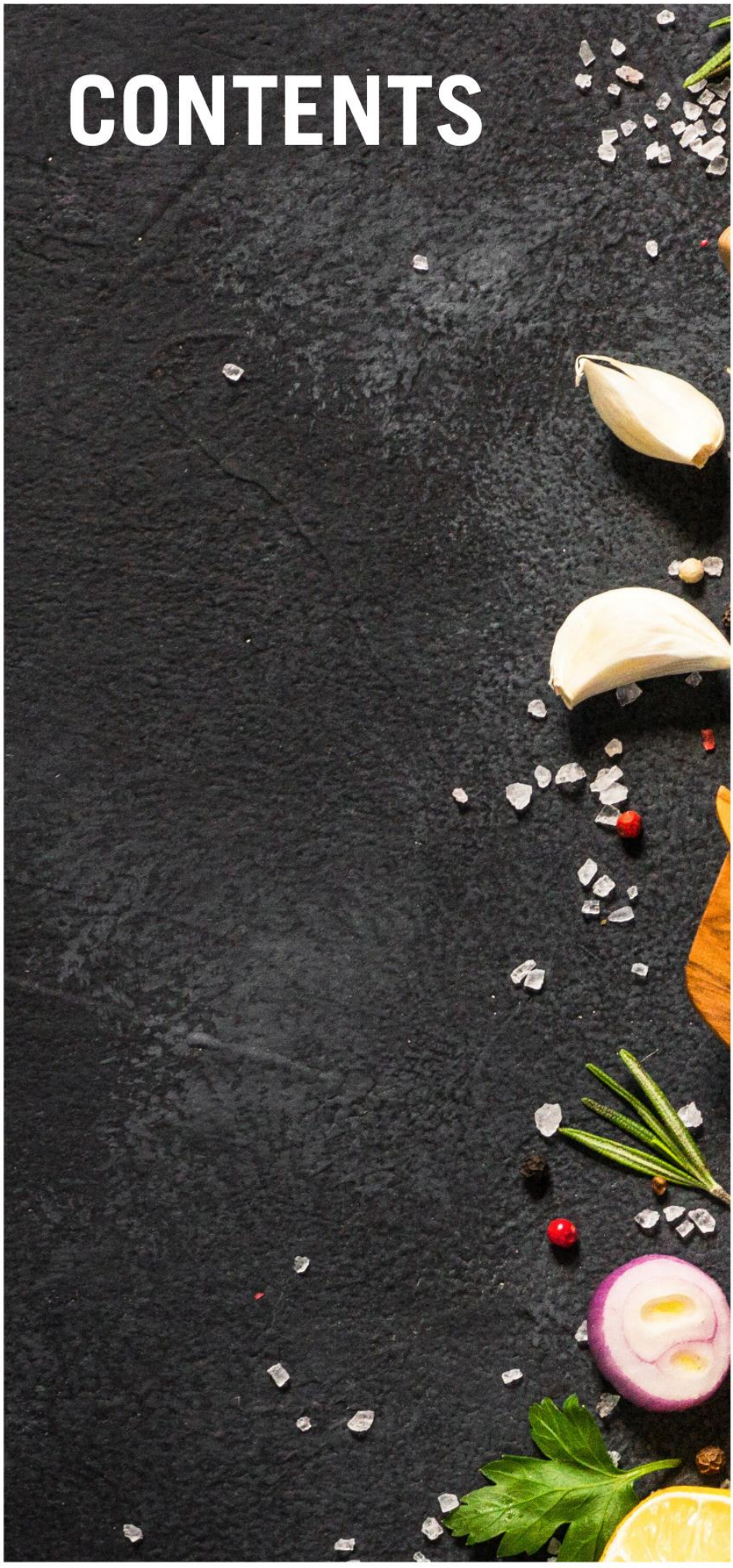
COMPASS GROUP

GLOBAL PRIVACY POLICY

APRIL 2025

CONTENTS



PURPOSE AND SCOPE

The Compass Group Privacy Policy (this "**Policy**") applies to Compass Group PLC (collectively, "**Compass**", "us" or "we") and all "**Compass Personnel**" (individually and collectively "**you**").

This Policy relates to personal information Compass collects or processes across our business activities and interactions with our stakeholders. Our stakeholders include customers, consumers, business partners, suppliers, investors, and other people Compass does business with.

WHAT IS DATA PRIVACY?

Data privacy relates to the protection of Personal Identifiable Information or Personal Data (**PII**). PII means information that relates to a living person or information that can be used, alone or in combination with other information, to identify a living person.

Examples of PII may include forenames and surnames, addresses, date of birth, personal identification numbers, allergen information, gender, age, ethnicity, religious beliefs, health or medical records, IP addresses, personal bank account details, company user ID. Please note that the information that constitutes PII can differ in different countries, so if unsure check with your country Legal team or Privacy Lead.

Data privacy and the protection of PII is very important to Compass. We are committed to compliance with applicable data privacy laws and recognise we have a regulatory, ethical and contractual responsibility (where applicable) to protect and safeguard the PII we hold of our stakeholders. Privacy compliance forms part of how we uphold Compass's core values and maintain a reputation as a responsible business underpinned by strong governance.

PURPOSE AND SCOPE CONTINUED

WHO DOES THIS POLICY APPLY TO AND WHAT DOES IT DO?

Privacy compliance is a responsibility for everyone at Compass. We all play an important role in the implementation of this Policy and Compass's compliance with data privacy laws. This includes, amongst other things, identifying and escalating privacy risks, actual or suspected data incidents, data losses and local Privacy Policy violations to your Line Manager or Legal team representative. It is important we all adopt, practise and cultivate the culture and behaviours as outlined in this Policy.

This Policy contains the general principles necessary to enable us to identify, assess and appropriately manage privacy risks. These principles ensure the lawful and compliant use of PII, including the prevention of its unauthorised use, disclosure or access.

In certain countries, the application of all the elements of this Policy may not be required under local laws or regulations, though some elements may be required under contractual obligations with other parties.

We require all Compass Personnel to comply with our Data Privacy Principles and act in accordance with our Code of Business Conduct promoting ethical and responsible practices in relation to privacy and the management of PII within our business.

The expectations set out within this Policy contain the framework within which your local Management Team are required to implement their own Privacy Policy in addition to any country specific data protection policies, standards and processes.

Compliance with this Policy is monitored by our Group Data Privacy Programme Minimum Reporting Standards.

PRIVACY PRINCIPLES

The Data Privacy Principles set out below must be followed by all Compass Personnel:

1. **Lawfulness, fairness and transparency** - where we process PII we do so in a manner that is clear and transparent, strikes an ethical balance between the individual's right to privacy (observing any individual rights of access they may have) and Compass Group's legitimate business interests, and which is in compliance with applicable data privacy laws;

2. **Purpose limitation** - We are clear on the purpose of any PII collected or used to undertake a business activity. We should not collect PII because it would be 'nice to have'. Any PII we collect is necessary for the purposes for which we need to use it, we do not collect any more PII than we need, and we have appropriate controls in place to ensure that the PII we are collecting is accurate and will not be used for further incompatible purposes;

3. **Data minimisation** – We only collect PII if necessary for the purposes for which it is processed and only if that purpose could not reasonably be fulfilled by other means. Where viable, we seek to collect and process, only anonymized, deidentified, or aggregate information instead of PII;

4. **Accuracy** – PII must be kept accurate and up to date;

5. **Storage limitation** – PII must not be stored for longer than is necessary for the purpose for which the PII is processed and in compliance with your local Retention Policy/Principles;

6. **Data security** – PII must be processed in a manner that ensures the confidentiality, integrity and availability of PII including protection against unauthorised access, accidental loss, destruction or damage. Where we may share PII with authorised third parties, we undertake third party due diligence and implement appropriate controls to manage any privacy risks;

7. **Accountability** - Compass shall be responsible for, and be able to demonstrate compliance with, these Data Privacy Principles and applicable data privacy laws.

These Data Privacy Principles are the minimum standards you must comply with. Your local data privacy laws may set out additional or more stringent obligations, in which case those more stringent local data privacy laws must be complied with. If you are unsure, please consult your local Privacy Policy for further details.

1 Lawfulness, fairness, and transparency

Where Compass processes PII we must ensure that we do so in a manner that is clear and transparent, strikes an ethical balance between the right to privacy of the individual and Compass's legitimate business interests, and is compliant with applicable data privacy laws.

As a global business, we may need to transfer PII across country borders (including to other Compass businesses). Where we transfer PII internationally, we must do so with adequate protections and safeguards in place, as required by applicable data privacy laws, and as a minimum in accordance with the requirements of the Group Data Sharing Agreement.

Our Expectations

- PII must only be processed where Compass has lawful grounds to do so in compliance with applicable data privacy laws. Such grounds may include, where necessary for the performance of a contract with the individual, where required to comply with our legal obligations, where we have a legitimate business purpose or where the individual has consented to such use.
- Prior to any processing, we must provide to individuals a clear and transparent notice in a manner such that they understand about: (i) the type of PII we collect about them, (ii) the intended processing of their PII, and (iii) the purpose for such processing ("**Privacy Notice**"). This Privacy Notice must be updated if we need to use the PII collected for additional purposes than originally intended.
- Whenever Compass is required to process children's PII, additional safeguards must be applied to protect them. We must take all reasonable measures to ensure that appropriate consent has been obtained before the processing can take place.
- Certain categories of PII are considered **Special Categories** of PII or **Protected Characteristics** as these are more sensitive and require extra care. We will only process Special Categories of PII if; (i) we have complied with any obligations required under applicable data privacy laws, including obtaining explicit consent where relevant; or (ii) processing is necessary for carrying out a legal obligation under applicable local laws (e.g., to meet Health and Safety requirements). If you are unsure about what you should do, please contact your Privacy Lead.

What You need to do

- There may be occasions where we need to undertake High-Risk Processing Activities which includes: (i) processing of Special Categories of PII; (ii) processing PII about vulnerable people (which can vary depending on country, but can include children, the elderly, or those with disabilities); (iii) processing PII based on automated decision making or profiling; (iv) processing PII on a large scale [1]; (v) monitoring public areas through video surveillance; and (vi) new and innovative use of technology/AI. Prior to undertaking any High-Risk Processing Activity, you must assess the impact such processing will have on individuals and record such assessment in writing (known as a "**Data Protection Impact Assessment**" or "**DPIA**"). Where local data privacy laws prohibit processing activities that present a high level of risk, then such processing must not be undertaken. If you are unsure whether to continue with the activity speak to your Privacy Lead or a member of your country Legal team.
- Consult with your country Legal team (or your Regional General Counsel where there is no country Legal team) to prepare a **Privacy Notice** prior to undertaking any processing activities. The Privacy Notice should set out

[1] When determining whether processing is on a large scale you should consider: (i) the number of individuals concerned; (ii) the volume of data; (iii) the variety of data; (iv) the duration of the processing; and (v) the geographical extent of the processing

an overview of the processing activities relating to the PII being collected and all the information required by local data privacy laws.

- Prior to processing any children's PII, speak with your country Legal team to implement necessary measures and controls to demonstrate that appropriate consent has been obtained. We must stop processing a child's PII if consent is withdrawn either by the individual or their legal representative.
- Where we process Special Categories of PII on behalf of another organisation (e.g. a healthcare provider or school), we must ensure that our processing of that PII is compliant with applicable data privacy laws e.g. that the other organisation has obtained any required consents before we can process the PII and that the organisation has given written instructions on how to process the PII. If it has not, we should either refrain from processing such PII or where possible obtain consent ourselves directly from the individuals and issue them with a Privacy Notice.
- Where we process PII for our clients, we should assist them in meeting their privacy obligations. This involves providing our clients with information about how Compass processes PII on their behalf.
- Where we may need to transfer PII to another business in the Compass Group or to a third party located in another jurisdiction, you must consult your country Legal team to ensure that any transfers of PII are in compliance with this Policy, their applicable data privacy laws and all applicable contractual obligations. A transfer of PII to another jurisdiction could include: (i) access of PII from another jurisdiction; (ii) storage of PII on a database hosted in another jurisdiction; (v) communicating PII to another jurisdiction over the telephone, by email or other application or in person; or (vi) use of PII from another jurisdiction through external solutions such as a cloud platform.
- Consult with your Line Manager, country Legal team or HR team in a timely manner where you think you have received a request from an individual to exercise their privacy rights. Please consult your local Privacy Policy for further details on this process.

2, 3 & 4 Purpose Limitation, Data Minimisation and Accuracy

Compass must be clear on the purpose of any PII collected or used to undertake a business activity. We should not collect PII because it would be 'nice to have'. Stakeholders of our business expect that any PII we collect is necessary for the purposes for which we need to use it, we are not collecting any more PII than we need, and we have appropriate controls in place to ensure that the PII we are collecting is accurate.

Our Expectations

- Prior to the collection of any PII, determine what is the purpose for which that PII will be processed and consider whether it is reasonably necessary to achieve the business purpose.
- Any processing of PII that is incompatible with the original purpose that it was collected for must be approved by the Privacy Lead. In some cases, applicable data privacy laws or regulatory guidance may require renewed consent by individuals, a revised DPIA, and an updated Privacy Notice.
- Implement appropriate controls to ensure that PII is accurate and, where necessary, kept up to date. Such controls should be reviewed regularly.
- HR Directors, with support from the Legal and Digital & Technology Services teams, shall be responsible for ensuring appropriate systems and procedures are in place to process Compass Personnel PII.

What You need to do

- Where appropriate, you should seek to collect and process only anonymized, deidentified, or aggregate information instead of PII. Where we don't need PII, don't collect it.
- Before undertaking any new business activity, ask the following questions: (i) do we need the PII to carry out or enable the business activity; (ii) can we undertake the same activity in the same way without PII; (iii) is all the PII we are collecting for the activity necessary?
- Regularly review activities you undertake that collect and process PII. Do you still require the PII to undertake the activity, is the PII still accurate and up to date?
- Ensure appropriate controls are in place when processing PII to maintain its accuracy (e.g., access controls, password protection, enhanced encryption). Review these controls regularly to maintain their adequacy.

5 Storage Limitation

PII should never be retained longer than is necessary to achieve the purpose for which it was collected and should periodically be deleted when no longer required. Appropriate measures should be put in place to ensure that Compass systematically and regularly reviews the PII it holds and removes any PII no longer required. In some circumstances this may result in the reduction of categories of PII that are retained.

Our Expectations

- Stakeholders do not expect us to retain their PII indefinitely. We should not keep PII for longer than necessary or as required by local law (e.g., tax and social security laws, statutory limitation periods).
- A Data Retention Policy or Data Retention Principles should be produced by Local Management and implemented appropriately (such as by updating system configuration, rules or policies) to determine specific retention periods that reflect any local legal requirements as well as business needs. Such retention periods must be regularly reviewed.
- Maximum retention periods must be set prior to processing PII. Once a retention period has been reached, PII should be deleted, destroyed or put beyond use.

What You need to do

- You should familiarise yourself with your local Data Retention Policy or Data Retention Principles and time periods contained within it.
- Prior to undertaking any new business activity that involves PII, ask yourself why Compass needs such PII; and how long do we need to retain it?

6 Data Security

Where we process PII, we must ensure that we have adopted appropriate measures to ensure the integrity, availability and confidentiality of PII. Individuals expect us to keep their PII safe and secure and prevent it from unlawful or unauthorised access, loss, and destruction.

Where we may share Compass PII with authorised third parties, we must undertake third party due diligence to identify privacy risks. This allows us to better understand and manage data privacy risks, which in turn reduces the risk of fines or other enforcement, and damage to the Compass brand, and stakeholders' trust.

Our Expectations

- Appropriate measures must be adopted to ensure the integrity, availability and confidentiality of PII. This will include protection against unauthorised or unlawful processing and against accidental loss, alteration, destruction or damage, using appropriate technical or organisational measures including compliance with the Group's Key IT Controls, the Information Classification Policy and any local requirements.
- The Group Chief Information and Security Officer (CISO) shall design a framework for such data security measures. Country Management shall be responsible for implementing such measures and review their implementation with the Privacy Lead on a regular basis against the Group Minimum Reporting Standards and the Group's Key IT Controls.
- As appropriate, sensitive and highly sensitive data is to be encrypted both at rest and in transit, and access controlled at all times.
- When transferring or giving access to PII to authorised third parties, we must ensure that such third parties have adequate safeguards and procedures in place to protect the PII being handled.

What You need to do

- Be conscious of the confidentiality of PII and adopt appropriate working practices to maintain such confidentiality e.g., lock your PC when you are not at your desk, do not leave PII in hard copy in shared areas including kitchens and Front of House, and ensure any hard copy documentation containing PII is disposed of appropriately via confidential shredding or other destruction techniques.
- Ask yourself whether you consider if any PII that you handle as part of your role needs additional security. Think about how you would feel if it was your PII.
- When sharing PII both internally and to authorised third parties ensure appropriate safeguards are included for such transfer e.g., enhanced email encryption, document password protection, anonymisation or obfuscation methods.
- Document your assessment of the safeguards and procedures to protect Compass PII by third parties. Work with your local Legal team to ensure appropriate contractual terms are in place with that third party in relation to privacy and security, including any contractual terms that are mandated by applicable data privacy laws.

7 Accountability

Compass is accountable for how it uses PII. We are accountable to you and our other stakeholders to ensure that we process PII in accordance with the Data Privacy Principles.

In the event of the unauthorised access, use, loss, or acquisition of PII (also referred to as a "**Data Privacy Incident**"), a Compass entity may be required under applicable data privacy laws to inform their applicable Regulator. Similarly, we may be required to inform individuals about certain Data Privacy Incidents that may affect them. In addition to these regulatory obligations, we may also be under contractual obligations to report actual or suspected Data Privacy Incidents to our other stakeholders such as vendors and clients.

Our Expectations

- Due consideration to privacy in relation to all aspects of our business (privacy by design and default).
- Consideration of the Data Privacy Principles is required before the implementation of a new or change to an existing business process and/or IT system that involves the processing of PII.
- All personnel must receive adequate training to handle and process PII, to identify any actual or potential Data Privacy Incident, to comply with Compass's notification process and to report potential or actual Data Privacy Incident upon identification.
- Prior to processing any PII, any third party that processes PII on our behalf must receive written instructions from Compass which provides the parameters upon which the third party may handle and process PII and comply with Compass's notification process and to report any potential or actual Data Privacy Incident upon identification.
- Regular review of your privacy policy and procedures which as a minimum, should be every 3 years.

What You need to do

- If you think you have committed or have encountered a Data Privacy Incident, please notify your Line Manager or Legal team as soon as possible. Line Managers are responsible for escalating a Data Privacy Incident to the appropriate Privacy Lead in accordance with your local Data Privacy Incident process.
- Local Country Management Teams including any appointed Privacy Lead/Data Protection Officer (DPO) are responsible for determining the severity of a Data Privacy Incident. Depending on the severity of the Data Privacy Incident a notification may be required to the Director of Data Privacy, Group Ethics & Integrity. For further information regarding the reporting thresholds, please refer to your Country or Regional General Counsel.
- In the event of a Data Privacy Incident, your Local Privacy Lead/DPO are responsible for determining whether additional notifications are required to individuals or the Regulator.
- Any high-risk processing activities, unlawful processing (see section 1 above), or other serious non-compliance with this Policy, must be notified to your Country General Counsel or if one doesn't exist your Regional General Counsel. The Regional General Counsel are responsible for escalating such activities to the Director of Data Privacy and the Group Head of Ethics and Integrity (as appropriate) depending on the severity and scale of the activity.
- In the event of serious non-compliance with this Policy, an assessment of such non-compliance and remedial action plan will be agreed between the Director of Data Privacy, Group Head of Ethics and Integrity and the Country Management Team including determining whether additional notifications are required to individuals or regulators.

Glossary

Compass Personnel	meaning all directors and officers, employees, workers, contractors, and consultants working for or at any Compass business anywhere in the world, whether permanent, fixed term or temporary.
Consent	must be a freely given, specific, informed, and unambiguous indication of an individual's wishes. This shall signify agreement to the processing of PII for the purpose for which Compass or Compass clients have informed the individual. Under some applicable Data Privacy Laws, consent must be given through an "opt-in" affirmative action, rather than an "opt-out".
Data Privacy Incident	unauthorized access, use, loss or acquisition of PII.
High-Risk Processing Activities	(i) processing of Special Categories of PII; (ii) processing PII about vulnerable people (which can vary depending on country, but can include children, the elderly, or those with disabilities); (iii) processing PII based on automated decision making or profiling; (iv) processing PII on a large scale; (v) monitoring public areas through video surveillance; and (vi) new and innovative use of technology /AI.
Personal Identifiable Information or Personal Data (PII)	PII is information relating to natural persons who: • can be identified or who are identifiable, directly from the information in question; • or can be indirectly identified from that information in combination with other information. Examples of PII may include forenames and surnames, addresses, date of birth, personal identification numbers, allergen information, gender, age, ethnicity, religious beliefs, health or medical records, IP addresses, personal bank account details, company user ID. Please note that the information that constitutes PII can differ in different countries, so check your local Privacy Policy.
Privacy Notice	a clear and transparent notice must be provided to individuals in a manner such that they understand about: (i) the type of PII we collect about them, (ii) the intended processing of their PII, and (iii) the purpose for such processing.
Processing	Processing has a wider meaning than you may think and relates to any operations or set of operations performed on PII, whether by automated means or manually. Processing includes using, collecting, recording, organising, structuring, storing, adapting, or altering, retrieving, disclosing, aligning or combining, restricting, erasing and destroying PII.
Profiling	Profiling means any form of automated processing of PII consisting of the use of PII to evaluate certain personal aspects relating to a natural person's performance, capability, preference, economic situation, health interest, reliability, behaviours, location and/or movement.
Special Categories of PII or Protected Characteristics	These include racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data, and data concerning health and allergen information, or sex life or sexual orientation of that individual.