# Komfort Partitioning Limited
# GDPR Compliance and Privacy Policy

| Authorised and owned by: | Signature | Date | Review |
|---|---|---|---|
| John Cowdell, Compliance Officer | | April 2021 | April 2022 |

**Contents**



## 1. Purpose and scope

The ***EU General Data Protection Regulation ("GDPR")*** came into force across the European Union on 25thMay 2018 and brings with it the most significant changes to data protection law in two decades. Based on privacy by design and taking a risk-based approach, the GDPR has been designed to meet the requirements of the digital age.
The 21st Century brings with it broader use of technology, new definitions of what constitutes personal data, and a vast increase in cross-border processing. The new Regulation aims to standardise data protection laws and processing across the EU; affording individuals stronger, more consistent rights to access and control their personal information.

This GDPR policy ensures Komfort Partitioning :-

- Complies with data protection law and follows good practice.
- Protects the rights of staff, clients and interested parties.
- Is open about how it stores and processes individuals' data.
- Protects itself from data protection risks such as breaches of confidentiality, failure to offer choice and reputational damage.

This policy applies to:-

- All staff of Komfort Partitioning
- All contractors, suppliers and other people working on behalf, or have an interest in Komfort Partitioning.

## 2. Our commitment

**Komfort Partitioning** are committed to ensuring the security and protection of the personal information that we process, and to provide a compliant and consistent approach to data protection. We have always had a robust and effective data protection program in place which complies with

existing law and abides by the data protection principles. However, we recognise our obligations in updating and expanding this program to meet the demands of the GDPR.

**Komfort Partitioning** are dedicated to safeguarding the personal information under our remit and in developing a data protection regime that is effective, fit for purpose and demonstrates an understanding of, and appreciation for the new Regulation. Our preparation and objectives for GDPR compliance have been summarised in this statement and include the development and implementation of new data protection roles, policies, procedures, controls and measures to ensure maximum and ongoing compliance

## 3. How we comply with GDPR

**Komfort Partitioning** already have a consistent level of data protection and security across our organisation, however it is our aim to be fully compliant with the GDPR.
***Our preparation includes: –***

- ***Information Audit*** – carrying out a company-wide information audit to identify and assess what personal information we hold, where it comes from, how and why it is processed and if and to whom it is disclosed.
- ***Policies & Procedures –*** we have revised our data protection policies and procedures to meet the requirements and standards of the GDPR and any relevant data protection laws, further information can be found in section 9 of this policy.
- ***Legal Basis for Processing*** – we are reviewing all processing activities to identify the legal basis for processing and ensuring that each basis is appropriate for the activity it relates to. Where applicable, we also maintain records of our processing activities, ensuring that our obligations under Article 30 of the GDPR and Schedule 1 of the Data Protection Bill are met.
- ***Privacy Notice/Policy*** – we have revised our Privacy Notice(s) to comply with the GDPR, ensuring that all individuals whose personal information we process have been informed of why we need it, how it is used, what their rights are, who the information is disclosed to and what safeguarding measures are in place to protect their information.
- ***Obtaining Consent*** – we have revised our consent mechanisms for obtaining personal data, ensuring that individuals understand what they are providing, why and how we use it and giving clear, defined ways to consent to us processing their information. We have developed stringent processes for recording consent, making sure that we can evidence an affirmative opt-in, along with time and date records; and an easy to see and access way to withdraw consent at any time.

- ***Direct Marketing*** – we have revised the wording and processes for direct marketing, including clear opt-in mechanisms for marketing subscriptions; a clear notice and method for opting out and providing unsubscribe features on all subsequent marketing materials.
- ***Data Protection Impact Assessments (DPIA)*** – where we process personal information that is considered high risk, involves large scale processing or includes special category/criminal conviction data; we have developed stringent procedures and assessment templates for carrying out impact assessments that comply fully with the GDPR's Article 35 requirements. We have implemented documentation processes that record each assessment, allow us to rate the risk posed by the processing activity and implement mitigating measures to reduce the risk posed to the data subject(s).
- ***Processor Agreements*** – where we use any third-party to process personal information on our behalf (*e. Payroll, Recruitment, Hosting etc*), we have drafted compliant Processor Agreements and due diligence procedures for ensuring that they (*as well as we*), meet and understand their/our GDPR obligations. These measures include initial and ongoing reviews of the service provided, the necessity of the processing activity, the technical and organisational measures in place and compliance with the GDPR.
- ***Special Categories Data –*** where we obtain and process any special category information, we do so in complete compliance with the Article 9 requirements and have high-level encryptions and protections on all such data. Special category data is only processed where necessary and is only processed where we have first identified the appropriate Article 9(2) basis or the Data Protection Bill Schedule 1 condition. Where we rely on consent for processing, this is explicit and is verified by a signature, with the right to modify or remove consent being clearly signposted.

## 4. Legal processing

Under the GDPR, there is requirement to have a valid lawful basis in order to process personal data. There are six available lawful bases for processing set out in Article 6 of the GDPR:-

(a) Consent: the data subject has given clear unambiguous consent for their personal data to be processed for a specific purpose

(b) Contract: processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract
(c) Legal obligation: processing is necessary for compliance with a legal obligation.
(d) Vital interests: processing is necessary to protect the vital interests of a data subject or another individual.
(e) Public task: processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
(f) Legitimate interests: processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

## 5. Data Subject rights

In addition to the policies and procedures mentioned above that ensure individuals can enforce their data protection rights, we provide easy to access information via contacting our office of an individual's right to access any personal information that **Komfort Partitioning** processes about them and to request information about: –

- What personal data we hold about them
- The purposes of the processing
- The categories of personal data concerned.
- The recipients to whom the personal data has/will be disclosed.
- How long we intend to store your personal data for
- If we did not collect the data directly from them, information about the source.
- The right to have incomplete or inaccurate data about them corrected or completed and the process for requesting this.
- The right to request erasure of personal data (*where applicable*) or to restrict processing in accordance with data protection laws, as well as to object to any direct marketing from us and to be informed about any automated decision-making that we use.
- The right to lodge a complaint or seek judicial remedy and who to contact in such instances.

The right to erasure enables an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

Individuals have a right to have personal data erased and to prevent processing in specific circumstances:-

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed.
- The personal data has to be erased in order to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a child.

There are some specific circumstances where the right to erasure does not apply and the company can refuse to deal with a request. This is where the personal data is processed:

- To exercise the right of freedom of expression and information.
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- For public health purposes in the public interest.
- For archiving purposes in the public interest, scientific research historical research or statistical purposes; or
- For the exercise or defence of legal claims.

If the company has disclosed the personal data to others, it must contact each recipient and inform of the erasure of the personal data – unless this proves impossible or involves disproportionate.

## 6. Information security and technical measures

**Komfort Partitioning** takes the privacy and security of individuals and their personal information very seriously and take every reasonable measure and precaution to protect and secure the personal data that we process. We have robust information security policies and procedures in place to protect personal information from unauthorised access, alteration, disclosure or destruction and have several layers of security measures, including:

**SSL,** access **controls, password policy, encryptions, pseudonymisation, practices, restriction, IT, authentication**

Komfort Partitioning works in partnership with several external IT companies to provide help and security of our cloud based servers and as IT support within our day to day activities. These companies also carry out penetration testing and offer advice on our IT security.

## 7. GDPR roles and responsibilities

Komfort Partitioning have designated Data Protection Officer (DPO)/Appointed Person and have appointed a data privacy team to develop and implement our roadmap for complying with GDPR. The team are responsible for promoting awareness of the GDPR across the organisation, assessing our GDPR readiness, identifying any gap areas and implementing the new policies, procedures and measures.
Komfort Partitioning understands that continuous employee awareness and understanding is vital to the continued compliance of the GDPR and have involved our employees in our preparation plans. We have implemented an employee training program specific to the Company which will be provided to all relevant employees and forms part of our induction and annual training program.
If you have any questions about our preparation for the GDPR, please contact our Data Protection Officer (DPO)/Appointed Person

## 9. Policies and Procedures

***All Komfort employees are to read and sign the Policies stated below:***

***BMSF281 – Data Security Policy***

***BMSF285 – Password Policy***

.

***BMSF287 – Clear desk and Screen Policy***

***BMSF288 – Mobile and Teleworking Policy***

***BMSF304 – Access Control Policy*** –

***BMSF305 – Acceptable Use Policy***

***BMSF306 – IT Management Operating Procedure***

***BMSF324 – Incident Response plan***

***BMSF336 – Privacy Policy***

| Revision | Details of Revisions | By Whom | Date |
|---|---|---|---|
| 01 | First draft | John Cowdell | April 2021 |
| 02 | | | |
| 03 | | | |
| 04 | | | |