General Data Protection Regulation (GDPR)

Customer Guidance Instruction

Introduction

From May 25 2018, The General Data Protection Regulation (GDPR) will become enforceable. This has been introduced by The European Union, which has taken a monumental step in protecting individual rights in regards to data privacy. Think Office ensures data will be processed in accordance with the General Data Protection Regulation, as protecting your data is important to us. This is to safeguard the privacy of individuals who provide Think Office with personal information. The compliance encompasses any activities carried out or on behalf of Think Office by third party suppliers.

As part of Think Office commitment to GDPR compliance, Think Office has ensured that all third party suppliers approach the GDPR in a vigorous and unfailing manner in the management and security of personal data. These requirements take the relevant data protection legislation into account, including but not limited to:

- Data Protection Act 1998;
- Regulation 2016/679 of the European Parliament and of the Council of the European Union of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and the repealing Directive 95/46/EC, and any successor laws arising out of the withdrawal of a member state from the European Union (General Data Protection);
- Privacy and Electronic Communication (EC Directive) Regulations 2003 (SI2003/2426)

Guidelines

For the purpose of this document and our continuing relationship, Think Office will be classified as the data processor, you as the customer will be the data controller, under GDPR regulations.

Where used, the terms in reference to “data subject”, “personal data”, “data controller”, “process”, “data processor” and “supervisory authority” will bear their corresponding meanings specified in the General Data Protection Regulation.

Processing

personal data By purchasing a product from Think Office, you as the customer, have agreed to enter into a contractual agreement with Think Office. This will encompass the process of purchasing a product, through to the installation of a product. As part of our GDPR compliance, we will ensure that any supporting and/or secondary data processing activities, shall;

- Carry out the processing of personal data strictly in accordance with our documented policies and procedures in place, in accordance with GDPR.
- Process personal data only on accepted instructions from the controller.
- Take appropriate security measures when processing personal data Only disclose or allow access to personal data to our employees or third parties who;
  + Have had relevant training in data protection and security, integrity and confidentiality of personal data;
  + Only use that data for the purpose of their job function;
  + Will only process the data on strict instructions from you the controller and/or Think Office the processor;
- Inform the controller of any requests from data subjects, who are excising their rights under the data protection act. We will assist with providing all the relevant information, under the obligation of the General Data Protection Act;
- Delivery Partners used by Think Office are reputable, respected companies and adhere to the fundamentals of the GDPR.

Security measures

Think Office will implement and maintain, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, applicable technical and organisational procedures to ensure a level of security appropriate to the risk. This may include but is not limited to;

- The pseudonymisation and encryption of personal data;
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Our Obligations

Loss or damage of data
If any personal data in the control of Think Office is rendered unusable, lost or corrupted, for any reason, Think Office will contact you and promptly, restore the personal data back to its original state, using up to data backups and disaster recovery methods.

Termination of service
If you terminate your services with Think Office we will immediately begin our process of collating your data in a machine-readable format. We will arrange for the safe return of the data, or destroy the data, depending on the strict instruction given to Think Office by you. We may refuse this service if the European Union, Member state and/or UK law requires access to the storage of your personal data.

Personal data breach
A personal data breach means a breach of security leading to the unintentional or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

In the event of a data breach, Think Office shall notify you without undue delay after becoming aware of a personal data breach. Think Office will provide the nature of the personal data breach, including the approximate number of data subjects involved, the number of personal data records compromised and the time taken place. From this point, it is then your responsibility as a controller to notify the data subject of the breach. Think Office will provide the data subject, if instructed to do so by you, with as much information as possible. We will notify you, no later than 72 after becoming aware of a breach.

Think Office will ensure its processes reduce the risk of internal data breaches (own employees) as practical as possible. However, in the event of an internal data breach, an investigation will commence measuring the severity and risk for the rights and freedoms of the data subject. If Think Office Data Protection Officer deems the data breach is unlikely to result in a risk for the rights and freedoms of the data subject, we may choose not to notify you of the data breach.

Supervisory authorities

Think Office will immediately notify you upon receiving a notice from any regulatory or government body, including the Information Commissioner and any supervisory authority, which directly or indirectly relates to the processing of your personal data. We shall cooperate with any relevant European Union or Member State supervisory authority.

Transfer of personal outside of the EU

Think Office will only process data to third party organisations if safeguards are in place to protect human rights and fundamental freedoms of data subjects, there are binding corporate rules in accordance with the GDPR, have approved codes of conduct in place and adhere to a standard of data protection clauses adopted by the Information Commissioner.

- Think Office use an electronic marketing platform, who provide email services for marketing campaigns. They are Privacy Shield Certified. The EU-US Privacy Shield is a program where participating US companies are considered to have adequate data protection, and can therefore facilitate the transfer of EU data;
- Think Office LinkedIn, for the sole purposes of posting product content & images, videos, company news, case studies, blog articles and online discussions, for our customers and suppliers to freely view. We do not use social media platforms to obtain, store or distribute personal data.

Documentation

Think Office Furniture will keep all documentation, where relevant, up to date and under the guidelines of the General Data Protection Regulation. Where necessary, Think Office will provide you with documentation, relating to management system policies.

Signed on behalf of Think Office Ltd.

Calum Haddow
Position: Director

Date written: 08/04/2021
Date reviewed: 08/04/2021