General Data Protection Regulation (GDPR)

Supplier Guidance Instruction

Introduction

From May 25 2018, The General Data Protection Regulation (GDPR) will become enforceable. This has been introduced by The European Union, who has taken a monumental step in protecting individual rights in regards to data privacy. Dams Furniture will require all suppliers to work in accordance with the General Data Protection Regulation. This is to safeguard the privacy of individuals who provide Dams with personal information. The compliance encompasses any activities carried out or on behalf of Dams by third party suppliers.

As part of Dams commitment to GDPR compliance, Dams 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, Dams will be classified as the data controller, you as the supplier will be the data processor, 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 providing Dams with your products or services, you as the supplier, have agreed to enter into a contractual agreement with Dams. This will encompass collecting and delivering products to, or on behalf of Dams. As part of our GDPR compliance, you 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;
  o Have had relevant training in data protection and security, integrity and confidentiality of personal data;
  o Only use that data for the purpose of their job function;
  o Will only process the data on strict instructions from Dams the controller;

- 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 obligation of the General Data Protection Act;

Security measures

Dams 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 your organisation is rendered unusable, lost or corrupted, for any reason, you will contact Dams and promptly, restore the personal data back to its original state, using up to data backups and disaster recovery methods.

Termination of service

If Dams terminate your services you will immediately begin your implemented process of collating Dams data in a machine readable format. You will arrange for the safe return of the data, or destroy the data, depending on the strict instruction given to you by Dams. You may refuse this service if the European Union, Member state and/or UK law requires access to the storage of Dams 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, you shall notify Dams without undue delay after becoming aware of a personal data breach. You will provide the nature of the personal data breach, including the approximate number of data subjects involved, number of personal data records compromised and time taken place. From this point it is then Dams responsibility as a controller to notify the data subject of the breach. You will provide the data subject, if instructed to do so by Dams, with as much information as possible. You will notify Dams, no later than 72 hours after becoming aware of a breach.

At Dams we take into consideration not all data breaches will require reporting, though, you will ensure your processes reduce the risk of internal data breaches (own employees) where practical as possible.

Supervisory authorities

You will immediately notify Dams 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

Dams personal data. You shall cooperate with any relevant European Union or Member State supervisory authority.

Transfer of personal outside of the EU

You will only process data to third party organisations under strict guidelines from Dams. You will ensure 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.

- Dams 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;

- Dams use Twitter, Facebook, LinkedIn and YouTube, 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

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

Chris Scott

Managing Director
Dams Furniture
May 2018