General Data Protection Regulation Statement of Compliance

Introduction

The EU General Data Protection Regulation ('GDPR') came into force across the European Union on 25 May 2018 bringing 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 GDPR strengthens the rights of individuals regarding their personal data and seeks to unify local data protection laws across Europe affording individuals stronger, more consistent rights to access and control their personal information.

Our commitment

Fisher German are committed to the protection and privacy of personal information.

Trust is one of our core Values and is the foundation on which our company is built. This is reflected in the way in which we manage and maintain data and we 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 GDPR.

Our objectives for GDPR compliance have been summarised in this statement and include the development and implementation of data protection roles, policies, procedures and controls to ensure maximum and ongoing compliance.

This statement will be subject to ongoing updates as we continue to monitor our compliance with GDPR and adjust our plans accordingly.

GDPR roles and responsibilities

Fisher German will appoint a Data Protection Officer (DPO) to oversee all aspects of GDPR compliance. The DPO will report to the Managing Partner, ensuring data privacy is embedded at the highest level. The nominated DPO is:

Clare Phillipson, Partner

If you have any questions about GDPR or the processing of your personal data, please contact dataprotection@fishergerman.co.uk or write to the Data Protection Officer, Fisher German LLP, The Head Office, Ivanhoe Office Park, Ivanhoe Park Way, Ashby de la Zouch, Leicestershire, LE65 2AB

Summary of activities

The following is a summary of activities carried out which demonstrates the actions we have taken, and continue to take, in order to ensure compliance with GDPR. During the course of our business we collect, process and store personal data relating to individuals including employees, clients, suppliers and others we communicate with. The following summary is to provide the necessary assurances to those individuals in relation to how we handle their personal data.

Information audit

We carried out an information audit based on the '5 Ws' including: WHY is personal data processed?; WHOSE personal data is processed?; WHAT personal data is processed?; WHEN personal data is processed?; WHERE is personal data processed? This audit was carried out extensively across the business with the help of nominated regional co-ordinators who worked within their regions to collate the information.

The results of the information audit enabled a better understanding of the data we hold, the format it is held in and how long it is kept for and identified key risks and actions arising formulating the basis of our ongoing action plan.

The information audit is an important step in helping us to comply with the GDPR's accountability principle which requires organisations to be able to show how they comply with the data protection principles and provides a full record of our processing activities which is compliant with Article 30, GDPR.

Policies and procedures

We have established policies and procedures to meet the requirements of GDPR and any other relevant data protections laws. These include the following:

- Data Protection Policy: our overarching policy document summarising the arrangements in place to comply with data protection laws, comprehensively reviewed to meet the requirements of GDPR. The policy confirms that accountability and governance measures are in place to ensure that we understand and adequately disseminate and evidence our obligations and responsibilities, with a dedicated focus on privacy by design and the rights of individuals.
- Records Management, Retention and Erasure: we have reviewed our records management policy and schedule to ensure that we meet the *'data minimisation'* and *'storage limitation'* principles and that personal information is stored, archived and destroyed compliantly. We have implemented procedures to meet the new *'Right to Erasure'* obligation and other data subjects' rights, along with any exemptions, response timeframes and notification responsibilities.
- Data Breaches: our data breach procedures have been reviewed to ensure that we have safeguards and measures in place to identify, assess, investigate and report any personal data breach at the earliest possible opportunity. We communicate to all personnel, making them aware of the reporting requirements and steps to follow.
- Subject Access Requests: the rules for dealing a Subject Access Request (SAR) changed under GDPR, which includes a change in timescales to respond and the removal of the ability to charge a fee. We have reviewed our SAR procedures to accommodate the revised 30-day timeframe for providing the requested information and for making this provision free of charge.

Legal basis for processing and consent

GDPR places greater emphasis on identifying the legal basis for processing data and is required when drawing up our privacy notices and when answering a SAR. The legal basis for processing is important when identifying individuals' rights.

We have reviewed our 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 are met. This will need to be documented to comply with the GDPR's accountability requirements.

Under GDPR data controllers must be able to demonstrate that consent was given. Consent cannot be inferred from silence, pre-ticked boxes or inactivity, it must be freely given, specific, informed and unambiguous. We have therefore 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 process for recording consent, making sure we can evidence an affirmative opt-in.

We have reviewed our 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.

Privacy notice(s)

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.

Data subject rights

We acknowledge that under the GDPR, individuals can exercise certain rights over their personal data and we have reviewed our policies and procedures to ensure we can facilitate data subject rights requests, which may include an individual's right to access any personal information relating to:

- 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 their 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

We have also reviewed how we provide easy-to-access information externally via our website and internally via our intranet. Individuals should contact dataprotection@fishergerman.co.uk for further guidance should they wish to exercise their data subject rights in connection with the above.

Data protection impact assessments

We have introduced a process for confirming the requirement for, and completion of, a Data Protection Impact Assessment (DPIA). A DPIA is a process designed to help assess the data privacy risks associated with organisational changes in relation to processing personal data, in particular where the processing involved large scale processing or includes special category data.

The implementation of stringent procedures and the use of assessment templates for carrying out impact assessments ensures that we fully comply with the GDPR's Article 35 requirements.

Information security, technical and organisation measures

We take 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 identify, manage and put measures in place to mitigate business risk and we regularly assess and manage the risks associated with protecting the confidentiality, integrity and availability of the personal data we process.

We carried out an extensive review of our information security policies and procedures to protect personal information from unauthorised access, alteration, disclosure or destruction including:

- Information Security Policy: overarching policy covering our information assets including documents and files which can be electronic or physical.
- Remote Working Policy: outlines how we control remote access to IT systems and defines how personnel should adhere to this when working remotely.
- Internet, Email and IT Policy: outlines the standards required by personnel when using the internet, email and other IT systems.
- Business Continuity Policy: overarching policy together with associated business continuity arrangements and local office plans essential to mitigate the impact of any disruptive incidents or disasters.

We are developing our systems to ensure we can fulfil our obligations for a data subject's right of access to, rectification or restriction of personal data. All personal data is backed up and stored securely. This includes reviewing our systems to ensure we can fulfil our obligations for the 'right to be forgotten' (Article 17, GDPR 2016) which requires that personal digital data can be securely and fully removed from our systems and the 'right to data portability' (Article 20, GDPR 2016) which requires that all personal data can be exported from our systems electronically and in a commonly used format. We have produced data process maps which identify the flow of data through our systems and where data is held. This will form part of an ongoing review process.

Disaster recovery is in place for our critical systems and is regularly tested.

All laptops and desktops run the latest security patches and antivirus software.

We have an ongoing process of update to startup encryption on all laptops and desktops.