General Data Protection Regulation
Statement of Compliance

Introduction

The ***EU General Data Protection Regulation ('GDPR')*** comes into force across the European Union on 25 May 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.

Our commitment

Fisher German is 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 programme in place which complies with existing law and abides by the data protection principles. We do, however, recognise our obligations in updating and expanding this programme to meet the demands of the GDPR.

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 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.

This statement will be subject to ongoing updates as we progress with our GDPR readiness.

GDPR roles and responsibilities

Fisher German has designated **Clare Phillipson** as its **Data Protection Officer (DPO)** and has appointed a Data Privacy team to develop and implement our roadmap for complying with the new data protection Regulation. The team is 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.

Fisher German understands that continuous employee awareness and comprehension is vital to the continued compliance of the GDPR and has involved personnel in our preparation plans. We are reviewing our induction and training programme to feature GDPR, including a mandatory elearning module, presentations at our internal training days and regular updates and guidance via the firm's intranet.

All personnel who are authorised to process personal data do so on a strictly 'need-to-know' basis as necessary to perform their role in the provision of required services. All Fisher German personnel have signed a confidentiality agreement which forms part of their contract of employment.

If you have any questions about our preparation for the GDPR, please contact dataprotection@fishergerman.co.uk or write to the Data Protection Officer, Fisher German LLP, The Estates Office, Norman Court, Ashby de la Zouch, Leicestershire, LE65 2UZ

How we are preparing for the GDPR

We already have a consistent level of data protection and security across our organisation. It is, however, our aim to be fully compliant with the GDPR. We have provided a summary of the areas we are currently working on below:

Detail of activity	Completed (Yes/No/Partial)	Date for completion
Information Audit		
We have carried out an information audit to identify what personal data we hold. This has been 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?. We have carried out this audit extensively across the business with the help of nominated regional coordinators who have worked within their regions to collate the information. The results of the information audit have identified key risks and actions arising which now form the basis of our ongoing action plan. The audit remains under ongoing review. 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.	Yes	Completed
Policies and procedures		
We are in the process of reviewing our **data protection policies and procedures** to meet the requirements and standards of the GDPR and any relevant data protection laws, including: • **Data Protection Policy** – our overarching policy document is being reviewed to meet the standards and requirements of the GDPR. 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 are reviewing 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 will be implementing dedicated erasure procedures to meet the new *'Right to Erasure'* obligation and other data subjects' rights, along with any exemptions, response timeframes and notification responsibilities.	Yes Yes	Completed Completed

Detail of activity	Completed (Yes/No/Partial)	Date for completion
• **Data Breaches** – our data breach procedures are being 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 time. We will communicate to all personnel, making them aware of the reporting requirements and steps to follow. • **Subject Access Request (SAR)** – the rules for dealing with subject access requests are changing under GDPR, which includes a change in timescales to respond and the removal of the ability to charge a fee. We are reviewing our SAR procedures to accommodate the revised 30-day timeframe for providing the requested information and for making this provision free of charge.	Yes Yes	Completed Completed
Legal basis for processing		
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 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 are met. This will need to be documented to comply with the GDPR's accountability requirements.	Yes	Completed
Privacy notice(s)		
We are revising 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.	Yes	Completed
Obtaining consent		
It is clear under GDPR that 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 are revising 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 are developing stringent processes for recording consent, making sure that we can evidence an affirmative opt-in,	Yes	Completed

Detail of activity	Completed (Yes/No/Partial)	Date for completion
along with time and date records, and an easy to see and access way to withdraw consent at any time.		
Direct marketing		
We are revising 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.	Yes	Completed
Data protection impact assessments (DPIA)		
We are reviewing our business to identify any areas where we may process personal information that is considered high risk, involves large scale processing or includes special category data. Where this is found to be relevant, we will be developing stringent procedures and assessment templates for carrying out impact assessments that comply fully with the GDPR's Article 35 requirements.	Yes	Completed
Data subject rights		
In addition to the policies and procedures mentioned above that ensure individuals can enforce their data protection rights, we are reviewing how we provide easy to access information externally via our website and internally via our intranet of an individual's right to access any personal information that we 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 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	Yes	Completed
Information security, technical and organisational measures		
We take the privacy and security of individuals and their personal information very seriously and take every		

Detail of activity	Completed (Yes/No/Partial)	Date for completion
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 are carrying 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.	Yes	Completed
• **Remote Working Policy** – outlines how we control remote access to IT systems and defines how personnel should adhere to this when working remotely.	Yes	Completed
• **Internet, Email and IT Policy** – outlines the standards required by personnel when using the internet, email and other IT systems.	Yes	Completed
• **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.	Yes	Completed
We are reviewing 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.	Yes	Completed
We are in the process of producing data process maps which will identify the flow of data through our systems and where data is held. This will form part of an ongoing review process.	Yes	Completed
Disaster recovery is in place for our critical systems and is regularly tested.	Yes	Completed
All laptops and desktops run the latest security patches and antivirus software.	Yes	Completed

Detail of activity	Completed (Yes/No/Partial)	Date for completion
We have an ongoing process of update to startup encryption on all laptops and desktops.	Partial	1st Qtr 2019