Willis Towers Watson - our approach to the General Data Protection Regulation

What is the European General Data Protection Regulation ("GDPR")?

The GDPR came into effect on 25 May 2018 across all Member States of the European Union and the European Economic Area ("EEA"). It is now generally recognised that the GDPR significantly increases compliance and accountability standards for organisations, as well as strengthening the enforcement powers of regulators and the rights of individual 'data subjects'.

The GDPR is concerned with the processing of personal data. *'Personal data*' is any information which can directly or indirectly identify an individual, and '*processing*' is anything which an organisation does with personal data, including merely storing it.

How does the GDPR apply to Willis Towers Watson?

Willis Towers Watson processes the personal data of its clients, insured persons, employees, business contacts, office visitors etc. We undertake these processing activities in the role(s) of independent controller, processor and/or joint controller depending on the work and line of business in question.

We have put in place systems and controls in line with the differing requirements on these respective categories and have advised our teams accordingly.

We have worked hard to build a comprehensive GDPR compliance programme, ensuring our internal business units are continually educated and assessed regarding GDPR compliance. We are dedicated to working with our clients to help ensure that we and you meet our respective regulatory requirements.

How does Willis Towers Watson meet the requirements of the GDPR?

Even before the GDPR came into force, Willis Towers Watson took data protection and privacy very seriously. We have specific resources assisting the various corporate and business teams with their compliance to help ensure managing privacy risk is at the heart of everything we do.

The following summarizes the primary GDPR compliance efforts that have been implemented by Willis Towers Watson as part of the GDPR compliance programme:

- Development of a governance structure for oversight of GDPR compliance, including but not limited to the creation of a Privacy Steering Committee and an EMEA Privacy Working Group;
- Appointment of a Group EMEA Data Protection Officer supported by a network of country data protection officers (where required);
- Appointment of an EMEA Privacy Counsel;
- Review of our externally-facing privacy notices, data protection policies, and our procedures for GDPR compliance including, for example, the data subject request procedure;
- Implementation of an internal education and awareness programme through creation of internal training materials, resources and points of contact and a comprehensive GDPR training programme (see below);

- Compilation of records of data processing and Data Protection Impact Assessments; and
- Coordination with clients and suppliers (acting as processors or sub-processors) to update existing contracts and contract templates.

We are committed to ensuring ongoing compliance in line with the principles of the GDPR, fully embed a culture of privacy within our organisation and continually review and enhance our systems, controls and processes.

Group EMEA Data Protection Officer contact details:

Carlos Pereira
DPO@willistowerswatson.com
Willis Towers Watson, 51 Lime Street, London EC3M 7DQ

What technical controls does Willis Towers Watson have in place to protect the security of personal data?

Willis Towers Watson maintains appropriate security measures for both personal data and confidential company and client data globally. We adhere to Information Security Standards to mitigate against the risk of a compromise to the confidentiality, integrity, and availability of our information assets. For example, client data is held on systems with physical access controls that meet or exceed industry standards for security; Willis Towers Watson standard encryption tools are implemented where personal data is transmitted across public networks and portable handheld devices; and third party suppliers are assessed based on various criteria such as type of service and data handled.

How does Willis Towers Watson deal with security incidents?

Willis Towers Watson has a global Cyber Security Incident Response Plan ("CSIRP") for identifying and managing cyber security threats, including those with the potential to adversely affect information security and data privacy, globally. The CSRIP defines the roles and responsibilities of our stakeholders involved with responding to cyber security events, severity levels, and threat categories, and outlines a process for incident management, including escalation and communication procedures to supervisory authorities, data subjects, and clients, as appropriate. The CSIRP is reviewed and tested annually.

Does Willis Towers Watson transfer or hold any client data outside of the EEA?

Willis Towers Watson is a global organisation operating in more than 140 countries and our business activities are global in nature. As such we sometimes transfer personal data to countries located outside of the EEA. When making these transfers, we will take steps to ensure that such personal data is adequately protected and transferred in accordance with the requirements of the GDPR. For example, as part of its privacy compliance framework, Willis Towers Watson has entered into an Intercompany Data Transfer Agreement, which contains the European Standard Contractual Clauses. This Data Transfer Agreement has been entered into by Willis Towers Watson's group companies in the EEA, USA and other countries where Willis Towers Watson may transfer EEA personal data, for example the Willis Towers Watson support centres in India and the Philippines.

This Intercompany Data Transfer Agreement will also allow Willis Towers Watson's group companies to transfer personal data to and from the United Kingdom even if the United Kingdom becomes a third country in the event of a no deal Brexit.

What education and training does Willis Towers Watson provide to employees?

We ensure that new employees receive information on and training in adhering to data protection legislation and Willis Towers Watson policies. Current employees receive this training at least annually with the aim of refreshing their knowledge, informing them about any new requirements and sharing common experiences. The training includes a particular focus on key elements such as recognizing and reporting a potential personal data breach, recognizing and properly addressing a data subject request, and the proper methods for transfers of personal data outside of the EEA.

What is Willis Towers Watson's approach to Data Protection Impact Assessments and "Privacy by Design and Default"?

We view 'Data Protection Impact Assessments' and 'Privacy by Design and Default' as important tools to effect a cultural change and embed privacy awareness into everything we do. We have rolled out these tools across our business accompanied with training to help our employees understand their responsibilities and play their part in helping us achieve good information governance.