**Aon Service Corporation**
Law | Global Privacy Office

# Aon

# GDPR FAQ's

Empower Results®

1. ***Will Aon be ready for GDPR compliance by 25 May 2018?***

   We take data privacy extremely seriously and we have invested significant resources to the development of a framework to ensure that our core products and services are compliant with applicable data privacy laws and that wider data privacy risks are effectively managed. We see GDPR compliance as an ongoing process and will continue to develop our GDPR compliance program in the run up to May 2018 and beyond.

2. ***Does Aon maintain a personal data inventory?***

   We maintain appropriate records of our processing activities involving personal information which will provide us with a view of where we collect, use, retain and disclose personal information across our business globally. These processing records have been designed to enable us to meet our data privacy and regulatory obligations and we have implemented appropriate procedures to ensure our processing records are reviewed periodically and kept up to date.

3. ***Do you have processes in place to comply with requests from individuals to exercise their rights to (i) access, rectify, or erase their personal data; (ii) object to, or restrict, the processing of their personal data; (iii) object to the automated processing (including profiling) of their personal data; and (iv) the data portability of their personal data?***

   We have in place standard operating procedures to ensure we take a consistent and rigorous approach to managing operational data privacy tasks including those related to requests from individuals to exercise their rights under data protection laws, in line with our legal, regulatory and contractual obligations.

4. ***Can you provide sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of the General Data Protection Regulation (GDPR) and ensure the protection of the rights of the data subject?***

   Aon maintains appropriate technical, organizational, and physical safeguards designed to protect the personal information we process in accordance with client instructions and in line with our legal and regulatory obligations.

5. ***Do you have processes in place, when engaging sub-processors, such that (i) you only appoint a sub-processor with the prior written authorization of the controller; and (ii) you put a contract in place with each such sub-processor which flows down the mandatory obligations for processor contracts under Article 28 of the GDPR?***

   Aon has in place a Supplier Risk Governance framework designed to ensure that we engage with third party suppliers in line with our legal, regulatory and contractual obligations. We have in place mandated guidelines for selecting and managing our suppliers, including assessments of their operational capabilities and adherence to our privacy and data security requirements. We ensure that we have in place appropriate contractual terms with all third parties with whom we engage that reflect the requirements of applicable data privacy laws (including Article 28 GDPR where applicable) and to ensure that wider data privacy risks are effectively managed.

6. ***Do you comply with the international transfers provisions of the GDPR, as set out in Chapter V of the GDPR?***

We have in place standard operating procedures to ensure we meet the requirements of applicable data protection laws, including those relating to transfers of personal data outside the EEA under the current Data Protection Directive and forthcoming GDPR. In line with legal requirements and regulatory guidance we typically rely on the use of Standard Contractual Clauses where appropriate.

**7. Does Aon transfer personal data to any countries outside the EEA? If so, what security provisions do you use to safeguard the data?**

As is the case with many global companies certain aspects of our IT infrastructure in the EEA are supported from non-EEA countries, such as the US and India. Such services may be provided by Aon affiliates or our service providers, however they will not be providing any of the services defined in our contract to you, only IT services to us. To ensure compliance with data protection laws we have in place a matrix of intercompany agreements, imposing contractual provisions on Aon affiliates in respect of confidentiality, security and the use and disclosure of personal information. Where we have engaged IT service providers, we also rely on EU standard contractual clauses where applicable.

***8. Does Aon keep personal data secure? If so: i. How is it secured? ii. Have you relied on any protocols or standards for implementing security? iii. How have security measures / compliance with any such standards been checked?***

We have a framework of policies and procedures in place to ensure we are implementing our legal and regulatory obligations for data security. Aon protects personal data with appropriate technical, organizational, and procedural measures that are commensurate with the risks posed to individuals. For example, our strategic data security approach is to build controls to protect, detect, respond to, and recover from incidents which may affect the personal information we process. We maintain a suite of data and cyber security policies that set out our commitment and expectations for the protection and security of personal data. We implement a security awareness and training program to make our staff aware of their responsibilities for the protection of personal data. We operate a global security operations centre to monitor, detect and manage security incidents including any cyber threats to our network and systems.

***9. Does Aon have a policy regarding the deletion of personal data that it processes? What procedures are in place to ensure: (i) that records are deleted when no longer required – when / how is this determined? (ii) Are there any copies of this data? If so, why do we have copies, where is it stored, what is it used for, and who has access to it? (iii) Are there any databases or systems which still hold personal data that your process for us which are now redundant / dormant in your view which we can delete?***

Aon will retain data in accordance with its legal, regulatory and record keeping obligations, in accordance with applicable data protection laws, and in accordance with our contractual commitments with our clients. We have processes to securely erase data in accordance with our record retention schedule. Our periodic data protection mandatory training reiterates to all staff their adherence to Aon's secure disposal policies and procedures

***10. Does Aon have a process in place for dealing with subject access requests from data subjects?***

Aon has in place internal policies and processes covering data subject rights under applicable data protection laws, which set out how to identify and respond to such requests including

formalized logging procedures. Our Data Privacy Office provides support with any such requests where required.

***11. Does Aon have in place a process for immediately reporting a data security breach?***

We have in place robust processes to ensure that data security incidents are identified and responded to effectively, which ensure we comply with our legal, regulatory and contractual requirements as regards notification of those incidents.

***12. Does Aon have a defined process for logging and escalating data incidents?***

Aon has a standard process for the escalation of data incidents. Aon has a 24x7 Global Emergency Operations Centre (GEOC) charged with immediate management and response to incidents and emergencies, and an incident response program for managing potential data incidents. Aon maintains lists of key contacts within critical support functions to be able to respond quickly and effectively to an incident, and these individuals are notified and form an incident response team.

***13. Do the employees in your organization receive training on data protection and other relevant law? Are staff aware that unlawful access to and/or disclosure of personal data is prohibited?***

Our Global Privacy Policy is communicated to all colleagues as part of their data privacy training and within our Code of Business Conduct, which is reaffirmed by Aon colleagues on an annual basis. Our global privacy training sets out our expectations and requirements as regards the handling of personal information. This training is periodically reviewed to ensure it meets current legal requirements and regulatory expectations. We require certain key colleagues to undertake role specific or country specific training if there are specific actions we expect them to undertake. We conduct regular awareness campaigns and ad-hoc training roadshows to reinforce key training messages which can take the form of newsletters on the intranet and posters.

***14. How does Aon screen new employees?***

We undertake a risk-based approach to vetting new colleagues, taking into account data security and other fraud risk. As part of the recruitment process, all new colleagues are subject to comprehensive good repute checks prior to commencement of employment. These checks are made subject always to local legal requirements and may include employment and personal references; academic confirmation; eligibility for employment; criminal record check; fitness and propriety, financial and identity confirmation. At Aon, it is a condition of employment that colleagues are required to sign a non-disclosure agreement and abide by the Aon's policies on privacy, security and confidentiality.

***15. Do you currently have a Data Protection Officer or other such employee responsible for Data Privacy and Information Security?***

Our Chief Privacy Officer, supported by our Global Privacy Office, is responsible for promoting compliance and awareness of applicable data privacy laws across Aon, and advising on the implementation of and compliance with our data privacy policies and standards

*16.* ***Have you assigned senior management support for data security with overall responsibility to manage data security risk assessments and communication between the key stakeholders within the firm?***

The Global Chief Security Officer, as a leader of Security Risk Management, ensures that all policies meet global legislative requirements, are cognizant of international standards, and that the security risk is captured, owned, and appropriately managed. A quarterly security report including current security risk, details of incidents, and progress towards the agreed security maturity levels is presented to the Executive Committee on a quarterly basis.

***17. Does Aon conduct Data Protection Impact Assessments?***

We have standard operating procedures in place, which involves our Global Privacy Office where appropriate, to ensure new projects involving personal information undergo a Privacy Impact Assessment review prior to implementation to ensure data privacy risks posed to individuals are identified and effectively managed.

**18. *Does Aon operate as a data controller or data processor?***

Aon operates in its capacity as a Controller and/or a Processor depending on the nature of the services. Whether acting as a Controller or a Processor we take our data protection obligations extremely seriously and we have invested significant resources into the development of a framework to ensure that our core products and services are compliant with applicable data privacy laws and we process personal data in line with our legal and regulatory requirements and in accordance with our contractual commitments with clients.

About Aon

Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.