GDPR FAQs

The purpose of this document is to provide our clients with a better understanding of how Dealogic is preparing for the General Data Protection Regulation (GDPR).

Q: What is the GDPR?

A: The General Data Protection Regulation (GDPR) is a new landmark privacy law taking effect in the European Union (EU). It expands on the privacy rights granted to EU individuals and places many new obligations on organizations.

Q: Who does the GDPR apply to?

A: To organizations based within the EU that process personal data. The GDPR will also apply to an organization operating outside the EU if that organization offers goods/services to or monitors the behaviour of people in the EU. For example, the GDPR could catch a US-based client whose website uses tracking technology to collect personal data to create profiles of EU

Q: When does the GDPR come into force?

A: The GDPR will come into effect across the EU from 25 May 2018.

Q: Does "Brexit" mean the GDPR won't apply to the UK?

A: The GDPR will come into effect across the EU from 25 May 2018. As the UK will still be a member of the EU at this date, the GDPR will also apply to the UK, and will continue to apply after the UK's eventual exit from the EU. The UK government has confirmed this approach.

Q: How is Dealogic preparing for the GDPR?

A: Dealogic has a dedicated team of data protection, legal and security specialists who review its processing of personal data. We also have a network of privacy champions across our offices who are responsible for ensuring data privacy is always in mind. This team will ensure Dealogic meets or exceeds the requirements of the GDPR. We have undertaken a two-year project to prepare for the 25 May 2018 deadline. This has included independent audits of our processes and procedures.

Q: What is the difference between a data processor and a data controller?

A: A controller is the entity that determines the purposes, conditions and means of the processing of personal data, while the processor is an entity which processes personal data on behalf of the controller.

Q: Is Dealogic a Controller or a Processor?

A: Dealogic is a data processor in relation to the vast majority of its products, and our clients are the data controllers. The main exception is the Contacts Data Feed Product where Dealogic is a data controller responsible for the security of the Feed data up until the point of receipt by our clients. The receiving client is a separate data controller. For more information, please review the specific terms and conditions that apply to the Contacts Data Feed Product.

Dealogic is also a data controller in relation to its HR related data (e.g. employee personal data and applicant personal data).

Q: Will the GDPR stop Dealogic using personal data?

A: No. The GDPR does however place a greater focus on business accountability and transparency to individuals around how their personal data is being used. In the context of Dealogic services, we process a limited amount of business contact personal information which is necessary to enable the financial services industry to operate in an efficient manner and in compliance with other regulatory requirements. For example, some of our products enable a user to include the business contact information of an individual who attended a meeting. Inclusion of this information does not prejudice the individual whose details are added. In fact, it benefits the individual, as they may then be able to receive payment for services in line with MiFID II.

Q: The consent requirements will change under the GDPR. How will we and Dealogic comply?

A: If consent is relied upon it must be obtained in a transparent and unambiguous manner, e.g. not 'hidden' in terms and conditions or assumed through pre-ticked boxes. It is worth bearing in mind that consent is only one way of lawfully collecting personal data. Dealogic and many of our clients rely on 'legitimate interests' as an alternative to consent. To read more, please refer to our Product Privacy Policy.

Q: What measures has Dealogic taken in preparation for the GDPR?

A: Examples include:

- A dedicated group of professionals, including our General Counsel/DPO, Chief Security Officer, lawyers and privacy experts, data specialists, security personnel, technology teams and privacy champions who work to ensure privacy and data compliance across our global business.
- Regular data protection training for our employees. This includes eLearning modules, online resources, videos and face-to-face training for higher risk groups.
- Creation and maintenance of an internal data governance framework and several key processes and policies to underpin the requirements of the GDPR and to reinforce our own corporate values and principles.
- Data security policies and controls in place globally. These are continually tested (including regular external, independent audit) and evolve in line with changing regulations and governance requirements. Our data security programme is aligned to industry standards, including the most recent ISO27001 certification. Processes and policies are in place to isolate and manage security incidents in line with regulatory requirements.

External Links

GDPR frequently asked questions: http://www.eugdpr.org/gdpr-faqs.html

Further reading and resources: http://www.eugdpr.org/more-resources-1.html