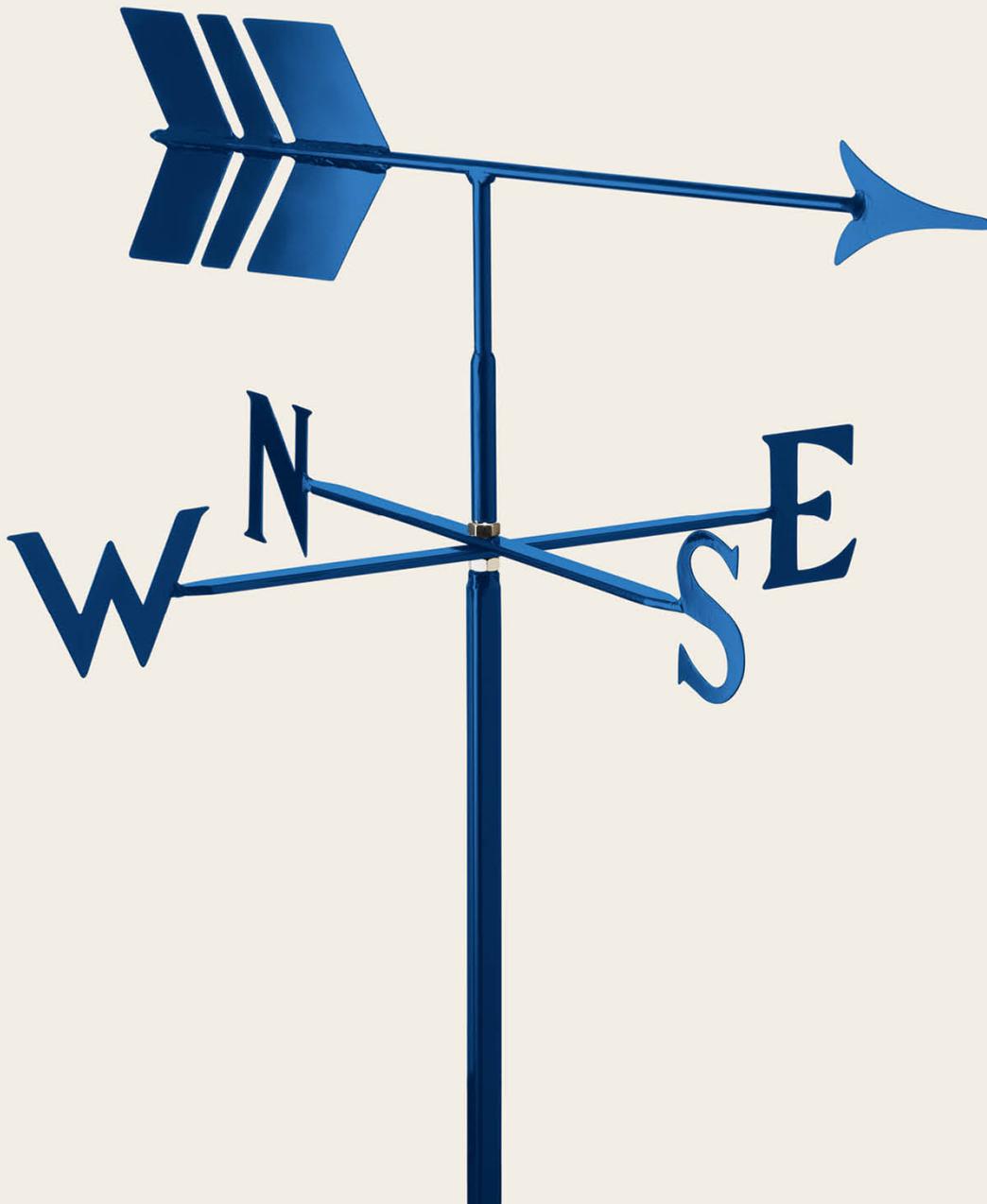


GDPR at Zurich

FAQs



Question #	Question	Answer
1	What is the EU GDPR?	The General Data Protection Regulation (GDPR) is European Union legislation that will replace the existing EU Data Protection Directive in May 2018. Just like the Directive established in 1995, the GDPR gives an individual - such as a policyholder, beneficiary, claimant or employee - certain rights with respect to their personal data when it is processed by others. The GDPR also imposes specific obligations on those who have access to any individual's personal data to protect it appropriately.
2	Does the GDPR only apply in EU/EEA countries?	Generally speaking, the GDPR applies to businesses, governments and other organizations that are physically located within the EU. However, the Regulation can apply outside of the EU when personal data is processed in order to (1) offer goods or services to residents in the EU; and/or (2) monitor EU residents.
3	What does the GDPR mean for individuals that share their data with insurance companies?	The GDPR builds on many of the rights of individuals that were established 20 years ago through the original EU Data Protection Directive. However, the GDPR makes it easier for a policyholder, beneficiary, claimant or employee to exercise those rights with respect to their own personal data. In that sense, the GDPR is not something new. Rather, the GDPR builds on data protection regulation that has been in place across the EU for over two decades.
4	What does the GDPR mean for EU Distributors?	In most cases, insurance distributors will be treated as "data controllers" with respect to the personal data they collect and process. Accordingly, insurance distributors must ensure that they collect, use, protect and share personal data in ways that are consistent with the GDPR.
5	If I have questions about whether Zurich has my personal data, who do I contact?	Information about how to ask a question regarding your personal data can be found in the notice of data processing or on the Zurich web site for the relevant country.
6	What is Zurich's position on GDPR?	Zurich welcomes the uniformity that GDPR is expected to bring to the European data protection landscape. The differences in the data protection laws of the EU Member States under the current regime are significant even though they are all based on the same Directive. The uniformity intended by the GDPR should facilitate the ease of doing business in the EU, while ensuring a high level of data protection for individuals.
7	Will Zurich be ready by the GDPR effective date in May 2018? Do you expect any significant gaps in IT applications by that date?	We do expect to be ready to meet the requirements of the GDPR by May 2018. Of course, IT changes can be complex and time consuming. In some cases, we may not have the final IT solutions in place by that time. However, we are confident that we will have appropriate alternative or temporary solutions in place so that the rights and interests of individuals that provide their personal data are protected.
8	Your competitors have been investing significant sums of money. How much is Zurich investing?	As a matter of principle we do not supply detailed budget information. However, we ensure that appropriate investments are made, including in existing initiatives, to ensure the personal data we hold is appropriately managed and protected in line with the GDPR.
9	Given the increased awareness of customers about their rights (e.g., "Right to be forgotten"), are you expecting an increase in the number of requests and inquiries to delete data?	We are prepared to handle any requests or inquiries we receive. At this time, it is difficult to predict whether an increase in requests or a change in the nature of requests will happen after the GDPR goes into effect in May, 2018.

10	How will you be handling data portability requests? Do we see a day when you will want customers to bring data over from their prior insurer?	Of course, we will comply with an individual's rights to data portability. However, it is likely to be several years before the insurance industry as a whole develops standards for data portability which will make large-scale data portability a practical reality.
11	How quickly can all of the personal data Zurich has pertaining to a particular individual (such as a policyholder, beneficiary, claimant or employee) be identified across the organization (i.e., across all systems)?	The GDPR establishes set time periods for responding to requests regarding personal data, including the possibility of an extension of that time where the situation warrants. We fully expect to be able to meet these requirements.
12	How will you ensure all relevant Zurich employees with access to personal data are properly trained?	All employees receive periodic training with respect to data protection and privacy. Specific training is provided to individuals working in areas that interact with high volumes of personal data (including handling data subject requests) and sensitive personal data. Zurich's relevant policies and procedures include authority and access limitations.
13	How can Zurich ensure its third-party business partners will be compliant with the GDPR?	The GDPR requires specific terms to be included in agreements that relate to the processing of personal data. As part of our GDPR implementation efforts, Zurich is undergoing an extensive process to update all relevant contracts with third parties to ensure that any such processing of personal data takes place under appropriate contractual terms.
14	Zurich has recently announced major investments in Robotics Process Automation and Artificial Intelligence to improve underwriting and claims management processes. What protection do customers have when a machine makes an important decision? How do we know the decision is made on sound data and comes to a reasonable conclusion?	The GDPR affords people certain protection in the case of automated individual decision making (i.e., when a computer makes a significant decision about an individual based on personal information). Instances of fully automated individual decision making are not common today in many aspects of the insurance industry although that may change. Zurich has procedures to identify and ensure the necessary protection is embedded in processes that use automated decision making.
15	Does Zurich expect to appoint a Data Protection Officer (DPO)?	The GDPR mandates the appointment of a Data Protection Officer (DPO) if a business's core activities consist of processing that requires "regular and systematic monitoring" of data subjects (i.e., identifiable individuals) on a large scale, and/or involves processing of special categories of data, such as health information or criminal offenses. Additionally, Members State law may require the designation of a DPO under broader circumstances or criteria. It is expected that Zurich will have a designated DPO in the European jurisdictions in which we operate.
16	What is Zurich's record retention policy?	Zurich's has a global data retention policy and complies with local regulatory requirements.
17	How does Zurich control the transfer of data out of the EEA?	Zurich has multi-lateral data processing agreements in place and currently relies on Model Clauses to ensure that personal data is appropriately protected when transferred outside of the EEA.

Zurich Insurance plc is regulated by the Central Bank of Ireland.
Zurich Life Assurance plc is regulated by the Central Bank of Ireland.