ACTUARIAL ASSOCIATION OF EUROPE
ASSOCIATION ACTUARIELLE EUROPÉENNE

1 PLACE DU SAMEDI
B-1000 BRUSSELS, BELGIUM
(+32) 2 201 60 21
INFO@ACTUARY.EU
WWW.ACTUARY.EU

GDPR FROM AN ACTUARIAL PERSPECTIVE

This note is intended to assist European actuaries who are working in insurance in considering some of the issues raised by GDPR implementation into daily practice. It is not intended to act as a legal guide to GDPR. In addressing elements of the requirements of GDPR, this note does not act in any way as a replacement for a thorough analysis of the regulation.

REGULATION FOCUS

GDPR, WHAT DOES IT MEAN FOR ACTUARIES?

Effective from 25 May 2018, the European General Data Protection Regulation (GDPR) is now fully in force. The GDPR will change the way in which businesses handle customer data, creating new rules around customer consent, profiling, data portability and the customer's 'right to be forgotten'. Any company handling European citizens' data will have to comply with this regulation, and the GDPR is going to have a huge impact on many sectors, including insurance.

As key data users, actuaries will be highly impacted, and we will have to change the way we store and treat data, the way we model and the way we communicate. Deletion of data will not be a helpful solution to data related problems for actuaries as some of the most prominent data users and analysts in insurance.

GDPR, WHAT DOES IT MEAN?

The European General Data Protection Regulation[1] (GDPR) came into force on the 25 May 2018 and applies to all EAA and non-EAA organisations offering goods and services to persons in the EAA. Organisations had a 2-year implementation period to ensure full compliance, and they must now be operate in full compliance with the GDPR. The aim of the GDPR is to protect all EAA citizens from privacy and data breaches. Although the key principles of data privacy are still consistent with the previous directive (established in 1995), many changes have been implemented.

'Personal data[2]' means any information relating to an identified or identifiable natural person ('data subject'[2]); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC
[2] See glossary on page 9

GDPR defines special categories for 'sensitive' personal data[3]. These special categories are more restrictive and are the following: racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

The key points of the GDPR are the following:

New Scope

Application
The GDPR applies to any company, regardless of its location, processing the personal data of people residing in the EAA.
It applies to the processing of personal data by controllers[3] and processors[3] in the EAA, regardless of whether the processing takes place in the EAA or not. The GDPR also applies to the processing of personal data of data subjects in the EAA by a controller or processor not established in the EAA, where the activities relate to offering goods or services to EAA citizens.

New Rights

Consent
Under GDPR, companies are no longer able to use long, incomprehensible terms and conditions full of legalese; consent for collection and use of personal data must be in plain language and detail the purpose of data processing. If an organisation is relying on consent, consent must be specific.

Right to access
Part of the expanded rights of data subjects outlined by the GDPR is the right for data subjects to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, free of charge, in an electronic and readable format in a month or less (unless it is a particularly complex request).

Right to be Forgotten
The right to be forgotten entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. It should also be noted that this right requires controllers to compare the subject's rights to "the public interest in the availability of the data" when considering such requests.

Data Portability
Data portability is the right for a data subject to receive the personal data concerning them which they have previously provided, in a 'commonly used and machine-readable format', and have the right to transmit that data to another controller.

[3] See glossary on page 9

New Governance

Data processing
The GDPR gives data subjects the right to object to data processing. That means organisations will be required to show they have a legal and compelling reason to continue processing data relating to that particular subject. Citizens now also have the right to question and fight decisions that affect them if they have been made on a purely algorithmic basis.

Pseudonymisation[4]
It also puts forth the idea of pseudonymisation, whereby the personal data is converted in a way that makes it impossible for unauthorized people to trace it back to an individual.

Responsibility
Both data controllers and processors must comply with the GDPR, including third parties such as brokers or reinsurers.

Privacy by Design[4]
It will be a legal requirement to consider data privacy at the outset of all projects and initiatives, not as an afterthought.

Data Protection Officer (DPO)[4]
Controllers and processors whose core business is regular and systematic monitoring of data subjects on a large scale or who deal with special categories of data are required to appoint a DPO. This will most likely apply to all insurers.

Data Breaches
Under the GDPR, breach notification is mandatory in all member states where a data breach is likely to "result in a risk for the rights and freedoms of individuals". This must be done within 72 hours of data processors first becoming aware of the breach. Data processors are also required to notify their customers and controllers "without undue delay" after first becoming aware of a data breach.

New Fines

Penalties
Organisations in breach of GDPR can be fined up to 4% of annual global turnover or €20 million (whichever is greater).

[4] See glossary on page 9

GDPR, WHAT DOES IT MEAN FOR COMPANIES?

Because data is the raw material of actuarial tasks, the GDPR has a significant impact on the insurance sector. All functions, all processes and all employees will be impacted.

There are two main impacts for the industry;

- Client relationship: how is the client relationship affected?
- Operations: what are the operating changes in the organisations?

CLIENT RELATIONSHIP

The customer data rights will drastically change the relationship between the insured and the insurer.

Consent

Insurers now have to make sure that consent exists to use and profile a customer's data. Insurers must also state how they intend to use the data; transparency is the key here to build the trust required in the data exchange relationship. It is a chance for insurers to explain how this can benefit the customer, for instance by providing more personalized policies.

Right to be forgotten

Insureds have the right to request access to and deletion of their personal data and insurers need to make sure every reasonable step has been taken to ensure that inaccurate personal data is rectified or deleted. Insureds do not need to prove damage or distress or inaccuracy for this to happen. Insurers must delete personal data on request under a number of specified grounds, including where the personal data is no longer necessary for the original purpose for which it was collected or processed and if the data subject withdraws their consent and no other legal ground for processing applies. However, there are a number of good reasons for which insurers can keep personal data, including compelling legitimate grounds, to comply with a legal obligation or to establish, exercise or defend legal claims. Insurers can also choose to anonymize the data in a clever way, to keep it for statistical purposes. GDPR does not apply to data where the subject is no longer identifiable.

Data portability

Customers have control and ownership of their own personal data, allowing them to use their data for their own purposes and to share it with organisations of their choice. Insurers should therefore accept that access to this customer data is only temporary and will stop the moment customers decide to change their insurer. Insurers must provide insureds with a copy of their personal data in a structured, commonly used and machine-readable format and not hinder the transmission of personal data to a new data controller (broker, insurer, bank). This means that insurance policyholders can not only request that insurance companies send their personal data to them but also that they send it to their competitors. Insurers therefore need to design new processes to satisfy these requests, remembering that they have less than one month to share the data with the insured following a request.

OPERATIONS

Insurers must report security breaches to the relevant authority "without undue delay, and where feasible, not later than 72 hours" after they first become aware of such breaches. Insurers should review all policies and procedures to make sure data breaches can be detected, reported and managed promptly.

Personal data is required to be processed in a manner that ensures appropriate security and confidentiality of the personal data, including preventing unauthorized access to or use of personal data. Third party processing (broker, outsourced IT, reinsurance) must also comply with GDPR and the insurers have responsibility to ensure compliance by third parties.

Many insurance products and policies rely on personal data being provided in order to support the requirements of the full value chain (underwriting, administration, claims management). In many cases, e.g. health, life or travel insurance, sensitive personal data can be required. The GDPR has defined this special category data. A key challenge for insurance is that, unlike the healthcare sector, there are no specific grounds under the GDPR for processing sensitive personal data.

Anonymisation / pseudonymisation could be the best solutions for the insurance sector to comply with sensitive personal data requirements. The explicit introduction of pseudonymisation in this Regulation is not intended to preclude any other measures of data protection. However, it is clear that the principles of data protection does not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or is no longer identifiable. The GDPR does not preclude the processing of such anonymous information, including for statistical or research purposes.

GDPR, WHAT DOES IT MEAN FOR ACTUARIES?

If actuaries receive, store and use only anonymous information, the GDPR should have a limited impact for them. However, it is common for actuaries to work with large extraction files of non-anonymous data, such as first name, last name, social security ID, etc.

What do actuaries working with EAA subjects' personal data have to do?

GOVERNANCE & DOCUMENTATION

1. **Personal data inventory**
   First of all, actuaries should prepare a data inventory to identify all personal data they store or use in their processes and data treatments. For each data type they have to identify whether or not they use it and need it. If they do not use it and do not need it, then the best solution would be to delete it from the process. In other words, they should not receive this kind of data any more.
2. **Use authorisation**
   If they use it or need the data, they must formally be assigned the right to do so by their DPO or equivalent. It is important to note that the authorisation is done at individual level. Each person of the actuarial team should have the authorization. If it is not the case, appropriate access controls must be in place to ensure the security of the data processes.

3. **Gap analysis**
   Actuaries, in coordination with the DPO or equivalent, should by now have performed a gap analysis by comparing what has been communicated to the insureds concerning permitted uses of data to the actual use of the data. If there are gaps, actions must be taken to inform the insureds or change the corresponding data processing.
4. **Documentation**
   Because the insureds have the right to know how and for what purposes their data is processed, actuaries have to explain to their DPO or equivalent the reasons for the way in which they treat data. This explanation should give a meaningful overview of the intended processing.

TIP: nominate a data protection lead or representative in your team to be in charge of GDPR actuarial topics. This person should be proactive to avoid key data decisions in the company being made without actuarial validation.

ANONYMISATION or PSEUDONYMISATION

To reduce the impact of the GDPR, anonymisation should be considered. The principles of data protection do not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or is no longer identifiable. As mentioned before GDPR does not concern the processing of such anonymous information, including for statistical or research purposes.

TIP: anonymisation should be a company process and not an actuarial process. If it is done at the beginning of the data flow and fully centralised it will facilitate all the downstream activities, including actuarial work.

To determine whether a natural person is identifiable, consideration should be given to all the means reasonably likely to be used either by the controller or by another person, to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.

Pseudonymisation (the separation of data from direct identifiers so that linkage to a person is not possible without additional information held separately) is another tool available for easier handling of data in day-to-day work. It is different to anonymisation, since it is still possible to reverse the procedure and reveal the personal data again. Pseudonymisation reduces the risk associated with data processing significantly, but it is important to mitigate the risk of unauthorized reversal of pseudonymisation by having in place appropriate technical (e.g. encryption, hashing or tokenisation) and organisational (e.g. agreements, policies, privacy by design) measures to separate pseudonymous data from the relevant identification key. When making use of these tools in data processing, the data controllers and processors are required to ensure a high level of security by referring to state of the art methods generally recognized for the task.

ALGORITHMS

Profiling and automated individual decision making

The GDPR defines the concept of profiling as any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. In the insurance industry, this will include for instance any underwriting, direct marketing, targeted advertising and e-recruitment processeswhich are performed electronically, rather than by a human being.

Insureds have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

The insurance sector makes many decisions using machines without human intervention in the decision-making process. For example, some underwriting applications are designed to price risks and allocate premiums automatically. These are decisions based on automated processing without human intervention. For the right of the insured mentioned to be applicable, the automated processing should result in a decision, e.g. an automated portfolio analysis generating an automatic premium increase for a particular class of policyholder. If there is any form of human intervention, the right will not apply.

This right is not applicable if automated processing is necessary for entering into a contract between the data subject and a data controller – and this could very well be the case for insurance contracts. It is however important to note that the automated processing should then be related to the contract execution only. Where there is other processing which is not related to the contract, a compliance issue could arise. Moreover, third party automated processing could be refused by the insured if not specified in the initial contract.

Non-discrimination

Under normal circumstances, processing of personal data from the special categories defined in the glossary is prohibited unless the data subject has given explicit consent. This also includes seemingly neutral proxies indirectly resulting in identifications of this nature; e.g. basing a decision on whether a person went to a particular school or has a doctor of a particular gender or race.

Actuaries must ensure compliance with this requirement. They must use appropriate mathematical or statistical procedures for profiling, and implement technical and organisational measures appropriate to ensure that:

- factors which result in inaccuracies in personal data are corrected and the risk of errors is minimized;
- personal data is secured in a manner which takes account of the potential risks involved for the interests and rights of the data subject and which prevents, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or in measures having such effects.

Automated decision-making and profiling based on special categories of personal data should be allowed only under specific conditions.

Right to have an explanation

As mentioned previously GDPR gives the insureds the right to know and obtain communication in particular with regard to the purposes for which the personal data are processed. This is also true in the case of automated decision-making, where the data subject possesses the right to access "meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject." In order to enable this, actuaries should communicate and explain clearly to their stakeholders what they do with personal data. The undertaking should then be able to explain clearly and simply how the personal data of the insured is used, so he or she can make an informed decision to potentially opt out.

This is a challenge for actuaries, especially where individual decisions are made using for instance machine-learning techniques. Good machine learning models are very difficult to train and even harder to explain, and considerable thought will be required to explain outcomes effectively. The data subject needs to be educated to a degree that enables intelligent deselection of the processing of their data. Actuaries could consider describing the logic behind the model and the data it was trained on, before moving on to clearly listing the benefits of allowing the automated-processing and the downsides of opting out.

To learn more: full access to General Data Protection Regulation

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG

GLOSSARY

Special categories of personal data
Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data controller
The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes, conditions and means of the processing of personal data.

Data processor
The natural or legal person, public authority, agency or other body that processes data on behalf of the data controller.

Data protection officer
An expert on data privacy who works independently to ensure that an entity adheres to the rules, policies and procedures set forth in the GDPR.

Data subject
A natural person whose personal data is processed by a controller or processor.

Personal data
Any information related to a natural person (data subject) that can be used to directly or indirectly identify the person.

Personal data breach
A breach of security leading to the accidental or unlawful access to destruction or misuse of personal data.

Privacy by design
A principle that forces companies to include data protection mechanism in the design of a product or a process and not after its implementation, thus ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.

Processing
Any operation performed on personal data, automated or not, including collection, use and destruction.

Profiling
Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Anonymous information
Information which does not relate to an identified or identifiable natural person or to personal data. The regulation does not apply to the processing of anonymised information, including for statistical or research purposes.

Pseudonymisation
The processing of personal data such that it can no longer be attributed to a specific data subject without the use of additional information provided that such additional information is kept separately.