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

REGULATION FOCUS

GDPR, what does it mean for Actuaries?

On the 25th of May 2018, the European General Data Protection Regulation (GDPR) will be 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 citizen data will have to comply with this regulation. The GDPR is going to have a huge impact on the insurance sector.
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…

GDPR, WHAT DOES IT MEAN?

The European General Data Protection Regulation[1] (GDPR) came into force on the 25th May 2016 and applies to all EU and non-EU organizations offering goods and services to persons in the EU. Organizations had a 2-year implementation period to ensure full compliance. On the 25th of May 2018, organizations must be operating in full compliance with the GDPR. The aim of the GDPR is to protect all EU citizens from privacy and data breaches. Although the key principles of data privacy still hold true to the previous directive (established in 1995), many changes have been proposed.

Personal data' means any information relating to an identified or identifiable natural person ('data subject'); 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.

GDPR defines special categories of personal data. 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.

[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

DRAFT

The key points of the GDPR are the following:

New Scope

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

New Rights

Consent
Under GDPR, companies will no longer be able to use long, illegible 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 organization 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's 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 subjects' 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 use and machine-readable format' and have the right to transmit that data to another controller.

DRAFT

New Governance

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

Pseudonymization
It also puts forth the idea of pseudonymization, whereby identifying 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 party player like brokers or reinsurers.

Privacy by Design
It will be a legal requirement to consider data privacy on the onset of all projects and initiatives,
not as an afterthought.

Data Protection Officer (DPO)
Appointment 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 will be required to appoint a DPO. This will most likely apply to all insurers.

Data Breaches
Under the GDPR, breach notification will become 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 first having become aware of the breach. Data processors will also be required to notify their customers, the controllers, "without undue delay" after first becoming aware of a data breach.

New Fines

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

DRAFT

GDPR, WHAT DOES IT MEAN FOR INSURANCE?

Because data is the raw material of the Insurance industry, the GDPR has a significant impact on our sector. All functions, all processes, all employees will be impacted.

The main impacts can be classified in 3 categories:

- Business: does the GDPR create insurance business opportunities?
- Client relationship: how is the client relationship affected?
- Operations: what are the operating changes in the Insurance organizations?

BUSINESS

The GDPR should have an impact on the cyber and data breach insurance policies. Organizations will be focused on cyber risk and should be more open to cover it. Even if it is likely that the GDPR fines will be excluded from the cover, Insurers will be a good channel to get advice on the GDPR compliance.

GDPR should result in greater levels of transparency, which in turn will engender customer trust. It will allow insurers to clearly present to the customer the advantages of sharing data and be able to sell the right products with the right guarantees. The GDPR could be a good opportunity for the salesforce to know better the clients.

CLIENT RELATIONSHIP

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

<u>Consent</u>

Insurers will have to make sure that consent exists to use and profile a customer's data. Insurers should 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, such as by providing more personalized policies.

<u>Right to be forgotten</u>

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 as to when 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 them for statistical purposes. GDPR does not apply to data where the subject is no longer identifiable.

DRAFT

Data portability

Customers have control and ownership of their own personal data, allowing them to use their data for their own purposes and share it with organization they want. Insurers should therefore accept that access to this customer data is only temporary, and will stop the moment customers decide to change their insurer. If the insured chooses to switch insurance provider, the previous insurer will have to pass the corresponding data; before then erasing or anonymizing it from their records. Insurer 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 but also that they send it to their competitors. Insurers will need to design new processes to satisfy these requests, by remembering that they have less than one month to share the data with the insured.

OPERATIONS

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

Personal data should 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. Insurers will have the responsibility to ensure the compliance.

Many insurance products and policies rely on personal data being provided for all the chain value (underwriting, administration, claim management). Many of them, like health or travel insurance, require sensitive personal data. The GDPR has defined this special category data. The challenges for insurance is that, contrary to the healthcare sector, there is no specific grounds under the GDPR for processing sensitive personal data. Pseudonymisation could be the best solution for Insurance sector to comply with sensitive personal data. Even if the explicit introduction of 'pseudonymisation' in this Regulation is not intended to preclude any other measures of data protection. But, it is clearly written in article 26 that the principles of data protection should therefore 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 no longer identifiable.

The GDPR does not concern 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. Unfortunately, it is frequent that actuaries even if they do not use it, they receive in the extraction files non-anonymous data, such as first name, last name, social security ID, …

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

DRAFT

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 if they use it and if they 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 anymore.
2. **Use authorisation**
   If they use it or need it the data, they must ask to their DPO or equivalent the right to store and use this data. 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 sealing of the data processes.
3. **Gap analysis**
   Actuaries, in coordination with the DPO or equivalent, should perform a gap analysis by comparing what they communicated to the insureds and get specific consent for and what they are doing with the data. If there are gaps, they should take actions to inform the insureds or change the corresponding data processing.
4. **Documentation**
   Because the insureds can be informed of the existence of the processing operation and its purposes, actuaries have to explain to their DPO or equivalent the reason of treatment. This explanation should be intelligible and clearly legible manner, and give a meaningful overview of the intended processing.

   TIP: nominate a data protection referent in your team in charge of GDPR actuarial topics. This person should be proactive to avoid key data decisions in the company 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 no longer identifiable. GDPR does not concern the processing of such anonymous information, including for statistical or research purposes.

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

To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as testing, 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.

The International Organization for Standardization (ISO) defines direct identifiers as “data that can be used to identify a person without additional information or with cross-linking through other information that is in the public domain.” They are data points that correspond directly to a person’s identity, such as a name, social security number or contact information.

DRAFT

To mitigate the unauthorized reversal of pseudonymization risk, controllers should have in place appropriate technical (e.g., encryption, hashing or tokenization) and organizational (e.g., agreements, policies, privacy by design) measures separating pseudonymous data from an identification key.

TIP: if the pseudonymization is done at the actuarial process level, it is recommended to ask to IT people the ID creation and reversal process to ensure a good level of security.

ALGORITHMS

Profiling or automated processing

The GDPR defines the concept of profiling in article 4.4 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 processes which are performed electronically, rather than by a human being.

Automated individual decision making

The 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 given directly from 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. To be applicable, the automated processing should result in a decision, for example, an automated portfolio analysis generating automatically premium increase for a particular class of policyholder. But if there is any form of human intervention, the right will not apply. Based on the insurance business, it is likely that all calculations performed should have a legal effect on the insured (written premium, premium increase, claim refusal…).

This right is not applicable if there is a specific contract between the data subject and a data controller. The insurance contract should be a good argument to reject the right. But, it is important to notice that the automated processing should be related to the contract execution. It means that if there is other processing not related to the contract, a compliance issue could raise. Moreover, third party automated processing could be refused by the insured, if not specify in the initial contract.

TIP: include as much as possible a final human intervention step (e.g. peer review, sign-off) to limit the consequences of fully automated processing.

Non-discriminations

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric

DRAFT

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 are prohibited.

Actuaries must use appropriate mathematical or statistical procedures for the profiling, implement technical and organizational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimized, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that 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 that result in measures having such an effect. Automated decision-making and profiling based on special categories of personal data should be allowed only under specific conditions.

Right to have an explanation

Insureds must be informed on the automated processing done with their personal data. Actuaries have to communicate and explain to their stakeholders what they do with personal data. The salesforce should be then able to explain in easy words what it is done with the personal data of the insured.
The level of information depends on the nature of the processing and on the consequences of it. Here below a summary of the different situations:

	Decision based solely on automated processing which produces legal effects or significantly affects	*Decision based with human intervention or not producing legal effect or having no significant affects*
Profiling	Reinforced information to be provided	Semi-reinforced information to be provided
Other automated processing using personal data	Reinforced information to be provided	Regular information to be provided
Non-automated processing using personal data	Regular information to be provided	Regular information to be provided

To learn more: full access to General Data Protection Regulation

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

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 concerning health
all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject.

Data controller
The entity that determines the purposes, conditions and means of the processing of personal data.

Data processor
The entity 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.

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

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.

Pseudonymization
The processing of personal data such that it can no longer be attributed to a physical person.

DRAFT

To know more…

GDPR homepage (other languages available)

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

Swiss regulation (other languages available)

https://www.admin.ch/opc/en/classified-compilation/19920153/index.html

https://www.admin.ch/opc/en/classified-compilation/20071826/index.html

https://www.admin.ch/opc/en/classified-compilation/19930159/index.html

Switzerland & GDPR (other languages available)

https://www.edoeb.admin.ch/edoeb/fr/home/documentation/bases-legales/Datenschutz%20-%20International/DSGVO.html

http://www.ictjournal.ch

http://www.agefi.com

References

https://www.eugdpr.org

https://www.actuaries.org.uk/

GDPR Compliance For Dummies®, Informatica Special EditionPublished by John Wiley & Sons, Inc. 111 River St. Hoboken, NJ 07030-5774

Norme de Pratique relative à l'utilisation et la protection des données massives, des données personnelles et des données de santé à caractère personnel - NPA 5 https://www.institutdesactuaires.com

https://www.dacbeachcroft.com

https://home.kpmg.com/ch/fr/home.html

https://www.pwc.ch/en.html

https://www2.deloitte.com/ch/en.html

https://www.pwc.co.uk/industries/financial-services/regulation/are-you-ready-for-the-general-data-protection-regulation.html

www.lexology.com

https://aeonlaw.eu/expliquer-lalgorithme-droit-a-linformation-profilage-gdpr/

DRAFT

https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-8-pseudonymization/

https://www.iso.org

DRAFT