Mphasis
WYDE™
The Next Applied

Insurance: How To Comply Smoothly With The GDPR?

Best industry practices and IS for successful compliance

Insurance : How to comply smoothly with the GDPR - Best practices métiers et SI pour une mise en conformité réussie (best business and IT practices for achieving successful compliance) is a work published by Mphasis Wyde (103/105, rue Anatole-France, 92300 Levallois-Perret – www.mphasis.com).

Author : Philippe Payet (Managing Director, Mphasis Wyde Europe)

Editor-in-Chief : Baptiste Sevezen (Marketing Manager, Mphasis Wyde France)

Associate Editor : Contenteo (contenteo.com)

Editorial Staff : Delphine Tissier

Acknowledgements : Adèle Adam, Philippe Bouvier, Umberto d'Amico, Olivier Iteanu, Quang Nghiem, Clara Petit

CONTENTS

1.
Editorial

The General Data Protection Regulation (GDPR), which was introduced on 25th May 2018, is a major change that will impact the insurance companies in what they can do with their customer data.

Customer's personal data is the heart of the insurance business. This data processed by insurers comes from a variety of sources (customers who use the insurance service, the organisation's staff or even the third-parties when claims are notified), and also contains various types of information which can be highly sensitive (state of health, identity of individuals, bank details, etc.). Processing this data therefore requires the greatest prudence. The GDPR strengthens and unifies data protection from exploitation by –

- Guaranteeing data portability
- Right to be forgotten
- Reporting data breach

Insurance companies will have no choice, but to adapt to this new environment. They will have to appoint a Data Protection Officer (DPO) to oversee compliance, and to ensure that processors and service providers meet the same GDPR obligations or map out all the data held.

This whitepaper is an opportunity for Mphasis Wyde to share its guidelines and best practices for smooth adoption of GDPR requirements.

As a digital services provider and specialised publisher, Mphasis Wyde intends to accelerate digitalising for the insurance industry. In that respect, the company offers to help insurers tackle the GDPR: why does it directly affect the insurance profession? How does the regulation transform the industry and its relationship with the customer? What checklist is needed to factor in regulatory changes affecting the management tools?

As part of this, we also share our best practices and feature the guidelines of experts (partners, lawyers, industry specialists) for a reassuring changeover to the GDPR.

2.
WHAT THEY SAY

Introduced in 2016, the GDPR applied directly from 25 May 2018 in all European Union Member States. The process is irreversible. The GDPR does not only present a financial risk, given the heavy penalties, but also the risk of loss of goodwill.

Maître Olivier Iteanu
Lawyer specialised in law on information technologies, Cabinet Itenau

My main concern as DPO is the processing chain, because it is important to understand that if just one link is non-compliant or lacks the requisite security measures, the whole chain is weakened.

Adèle Adam
DPO of Claranet

Insurers want to gather more and more data: the GDPR lets them do anything they want, provided they obey established rules. If one wants to store as much data as possible, one only has to anonymise it so that its owner cannot be traced and archive it as and when retention periods expire. It is very new, and it will transform business, management and customer relations.

Quang Nghiem
Adviser at Crysal

As a software publisher, our role involves raising awareness among our customers about the impacts of the GDPR on the insurance profession, and show that we too are working on it. Among other things, we advise insurers to plan ahead with regard to data portability.

Philippe Bouvier
Product Manager at Mphasis Wyde

Anonymisation aims to irreversibly prevent the direct or indirect identification of the data subject concerned. Then it can no longer be considered personal data. This tool should be distinguished from pseudonymisation, which is a process within the meaning of the GDPR, and which ensures that a data subject can no longer be identified at a given point in time, but a rollback is possible.

Maître Clara Petit
Lawyer specialised in personal data and e-reputation, Cabinet Itenau

As a single entity dedicated to insurance, RCI Malta has to deal with issues specific to this sector, more particularly with a project aimed at identifying needs and impacts on core activities. We started working on this in March 2017. Follow-up workshops with detailed documentation on implementation and evangelisation are organised every month with the different entities of RCI Corporate.

Umberto d'Amico
IT Manager at RCI Malta

3.
Part 1 – What Is GDPR?

200 pages, 99 articles

OBJECTIVES

- Give individuals the control to their personal data
- Harmonise practices in all European Union Member States
- Strengthen the rights of data subjects, in particular by creating a right to portability of personal data
- Make data processors aware of their responsibilities
- Give credibility to the regulation through closer cooperation between data protection authorities

ORGANISATIONS CONCERNED

- All private or public-sector organisations (managers and processors) having a place of business in the EU, or offering goods or services to EU citizens

SANCTIONS

- Administrative fine of up to 20 million Euros or 4% of worldwide turnover if the basic principles of data processing are breached
- Fine of up to 10 million Euros or 2% of worldwide turnover if the process guaranteeing compliance is breached
- Right to compensation for the loss suffered for any victim of a personal data breach

CONTROL

- The supervisory authorities (the *Commission nationale de l'informatique et des libertés CNIL* for France) can intervene without prior notice and order for regular controls of compliance with the regulation, after an initial unintentional breach

GDPR: The key points

A new European regulation on data protection

The culmination of hard work by the European Member States, which commenced in 2012, the General Data Protection Regulation (GDPR), applied as of 25th May 2018, in all companies that collect, process and store personal data in Europe. Highlights of the key points to remember-

"Strengthen the control that European residents have over their personal data."

The main objective of the GDPR is to give European Union residents greater control over third-party use (private or public-sector organisations) of the personal data.

It unifies the legal framework for all European countries, and harmonises online security regulations that govern the companies. They must ensure that personal data is totally secure, everywhere and at all times, and protected against the risk of loss, theft and disclosure.

In technical terms, the new regulation not only makes up for the differences in applicability of the previous European directive of 1995 on data protection, but more importantly strengthens the regulatory framework, and adapts it to the digital revolution and the explosion in the volume of data, its collection and use.

The GDPR will have many important consequences. The changes most French companies expect include:

- **The obligation to notify the CNIL** (Commission Nationale Informatique et Libertés, the French data protection authority) of any data breach within 72 hours
- **The mandatory appointment of a DPO** (Data Protection Officer)
- Greater **control of processors**
- The right to **data portability**
- The **obligation to indicate the data storage period,** the right to access, modify and delete data (the right to be forgotten) by electronic means

Given the new sanctioning powers conferred on national regulators (the *Commission nationale Liberté et Informatique* in France), namely 4% of the total worldwide annual turnover of companies (against 150,000 Euros currently in France), companies will be well-advised to achieve compliance swiftly. Since from 25th May 2018, the GDPR imposed the "Accountability" principle, all controllers must be in a position to implement internal mechanisms and procedures that demonstrate compliance with data protection rules.

Expert opinion

"Introduced in 2016, the GDPR applied directly from 25 May 2018, in all European Union member states. The process is irreversible. The GDPR does not only present a financial risk, given the heavy penalties, but also the risk of loss of goodwill. There is a real business advantage in achieving compliance as quickly as possible. The new feature is the horizontal extension of the regulation: companies must apply it, but also "force" their processors and partners to do likewise to avoid the risk of incurring liability themselves."

Maître Olivier Iteanu

Lawyer specialised in law on information technologies, Cabinet Itenau

Why will the insurers be directly affected?

Personal data at the heart of the business

The insurance industry handles personal data on a daily basis; this includes both high-risk data (bank details, social security number, details of offences and court rulings and real-time global positioning data) as well as sensitive data (health, biometric data, etc.). Due to this, the insurance industry is in the front line as far as the protection of personal data is concerned.

With the GDPR in picture, the insurance industry is faced with a number of challenges: achieving compliance with this new regulation, continuing to collect data to meet the requirements of insured persons, continuing to be in a position to launch new and increasingly contextualised offers, preparing quotations, offering new types of insurance cover or financial services, handling claims and customer relations.

Personal data: A raw material for the entire business line

Today, healthcare industry has gone digital and e-health encompasses robotics, telehealth (social media, serious games, etc.), telemedicine (remote monitoring, homecare services, etc.) and m-health (healthcare services available on a smartphone or tablet, where 'm' stands for mobile, such as apps for connected objects or sleep sensors, heart rate, etc.). The growth potential for connected health is estimated at 4 to 7% per annum between now and 2020[1]. The data collected through such new technologies represents an essential raw material for all activities in the insurance business, but the challenge today is the need to know customers better in order to offer them personalized services and products.

[1] Study by Precepta entitled L'e-santé au chevet du système de santé français (e-health at the bedside of the French health system) (2014).

All this data is also useful for other departments of an insurance company, like marketing to create customer profiles and personalise their offers, offer renewed contracts, perform statistical analysis and research on claims, prevent offences, authorise loans and other verifications for keeping customer records up-to-date. A point that shouldn't be ignored here is that to achieve all this, the insurers may disclose their customers' personal data to processors or service providers, such as consultants, specialised advisors, subsidiaries in the same group, market researchers - within or outside the European Union.

Insured persons are regaining full ownership of their data

The GDPR clarifies everyone's roles and responsibilities so that customers can reclaim full ownership of their own data. It also seeks to give all data subjects the right to dispose their data and control the use thereof. As for insurers, the controller must make sure that these new rights are effective, by providing tools such as dashboards and online forms that are easily accessible when the insured person wishes to exercise his right to object and rectify, or right to erasure ("right to be forgotten", Article 17 of the GDPR). The GDPR also requires companies to inform people of the data storage period. Each contractual document must therefore be modified to that effect, by means of a tick box for instance. The restrictions imposed by the GDPR give insured persons new guarantee of accountability. This enables the insurer to heighten customers' confidence and alleviate their fears regarding the use of their personal data.

Expert opinion

"As a single entity dedicated to insurance, RCI Malta has to deal with issues specific to this sector, more particularly with a project aimed at identifying needs and impacts on core activities. Workshops are organised to categorise personal data. Work on achieving compliance started in our group in March 2017. Follow-up workshops with detailed documentation on implementation and evangelisation are organised every month with the different entities of RCI Corporate."

Umberto d'Amico

IT Manager at RCI Malta

40 years of data protection in the insurance industry

1978

JANUARY 6

Law no. 78-17 on computing, files and freedoms, amended by the law of 6 August 2004, defines the principles to abide by when collecting, processing and storing personal data. It strengthens people's rights to their data, provides for a simplification of administrative declaratory formalities and specifies the CNIL's powers of control and sanctions.

1981

JANUARY 28

Convention 108 for the protection of individuals with regard to automatic processing of personal data. This is the first restrictive international instrument that sets out to protect individuals against the misuse of automatic processing of personal data and that regulates cross-border transfers of data.

1995

OCTOBER 24

European directive 95/46/EC on the protection of individuals with regard to the processing of personal data. It forms the general legal framework for the protection of personal data in the field of computing, for the right to access and rectify data, the principle of consent, etc. Article 28 requires each member state to institute a personal data regulator modelled on the CNIL in France.

2014

NOVEMBER

Insurance Compliance pack signed by the CNIL and all insurers, marking their willingness to deploy digital technologies and utilise personal data in a responsible and exemplary manner. The objective is effective regulation that protects consumers and efficient utilisation of data collected for the industry.

Launch of work on the compliance pack for connected vehicle insurance. The challenge consists of integrating the "protection of personal data" dimension from the product design stage (the Privacy by Design notion of the GDPR) and in ensuring transparency, and control of their data by individuals.

MARCH

2016

APRIL 27

Adoption of Regulation 2016/679 by the European Parliament and Council (GDPR) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

2018

MAY 25

The GDPR enters into force. For all processing prior to this date, companies have two additional years to achieve compliance.

4.
PART 2 - HOW WILL THE GDPR AFFECT THE INSURANCE BUSINESS?

Controlled use of personal data, more customer confidence

How will the GDPR transform core insurance activities?

The volume of data has increased exponentially in recent years. Insurance is one of the industries that has a vested interest in exploiting and capitalising data in order to offer its customers the most suitable products and services. With the introduction of the GDPR and new data protection rules, what will be the practical consequences for the industry and how to seize this opportunity to transform the way it manages data and enhances its customer relations?

Over half of the insurance companies (and banks) have already identified and initiated processes concerning the GDPR, according to an Optimind Winter survey conducted in the summer of 2017. Nothing surprising about that, when we know that sector-specific regulation of personal data has already been in place for several years *(see our timeline 40 years of personal data protection, page 12)*. While the GDPR is clearly identified by insurers and mutual insurance companies, several stumbling blocks still remain intact, like reconciling it with the Insurance Distribution Directive (IDD), data mapping, staff awareness and the transformation of the customer relationship.

How to reconcile the IDD with the GDPR?

2018 is set to be a pivotal year, not just with the entry into force of the GDPR on 25th May, but also the Insurance Distribution Directive (IDD) three months prior to that.

The IDD, which supersedes the Insurance Mediation Directive (IMD1), aims to enhance the protection of consumers in their relations with all insurance distributors. The problem here is that the principles instituted by the GDPR and the IDD can at times contradict one another. For instance, the GDPR requires companies to collect only the data they need for processing purposes, whereas the IDD states that the insurer has a duty to collect information relating to customers' needs and behaviour in order to offer them suitable products. For a life insurance product under the IDD, a company is perfectly entitled to determine a customer's risk profile, even if this has no direct bearing on the distribution of the product. But this is prohibited by the GDPR because it imposes the obligation to use only the data required for processing purposes.

"For a life insurance product under the IDD, a company is perfectly entitled to determine a customer's risk profile, even if this has no direct bearing on the distribution of the product. But this is prohibited by the GDPR, because it imposes the obligation to use only the data required for processing purposes."

The IDD also requires controllers (as well as their processors) to keep registers of a certain amount of data relating to the customer relationship. But the GDPR imposes strict rules in matters of data retention and storage periods.
So what would be the most appropriate storage period to have sufficient control over one's distribution system while complying with customers' rights? *"One can comply with one law and be at odds with another", notes Mphasis Wyde's Product Manager, Philippe Bouvier. "To draw up a health and welfare insurance contract, the prospective customer has to complete a medical questionnaire in order to determine whether he or she can be considered to be at risk. The insurer must guarantee that it uses such data at the time of pricing before deleting it if it does not meet a regulatory obligation of storage or use for processing purposes. So it is important to set up a data deletion or anonymisation system."*

Our advice

The scope of the IDD does not encompass the protection of personal data. **Compliance with the GDPR is a priority**, both in strategic terms to remain in the running and in financial terms, given the heavy sanctions are possible.

What new relations should be established with processors?

Processors are required to meet specific obligations with regard to safety, confidentiality and responsibility. They now act as consultants vis-à-vis the controllers with regard to compliance with certain GDPR obligations (security breaches, destruction of data, contribution to audits, etc.). *"My main concern as DPO is the processing chain, because it is important to understand that if just one link is non-compliant or lacks the requisite security measures, the whole chain is weakened",* stresses **Adèle Adam,** DPO of Claranet, a company specialising in facilities management for critical applications. As a host of data for certain service offers, relating to health and banking among other things, Claranet works to strengthen contracts, as provided for by article 28 of the GDPR, *"Certain subjects were missing in Claranet's standard service contracts, such as subsequent processing clauses. We had to revise our models to offer our customers a framework in line with the requirements of the GDPR."*

Our advice

Data transparency and security go beyond the frontiers of the organisation. The processors too are directly concerned. As the guarantor of the data of your insured persons, it is your responsibility to **use the services of partners who present all the requisite guarantees in matters of data protection**. This is the principle of co-responsibility. A single link in this chain of compliance could wreck all your efforts to protect your reputation in this respect. The processor can be inspected and penalised by the CNIL on the same basis as the controller. Each link must be in a position to demonstrate that it complies, and guarantee that the service providers both upstream and downstream of the processing chain, meet the requirements.

How to heighten awareness about the protection of personal data among the staff?

"Leading insurers have already mobilised their teams in respect of the GDPR, and some of them are spreading the word among their subsidiaries and branches", explains Quang Nghiem, adviser at Crysal, an Mphasis Wyde partner firm specialised in health and social welfare insurance. As for mutual insurance companies, they are yet to achieve a high degree of maturity on the subject. Raising awareness about the new issues at stake involves training staff about them. So anyone involved in a project must be made aware of the security rules governing personal data, the related risks and consumer rights in this respect. The Data Protection Officer can organise awareness-raising sessions internally that can be approved by organisations: *"We are intensifying our awareness-raising initiatives via an e-learning platform offering programs devoted to the security and protection of personal data. The concept of "personal data" within the meaning of the law remains abstract for many people. A business e-mail address is a piece of personal data for instance, as it identifies an individual",* stresses **Adèle Adam**.

"The concept of "personal data" in terms of the law remains abstract for many people. A business e-mail address is a piece of personal data for instance, as it identifies an individual."

The GDPR concerns all the company's activities apart from the front office: marketing, which capitalises on the data, and also technicians (developers, integrators, etc.) or even staff dealing with the processors. Since the GDPR entails a review of contracts with customers and suppliers, it makes it mandatory to enter into certain agreements with processors or include contract clauses fixing the extent of the parties' responsibilities. It is important to review outsourcing policies by including the concept of co-responsibility, which safeguards us against the consequences of data leaks when activities are outsourced.

Our advice

As the rules governing personal data must become an automatic reflex for all your staff, raise their awareness about this new issue. **Provide more and more digital training material and documentation** to arouse their curiosity and heighten their awareness.

What impact does this have on management and the customer relationship?

"The requirement for explicit consent for each data processing task transforms the way you view the customer relationship. Henceforth, the profession of general agent should be practiced only with the personal data that is strictly necessary. If he needs more information, he must seek the customer's consent and explain the purpose of using the data element", warns Quang Nghiem. Under these circumstances, how can you continue using the data as it is now undeniable that data use and enrichment improves predictions, and gives you a head start on your competitors in terms of personalised services and products?

"The requirement for explicit consent for each data processing task transforms the way you view the customer relationship".

The challenge of customer relations and confidence is a real business issue for the years to come in the insurance industry. *"Insurers want to gather more and more data; the GDPR lets them do anything they want, provided they obey established rules. If one wants to store as much data as possible, one only has to anonymise it so that its owner cannot be traced and archive it as and when retention periods expire. It is very new, and it will transform business, management and customer relations,"* stresses **Quang Nghiem.**

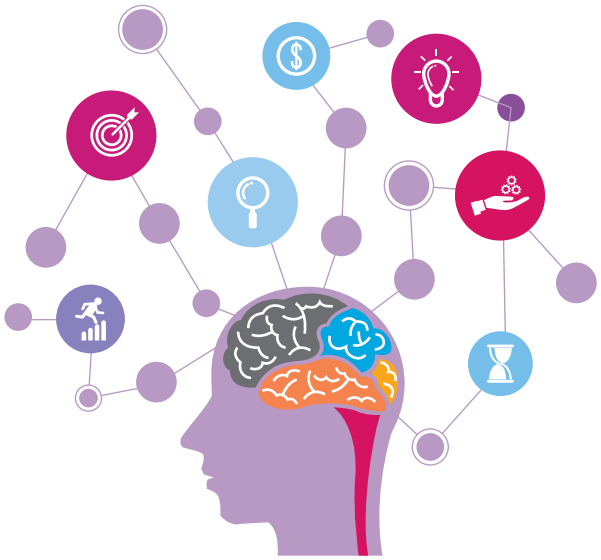
For insurance administrators (who use applications, and collect and process data), the GDPR strengthens several factors, such as the obligation to communicate all the data collected and the purpose for which it will be used, beyond management of the contract, to current and prospective customers before the contract is signed. Their task therefore consists of obtaining their formal and explicit consent. *"Article 6 of the GDPR sets out the six different fundamentals for lawful processing, including the processing necessary for the performance of a contract to which the data subject is party to, or even the consent of the data subject for one or more specific purposes. It must be possible to demonstrate such unqualified and well-informed consent. This may take the form of tick boxes for instance, with comprehensive information on processing in the insurance contract",* states **Maître Clara Petit,** a lawyer specialised in personal data and e-reputation, **Cabinet Itenau.**

Our advice

Don't regard the GDPR as a series of restrictions or a curb on data processing. Rather consider it as an **opportunity to boost confidence with your insured parties**. Being compliant with the regulation is ultimately a factor that will make you stand out from the competition and assert your good practices in matters of personal data protection. We can imagine organisations certifying the level of compliance that would then be a powerful marketing factor.

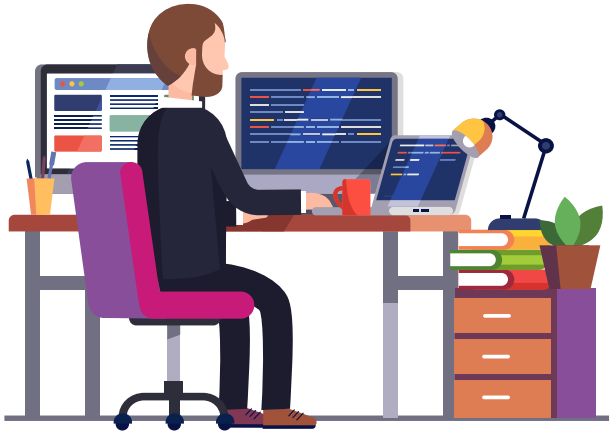
Best “insurance” practices to comply with GDPR

25th May 2018 was a deadline for implementing initial compliance measures. The CNIL pays attention particularly to evidence of compliance and to the efforts made by companies. Here are the best practices to prepare yourself.



Think across the board

Keeping data of a prospective customer for three years, for instance, is a valid principle for the front office, which needs relatively recent information. On the other hand, decision-makers, actuaries or even the marketing department may need a further two-year time to produce reliable statistics and gain better knowledge of the risks (number of claims, etc.). So it is important to properly harmonise rules governing data storage periods in order to satisfy all business requirements.



Work hand in hand with your software publisher

Learn to restrict user access. For instance, the health benefits service alone is allowed to access certain sensitive data, because the premiums service does not need to access such information. The higher the number of individuals who can access data that they don’t need to perform their tasks, the higher the risks are in terms of data security. In order to target dedicated administrators, all the data must be mapped out. This can be the subject of collaborative work between the software publisher and the insurance organisation. In small organisations, where staff does a number of different jobs, a veritable policy of change management in cultural, organisational and technical terms must be pursued.

Appoint a DPO with a hybrid profile

The Data Protection Officer (DPO) is the conductor of compliance. His appointment is mandatory in companies processing large volume of data to systematically monitor sensitive data to subjects or data. *"When a DPO is required, we recommend appointing an in-house DPO. From a point operational of view, he must be familiar with the architecture of his company, and with the legal and practical considerations ensuing from the business segment concerned. He must be easy to contact by staff"*, advises **Maître Clara Petit.**

The DPO can be multi-skilled: a corporate lawyer who understands computer language or a computer expert who knows legal requirements.If, in addition, your DPO already has core insurance skills or is a former CIL *(Correspondant Informatique et Libertés)* who has worked in the industry, then all the requisite expertise will be covered. Because his duties include not only ensuring that his company complies with personal data protection regulations, assisting controllers and staff involved by informing and advising them, but also supervising implementation of their files, cooperating with the CNIL, conducting impact assessments for high-risk processing, and finally guaranteeing the highest level of data security.

Expert opinion

"Appointing a DPO is becoming mandatory in companies processing large amounts of data to systematically monitor sensitive data subjects or data. As a facilities manager of critical applications, Claranet completely matches this configuration. It is important that we reassure our customers by showing them that we take the matter very seriously. Hitherto, the Correspondant Informatique et Libertés (CIL) only dealt with internal data processing. With the arrival of the Data Protection Officer (DPO), we need to have the capacity to address our internal compliance (the role of Controller) and our provision of services (the role of Processor)."

Adèle Adam

DPO and in charge of compliance for Claranet's e-health offer

5.
FACTORING REGULATORY CHANGES INTO MANAGEMENT TOOLS

Checklist for IT Departments

Distilling the spirit of GDPR into the tools

With regard to IT systems, it is not enough to merely add a layer of security to comply with the GDPR; the system as a whole must be transformed. IT staff must now take a very active interest in the data, its nature and life cycle, because one must now be able to say where such personal data is stored. To that end, it is essential to draw up a checklist of priorities.

Majority of consumers (83%) trust banks and insurance companies in matters of online security and data protection. Barely 30% trust the e-commerce sector, and only 13% trust telecoms operators and volume retailers. Paradoxically, only 20% of controllers in the banking and insurance industries consider themselves capable of detecting and countering cyberattacks[2]. Given this degree of trust, insurers should make the most of this GDPR opportunity to live up to the expectations of their customers. The cost of data theft in France is estimated at 30 billion Euros. 90% of vulnerabilities are concentrated in applications whereas 80% of security budgets are devoted to the infrastructure[3]. Hence, security policy must be reviewed to ward off the risk of cyberattacks.

How to make thousands of pieces of data stored secured in the IT system?

Guaranteed security of personal data is an important point of the GDPR. Besides the preventive measures required to protect the data, the CNIL must be notified within 72 hours in the event of data being compromised, lost or stolen. *"Claranet has adapted its processes (ISO 27001-certified since 2011), more particularly with regard to notification of data security breaches. For our customer to be able to assess the impacts and if necessary report breaches to the authorities and persons concerned, the nature of the incident, one of the mandatory criteria of the GDPR, has been added to our ticketing tool",* explains **Adèle Adam.**

"90% of vulnerabilities are concentrated in applications whereas 80% of security budgets are devoted to the infrastructure."

Reinforcing protection systems necessarily requires an increasing number of intrusion tests and audits. Artificial Intelligence could help in analysing logs and searching for possible fraudulent acts.

Our advice

In the matters of internet security, there is no room for a wait-and-see policy. It is essential to **have as many intrusion tests as possible,** update them at regular intervals and conduct annual audits. Anonymisation, for instance, will provide the assurance of minimising the damage in the event of theft.

[2] Report published by the Capgemini's Digital Transformation Institute entitled "The Currency of Trust: Why Banks and Insurers Must Make Customer Data Safer and More Secure" (2017).

[3] EMC study carried out in 2014.

How to map the data?

Within the framework of the future European regulation, companies are obliged to keep a data processing register. To have an inventory of all this data, a map is essential. Thousands of data units are indexed, regardless of the class of business (health, savings, welfare insurance, etc.), and the hardest task is to identify them. For that purpose, one needs to have thorough knowledge of the architecture of the tools. When the data is identified by class of business, it is up to the technical architects to identify it on a case-by-case basis. "It is advisable to install an automated process, but the human dimension is still imperative. One needs to identify who knows the tool best", says Philippe Bouvier. It is also up to the technical architects to find the hidden data. To do so, they need to evaluate the tool's database. To know where to look, thorough knowledge of the tools modelling is required.

"Personal data is scattered throughout the organisation's IT architecture. A comprehensive data inventory must stand the test of time."

The first task consists of mapping processes to know where the data is stored. "For that purpose, you need to interview all the in-house teams to understand how they work. We held several interviews to understand the data mapping changes that take place whenever new data is collected, and that shows the importance of a cross-functional approach between different lines of business," explains Adèle Adam. By mapping the processing of personal data, we can categorise the data (banking, health, biometric, social security number, etc.), determine the purpose of collection, the stakeholders (internal or external) who process it, and the data streams and potential transfers of data outside the European Union. "We launched a data management project to identify the data and then launched a process of anonymisation and custom development. These are not just regulatory problems, but involve the implementation of complex projects", notes Umberto d'Amico. All this data must be quickly accessible to allow data subjects to modify it, delete it (the right to erasure) or transfer it (the right to portability). Customer data is stored in business software and also in the marketing documents, in management reports and even in brokers' e-mails. In short, all this information is scattered just about everywhere in the IT architecture, not to forget all the paper records kept in the filing cabinets of small organisations. Compiling a comprehensive inventory of it seems to be a lengthy task.

Our advice

Compiling an inventory of all the personal data is a lengthy and tedious task, but an important stage in achieving compliance. In order to have an exhaustive overview, all the business units should be involved. In your processing map, remember to clearly indicate all the responsible persons (for processing or for operational services), as well as the processors who can access this data. Identify the categories of data and those regarded as the most at risk, and state the purpose of collecting such data and the storage period.

"All this data must be quickly accessible to allow data subjects to modify it, delete it or transfer it."

How to implement the right to erasure?

The GDPR allows data subject to exercise their right to erasure, in other words the right to have their personal data deleted, in six precise scenarios:

- The personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed
- The data subject's consent was required when the data was collected (this refers to cases of sensitive data)
- The data subject objects to the processing *"on grounds relating to his or her particular situation".* The controller must demonstrate that there are overriding legitimate grounds for the processing, for instance, cases of canvassing and profiling.
- The personal data has been unlawfully processed
- The data belongs to a minor
- Erasure is required by a statutory requirement (new law or court ruling for instance)

These restrictions are a lever of flexibility for putting in place the right to erasure. Indeed, the regulation states that available technologies and the cost of implementation should be taken into account. To delete the data, two processes are available: anonymisation and pseudonymisation. *"Anonymisation aims to irreversibly prevent the direct or indirect identification of the data subject concerned, which can then no longer be considered personal data. This tool should be distinguished from pseudonymisation, which is a process within the meaning of the GDPR, and which ensures that a data subject can no longer be identified at a given point in time, but a rollback is possible. These two processes require special technical measures to be put in place",* notes **Maître Clara Petit.** Each controller is obliged to ascertain that the data propagated externally, by processors for instance, has been erased.

Our advice

Before a data subject can exercise the right to erasure, we advise you to **plan different types of archiving**, one in an active database, a second intermediate type for the legal or litigation department, and a final stage in which the data is erased or anonymised. You can also allow for cases where certain data is preserved, as it will be converted into statistics to provide an overview of customer management. The idea is to always process as little data as possible for the purpose.

Expert opinion

"Many organisations are working on compiling an inventory of their data: Where is it stored? In paper records? In database-type archives? By the processors? Once the data has been categorised, it is essential to determine one's consent policy. A framing phase will assess the degree of compliance of what already exists with the new regulation, from a legal, organisational and IT point of view. Although this initial general road map is not enough in itself to achieve compliance, it has the merit of showing the CNIL that the company has provided initial proof, essential to mitigate the risk of sanctions!"

Quang Nghiem

Adviser at Crysal

Our solution

Wynsure in compliance with data portability as required by the GDPR

The Wynsure suite of solutions supports commercial functions and best practices in the insurance sector through end-to-end life cycle management of the entire ecosystem. It is a tool already rooted in good data protection practices, which is reinforced with the arrival of new principles like data portability and the right to erasure.

"As a software publisher, our role also involves raising awareness among our customers about the impacts of the GDPR on the insurance profession, and show that we too are working on it", assures Mphasis Wyde's Product Manager Philippe Bouvier. Wynsure is a suite of solutions that combines a modern front office based on a powerful back office (highly configurable, a set of insurance modules, etc.) in a single platform for consistent distribution through all digital channels.

Reporting to extract all the data

"We recommend making modifications in order to offer a GDPR-compliant product as quickly as possible, more particularly including the concept of data portability", adds **Philippe Bouvier.** Mphasis Wyde therefore suggests that you set up a reporting solution that can extract any type of data. *"Eventually, the aim is to make all areas of the tool accessible."*

A customer portal for the right to erasure

Mphasis Wyde urges you to set up a portal for the right to erasure. This customer portal appears to be an essential and practical way of retaining control over the data and have customers make modifications in real time, whether there is a change of address, removal of information or a request for consent. *"All paper records should disappear in the next 10 years, because this format defeats the object of the GDPR, namely data monitoring and control. With paper, there is no way of knowing which member of staff, internal or external, may have accessed customer information. The web portal is the ideal communication channel between an insurer and its customer",* concludes **Philippe Bouvier.**

Best practices for tooling oneself up

Security by design, data portability, protection of privacy by design - just some of the new concepts to master. Here are the best practices to prepare yourself.

Think about security by design

The approach known as "Security by Design" encompasses the modelling of risks and threats from the design stage of a tool or solution. This involves assessing vulnerability, analysing the risks to which the company is particularly sensitive, analysing the supervisory tool and their capacity to detect, qualify and notify a breach, and lastly, heightening awareness among the application developer teams. A company must be able to know which of its staff, customers and suppliers create the data in its IT system, and access the data and the applications. This is an opportunity to strengthen the various authentication systems.

Use reporting to export data

The trend is to find a comprehensive solution for data portability. Reporting is a native tool for certain major insurance groups. Other smaller organisations will need to set up specific processes for extracting data, such as manual identification of the data subject, data extraction requests. The limitation is that the insurer no longer has complete control over such processes. It has to be called in the publisher of the tool. It is also important to audit the tool to see whether it complies with the GDPR.

Apply protection of privacy at design time

The "privacy by design" concept presupposes about the protection of personal data before starting to design a product or service. This means taking technical, organisational and legal measures, such as data pseudonymisation or anonymisation. A Database Administrator (DBA) can perform this task with an automatic data encryption generator.This implementation involves all the business units participating in the process (marketing, legal, processor, statistics, etc.).

Audit your tools on a regular basis

An annual audit, at the very least, is advisable to apply updates. The software publisher should create control points, but without disrupting the development phases. *"This will also be a decisive factor for us as a publisher: for each major release, we will conduct an audit to ensure compliance. We are the guarantors of this building block to be integrated into the IT systems of insurance groups. It is a matter of co-responsibility",*
stresses **Philippe Bouvier.**

6.
EXECUTIVE SUMMARY

Among the current business issues affecting the insurance industry, the General Data Protection Regulation (GDPR) is quite focused or at least raises several questions regarding issues affecting the insurance industry.

The GDPR, which came into effect in 2016 and applied since 25th May 2018, to all companies and organisations that collect, process and store personal data in Europe, is underpinned by the protection of privacy and personal data. This new regulatory constraint has a major impact on both the core business and the IT department of companies.

The GDPR strengthens the rights of insured parties and imposes more stringent obligations on companies. This is an opportunity for them to transform their approach to data life cycle management and seize all available opportunities to stand out from the competition.

This whitepaper is an opportunity for Mphasis Wyde to share its guidelines and best practices for smooth adoption of GDPR requirements.

Author

Philippe Payet

Managing Director Europe, Mphasis Wyde

Philippe manages the operations of Mphasis Wyde, Europe. He is responsible for the Go-to-Market strategy, Business Development and oversees Technology Solutions Deployment Operations. With more than 19 years of experience in the field of new technologies in insurance and telecommunications, Philippe has in-depth knowledge of the insurance industry and has successfully managed major European accounts in the Telecom industries.

ABOUT MPHASIS WYDE

Mphasis Wyde is a global end-to-end Insurance Policy Administration Solution provider using Wynsure, a multi-language, multi-currency platform solution that can be deployed 'on premise' or 'on cloud'. Mphasis Wyde is headquartered in Bloomington, Minnesota, with offices in Canada, an R&D center in Paris, and a Centre of Excellence in India. Wyde was acquired in 2011 by Mphasis, a billion dollar publicly traded Information Technology services provider. Mphasis enables customers to reimagine their digital future by applying a unique formula of integrated cloud and cognitive technology. Mphasis X2C$^{2}_{TM}$ formula for success (shift anything to cloud and power everything with cognitive), drives five dimensions of business value with an integrated consumer-centric Front2Back™ Digital Transformation. Our integrated Wyde plus Mphasis solutions offering is aimed at creating value for our customers, helping them improve their business with minimum hassles and capital outlays. A perfect blend of domain expertise, technical excellence, business intelligence and customer experience management is what makes us endearing to our clients.

For more information, log on to
www.wyde.com

www.wyde.com

VAS 10/04/19 A4 SIZE BASIL 5293

Mphasis WYDE™
The Next Applied