Position Paper

Response to EC new questions to inform the preparation of the evaluation & review report of May 2020 on GDPR application

Our reference:	COB-DAT-20-011	Date:	29 January 2020
Referring to:	European Commission's preparation for its evaluation and review report on the application of the GDPR of May 2020		
Contact person:	Ana-Maria Llorente, policy advisor conduct of business	E-mail:	llorente@insuranceeurope.eu
Pages:	11	Transparency Register ID no.:	33213703459-54

Insurance Europe welcomes the opportunity to contribute to the preparation by the European Commission (EC) of its report on the evaluation and review of the General Data Protection Regulation (GDPR) due by 25 May 2020.

The responses to the EC new questions below should be read in conjunction with Insurance Europe's contribution to the EC stocktaking exercise of April 2019. These responses are based on the feedback of Insurance Europe's members and their 20-month experience with the application of the GDPR.

5. Experience with Data Protection Authorities (DPAs), the one-stop-shop mechanism (OSS) and the consistency mechanism (opinions under Article 64 GDPR):

c. Are the guidelines issues so far by the EDPB meeting your expectations as to the clarification of notions the GDPR uses/provision of legal certainty? [https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en]

The European Data Protection Board (EDPB) guidelines can be useful implementation and compliance tools. They can help to clarify and, therefore, meet GDPR requirements, while promoting consistent interpretations across the EU.

However, Insurance Europe would like to highlight the following important issues:

- The EDPB guidelines often exceed the requirements established in the GDPR and as such create unjustified additional constraints. Insurance Europe has attached in an annex examples of where EDPB guidelines go beyond the letter and spirit of the GDPR. These examples are extracted from Insurance Europe's contributions to consultations on the EDPB's draft guidelines.

  Insurance Europe recommends that EDPB guidelines that establish requirements that go beyond GDPR obligations should be revised to be aligned with the GDPR. Insurance Europe

Insurance Europe aisbl
Rue Montoyer 51, B-1000 Brussels
Tel: +32 2 894 30 00 • Fax: +32 2 894 30 01
E-mail : info@insuranceeurope.eu
www.insuranceeurope.eu

also takes the view that clarifications are needed to make it clear that guidelines are only of interpretational function and that the EDPB does not have the competence to develop additional requirements that exceed the GDPR.

- EDPB guidelines are often drafted in a way that requires additional interpretation (on top of the interpretation of the GDPR rules) by those who have to abide by the rules and by Data Protection Authorities (DPAs). This is not only defeating the very purpose of the guidelines – ie, to clarify data protection provisions and to promote a common understanding of European data protection laws across the EU – but also prevents their direct application.

  The EDPB should therefore ensure that its guidelines provide appropriate legal clarity and do not leave room for various interpretations.

- National policy documents and guidelines may only be available in local languages. To improve the consistency mechanism, it would be helpful for DPAs to provide a version of these documents in English and for these to be made publicly available on the EDPB website.

- In relation to gold-plating, our Dutch member reported an example of differing guidelines on the interpretation of "legitimate interest".

  On 1 November 2019, the Dutch DPA published a policy document laying out its views on legitimate interest as a legal basis for processing personal data. The DPA gives a number of new and far-reaching interpretations to this legal basis. These interpretations have been criticized by legal scholars and prominent lawyers in the Netherlands. The most concerning aspect is that the DPA rules out purely commercial interests and profit maximization as 'legitimate', therefore excluding it from reaching the necessity- proportionality- subsidiarity and balancing test (legitimate interest assessment).

  This interpretation is inconsistent with recital 47 of the GDPR, which explicitly notes that "*there is legitimate interest where there is a relevant and appropriate relationship between the data subject and the controller in situations as where the data subject is a client or in the service of the controller*". The interpretation of the Dutch DPA also conflicts with the interpretation of the ECJ in a number of cases and with the Article 29 Opinion on legitimate interest 06/2014[1].

  The Dutch DPA document causes legal uncertainty and unnecessary burdens, and it undermines the GDPR objective of "one law for the 28 member states". Furthermore, the Dutch DPA interpretation pushes for an unnecessary shift towards consent where this is not necessary. There is no hierarchy between legal basis provided under Article 6 of the GDPR. Consent may not always be the most convenient legal basis from the data subject point of view, and excessive reliance on consent may drive consumer fatigue.

  Importantly, as regularly pointed out by the European Commission, gold-plating creates an increasingly fragmented interpretation of the GDPR across member states and it should therefore be avoided[2/3].

[1] 'https://iapp.org/media/pdf/resource_center/wp217_legitimate-interests_04-2014.pdf

[2] "In some instances, Member States have introduced national requirements on top of the Regulation, in particular through many sectoral laws and this leads to fragmentation and results in creating unnecessary burdens.", European Commission's Communication on "Data protection rules as a trust-enabler in the EU and beyond – taking stock", July 2019

[3] "We must avoid fragmentation and temptation for adding additional conditions or expansive interpretation for the GDPR. The Commission will not tolerate the so-called 'gold plating'.", Commissioner Věra Jourová's intervention at the event "The General Data Protection Regulation one year on: Taking stock in the EU and beyond", June 2019

d. Considering the guidelines from the European Data Protection Board (EDPB) that have already been issued, in which area additional EDPB guidelines would be useful?

The ECJ rulings C-210/16 and C-40/17- Holstein and Facebook, and Fashion ID and Facebook – have set a very broad interpretation of joint controllership. Some national insurance associations interpret that the criteria used by the ECJ goes too far since it makes nearly every data processing activity carried out in cooperation with other companies fall under Article 26 GDPR (joint controllership).

This has created a situation of confusion where it is very difficult to distinguish what a joint controllership relation is and what it is not. This can create difficulties at the time of signature of contracts with data processors. Therefore, it would be useful to have guidance from the EDPB to better distinguish which relations fall within the notion of joint controllership.

In addition, the Spanish insurance association believes that additional matters may be addressed by the EDBP through guidelines with a view to achieving clarity and consistency, for example:

- Further clarifications about the appropriate legal bases to use depending on the different types of processing activities.
- The application of legitimate bases, in particular legitimate interest, public interest (essential public interest), treatment for assistance or treatment of assistance.
- The management of health care systems and services of Article 9.2(h) GDPR.
- The legal regime for the communication of personal data to third parties, the change of purposes, as well as the information obligations when the data is not directly collected from the data subject.
- The specific requirements for service providers establishing the minimum warranties required from those services suppliers, and the relation among those and their clients, beyond the mere controller-processor relationship.
- A firm commitment to risk management models applicable to the processing of personal data, based on a common methodological basis, to be developed, but with common foundations.

g. Are there any difficulty experienced in the dealings with DPAs in the context of complaints investigated under the OSS?

In September 2019, the Dutch DPA announced that the process to approve Binding Corporate Rules (BCRs) would take between three to five years due to the heavy workload. Complaints also take a long time to be processed.

The Dutch DPA often says that it has a heavy workload, affecting the period required to answer to, for example, complaints or data breach notifications.

A company reported that it had submitted Binding Corporate Rules (BCRs) for approval on April 2019 and that it has not had any decision from the DPA yet.

h. Do you think that the application of the consistency mechanism in the sense of Art 64(1) GDPR lives up to its expectations?

Insurance Europe's members reported that, overall, the consistency mechanism needs to be improved based on DPAs' and companies' experience.

The following examples were reported:

- In its guidance on legitimate interest, the Dutch DPA explained, among others, that the pursuit of purely commercial interests cannot serve as a legitimate interest, neither can the tracking of the behaviour of potential clients.

  This guidance is inconsistent with the guidance from the UK DPA, as well as with recital 47, which states that the "*processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest*." and that legitimate interest could exist where "*there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller.*"

  Our Dutch member is concerned that consumers will not benefit from this approach, because the less room there is for 'legitimate interest', the more will be left up to consent and thus consent fatigue. In that case, the customer will draw the burden of having to weigh the differing interests.

- National DPAs have published guidance on data protection impact assessments (DPIAs) containing very different criteria. For example, a guideline by the French DPA (CNIL) mentioned that DPIA are not required while the Dutch DPA noted that for that same situation DPIAs are required[4]. There are also differing opinions and approach in Denmark.

6. Experience with accountability and the risk-based approach (for members representing businesses):

b. How do SMEs cope with the implementation of accountability and the risk-based approach? Do they get advice from DPAs and/or from their associations?

Insurance Europe's members reported the following:

- In the Netherlands, the current exemption in the GDPR is of no use in practice. In practice every company needs to follow every GDPR requirement and carry out DPIAs even if the risk is low.

- In France, CNIL has published a list of categories of data processing that do not require impact studies in order to avoid, particularly for SMEs, significant and unnecessary costs.

- The Spanish DPA, as the French one, published a list of categories of data processing that do not require DPIAs. It has also published tools to facilitate the risk-based approach (practical guide to analysis for the processing of personal data, and impact assessment guide for data protection) on which data controllers and data processors can rely to carry out risk analysis and impact assessments of the personal data processing they carry out. It has also developed several computer tools to facilitate compliance with the GDPR, especially

[4] Dutch DPA list for required DPIAs: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stcrt-2019-64418.pdf

with the accountability principle, and aimed above all at SMEs and public administrations, such as:

- *FACILITA RGPD* enables the development of the record of processing activities and the establishment of guidelines for data controllers in relation to low-risk processing activities.

- *GESTIONA EIPD* assists for risk analysis and data protection impact assessments.

The impact of these initiatives, ie, whether they effectively facilitated compliance, has not been evaluated yet. It should, however, be noted that, these initiatives aim to provide support for not too complex data processing activities and are not relevant for activities such as high-risk data processing. Moreover, their use does not generate outputs that are directly applicable for effective compliance and require subsequent adaptation.

7. Data protection officers (DPO):

f. ***What is the experience as regards the cooperation between DPOs and the DPAs? Do the organisations you represent get advice from DPAs and/or from their associations?***

Insurance Europe's members reported the following:

- The German data protection authorities take part in regular meetings with the DPOs of insurance companies. The DPOs have the opportunity to raise questions with their DPAs at these occasions. Furthermore, the German DPAs have published interpretations, instructions and guidelines on the GDPR.

  Moreover, it is established that DPOs of insurance companies meet twice a year to discuss issues of common interest.

- The CNIL has adopted a dialogue-based approach with different stakeholders. This cooperation allows companies to be better supported in their application of the GDPR for the benefit of consumers.

- The Dutch DPA is still unexperienced if compared to other authorities such as the financial conduct supervisory authority or the Dutch national bank. For example, the Dutch DPA does not submit all its policy documents for consultation, which causes unnecessary stress for companies. Moreover, the Dutch DPA does not have enough resources for the supervision of financial markets. There are currently only three experts working on all financial markets.

- In Denmark, there is no dialogue established between insurance company DPOs and the DPA. The forum for cooperation and dialogue with the DPA is broader; contact with the DPA is done through DPO associations.

- In Greece, there is not any established mode of cooperation between the Greek DPA and DPOs of insurance companies. It should also be noted that the Greek DPA is rather understaffed.

9. **Have you experienced or observed any problems with the national legislation implementing the GDPR** (e.g. divergences with the letter of GDPR, additional conditions, gold plating, ***fragmentation***, etc.)?

Experience on GDPR fragmentation and divergence differs between jurisdictions. Insurance Europe's members reported the following:

- The GDPR principles are in line with most of the legal provisions already established in France. Similarly, new national laws and draft laws are consistent with the GDPR.
- The Netherlands has chosen to continue the national implementation and derogations as it was for 20 years under national law based on directive 95/46/EG. If those derogations fitted 95/45/EG, they should also fit GDPR.
- The Greek Law implementing the GDPR is ambiguous and diverts from the letter of GDPR. Thus, the Greek DPA has announced the need for amendments.
- In general, the Spanish personal data protection regulations are consistent with the provisions of the GDPR. However, they do establish additional conditions that have been imposed by the Spanish DPA through pronouncements, guides, sanctions, etc. These are related to, for instance, data processing in video surveillance systems, data processing in advertising exclusion, credit information, etc., or that are stemming from the law, such as the requirements on blocking data or the way to obtain consent.
- There are examples of fragmentation at national level due to the different interpretations of the DPAs concerning DPIAs or for example different opinions on the scope of legitimate interest.
- The non-uniform application of the GDPR across member states for processing health data in an insurance context can create obstacles to cross border operations.
- There is no uniform interpretation between DPAs on the criteria to trigger the obligation to notify data breaches (see question on data breaches).
- A general and agreed concern among insurance associations is that governments tend to think that the GDPR solves everything and, as such, no further action is necessary. Governments should be more active to cover any remaining legal vacuums at national level.

10. GDPR and new technologies

a. How do you assess the overall impact of GDPR on the approach of organisations you represent to innovation?

In some cases, the GDPR hinders the development of innovative products and services that are based on automated or digital processes involving the processing of personal data. For example, the unclear scope of Article 22 GDPR and its narrow exemptions are obstacles to the digitalisation of processes. Importantly, the EDPB interpretation to the exemption "necessity to perform or enter into a contract" in its guidelines on automated processing and profiling, makes it more difficult to offer innovative products, such as real-time travel or telematics insurance.

b. *How do you assess the impact of GDPR on the development of new technologies, such as artificial intelligence, blockchain, internet of things, etc.? Please provide concrete details.*

GDPR principles such as purpose limitation, data minimization and storage limitation make it difficult to test new applications and use data to train AI applications. As a rule, this is not possible with anonymised data because the controllers must monitor the effects of the software.

Blockchain technology has shown that the GDPR is not always compatible with technological developments. The nature of this technology is incompatible with the right to be forgotten, raises many questions on the right to access and on controllership.

It is worth mentioning that some DPAs have noted these incompatibilities:

- The French DPA published in October 2018 a note on the compatibility between blockchain and the GDPR. CNIL cooperated with business stakeholders in order to examine the creation of GDPR-compliant blockchains.

- To address the fact that GDPR unintendedly hinders the development of these types of new technologies, the Spanish DPA has published several notices and press articles related to the use of drones, blockchain and anonymisation with a view to establish a common standard for the use of those technologies.

  The Spanish insurance association considers these tools to be very useful, but points out that additional steps would be necessary to address other technologies, such as Internet of Things (IoT) and its impact on privacy.

c. *Do you think that GDPR provides sufficient protection for the trustworthy development of new technologies such as artificial intelligence?*

The GDPR already provides sufficient protection for the trustworthy development of new technologies, notably AI. Further legal restrictions would risk preventing innovation and the digitalisation of processes.

Furthermore, there are currently many different regulatory initiatives at European and national level on the trustworthiness of AI and new technologies. For example, the EC expert group on AI published guidelines on Trustworthy AI, the Dutch national bank has published its own guidelines, the EC has announced a legislative initiative on AI and the European Insurance and Occupational Pensions Authority (EIOPA) has established an expert group to develop guidelines on digital ethics, covering AI. In that respect, Insurance Europe believes that a holistic approach and effective coordination between all the relevant authorities are necessary to avoid any risks of duplications or inconsistencies between these various initiatives.

d. *In respect of artificial intelligence, what could be the potential gaps with respect to the protection of individuals' personal data for which further policy action may be necessary?*

-

11. Codes of conduct (under Article 40 GDPR)

a. Is your organisation engaged into the preparation of a Code of conduct? If yes, what is your experience with the preparation of such a Code?

Insurance Europe's members have reported a general willingness at national level to develop codes of conduct. However, they are often discouraged from developing codes of conduct due to the excessive requirements imposed by the EDPB guidelines or due to the risk of being fined if they do not enforce it properly (Article 83(4) GDPR).

Some end up adopting halfway solutions such as, codes of conduct that are not formally submitted for DPA approval due to the impossibility of financing a monitoring body, self-regulatory guidelines or national standards.

Insurance Europe's members reported the following examples:

- The Czech insurance association reported the willingness of their market to adopt a code of conduct, as well as the impossibility to do it due to the economic cost to maintain the monitoring body on the long term. Consequently, they opted for the adoption of a self-regulatory standard.

- The German insurance association has developed a code of conduct for the German insurance industry. The content has been approved by the German DPAs. Nevertheless, the association is reluctant to submit the code of conduct for approval according to Article 40 (5) GDPR. In their opinion the demand of a controlling body in the Guidelines 1/2019 goes far beyond the GDPR provisions. This will prevent controllers from implementing codes of conduct. The association is concerned about the continuation of the code in the long run due to the excessive costs to maintain the monitoring body.

- The Spanish insurance association is actively involved in the creation of a code of conduct for the insurance sector under GDPR. The code is currently being developed and it has been presented to the Spanish DPA last December.

  Moreover, the association is currently working on the standard codes registered in the General Data Protection Register for their adaptation to the GDPR and is in continuous contact with the Spanish DPA to this end.

  While this process is being completed, the association has published a Guide on the processing of personal data by insurance companies, which aims to help member insurance companies to adapt to the new national and EU rules on personal data protection.

  A Protocol for the improvement of GDPR understanding and application at the insurance industry has been recently signed between the Spanish DPA and the Spanish insurance association.

- The French insurance association opted for the development of a set of pedagogical guidelines to assist the insurance industry. The development of a code of conduct is not possible due to the too high financial costs.

- The Dutch insurance association updated their existing and formerly approved code of conduct in 2018. This cost over €100.000 in legal fees and the preparation took over a year. Because of the EDPB guidelines on codes of conduct, and especially the mandatory monitoring body, the Dutch insurance association chose not to submit the code to the DPA

for formal approval. They have a self-regulatory mandatory code for all members, but that is not approved by the Dutch DPA.

- The Danish insurance association has for the same reasons opted to develop a self-regulatory "GDPR seal".

- The Greek insurance association has developed a draft code of conduct specifying the way Greek insurance companies comply with the GDPR. The preparation took over a year and an external legal consultancy was needed. The first draft code was submitted to the Greek DPA in August 2018, prior to the publication of the EDPB draft guidelines on Codes of Conduct & Monitoring Bodies. Based on these guidelines, the DPA - before carrying out an in-depth evaluation of the code, asked for clarifications and supporting documentation, and, among others, asked for the development of mechanisms for the effective monitoring of compliance, and the establishment of a monitoring body. Following these requests, the Greek insurance association rephrased several articles of the Code and provided for the establishment of an internal Monitoring Committee aimed to carry out the compliance of the code's provisions by member companies. In August 2019 the Greek association resubmitted the Code to the DPA. The Code is still under review.

  The Greek association is concerned about the outcome of the DPA's decision on the insurance code. In case the DPA insists on the establishment of an independent external monitoring body, the financial burden of maintaining such a body might be unaffordable for the Greek association. If the DPA rejects the code, the Greek insurance association will consider the option for the adoption of a self-regulatory standard/ guidelines.

12. Data breach notifications (under Article 33 GDPR)

a. Have organisations that you represent notified a data breach?

Insurance Europe's members reported on the very different criteria and thresholds applied by DPAs to trigger the obligation to notify data breaches. The following examples were reported:

- The French association did not receive any notification from any of its members about it and the DPA has not yet publicly act against an insurer for data breach reasons.

- The Danish DPA has a very strict practice on data breach notifications. The threshold to meet the obligation to notify a data breach is very low. The DPA published a report on breaches every quarter. In 2019, the insurance and pension industry notified 206 breaches while 2780 breaches were notified in total – including public institutions and private companies. The DPA assesses the type of breaches and if there is repetitiveness then they issue recommendations.

- The German DPAs apply a very strict interpretation, the threshold to trigger the obligation to notify a data breach is very low. For example, even if the breached data is encrypted the company is obliged to notify it to the DPA. There were 12.600 breaches notified between May 2018 and January 2019.

- The Dutch DPA received 15.400 data breach notifications between May 2018 and January 2019. 20% belonged to the financial sector and 19% to the public sector.

- The Greek insurance association is not aware of any data breaches by insurance companies. The Greek DPA received a total of 80 data breach notifications in 2018. The DPA proceeded to examine 13 of the notified breaches, and imposed reprimands on three data controllers. The information on data breaches is not available for 2019.

b. What is their experience with data breach notifications?

The volume of data breach notifications varies significantly between jurisdictions. For example, the DPA of Bavaria had to process 2376 notifications between 25.05.2018 and 31.12.2018, while the French DPA merely had to process 742 between 25.05.2018 and 01.10.2018, and the data breach notifications doubled in the Netherlands to 20.881 for the year 2018.

The Spanish DPA publishes a monthly report with metrics and indicators in relation to data breach notifications. For 2019, a total of 1473 notifications by data controllers and data processors were reported as of November 2019. Notifications are made to the DPA through its website, which provides for a web form containing all the information that has to be provided by data controllers and data processors to assess the scope and impact of the notified data breach. The process is usually considered as fairly simple to use and the notification of breaches does not automatically result in the opening of a sanctioning procedure.

With regard to experiences, national associations reported the following:

- In Germany, companies and data protection authorities are overwhelmed by the amount of data breach notifications. The reason for this situation lies in the fact that the threshold of incidents to be reported has been significantly lowered in relation to the national law before the GDPR. The individual cases to be reported are often not significant, such as misdirected letters. In this respect, the interpretation of which incidents are to be reported does not appear to be uniform in the Member States. § 42a of the former German Data Protection Act contained the duty to notify data breaches only in cases where there was a real risk for data subjects. This would be a reasonable restriction.

- In the Netherlands, in most cases, data breaches are reported and then never heard from anymore. In some cases, the DPA asks questions, such as whether the breach was notified to customers or what measures were taken to prevent further harm. Contact is usually quite slow though, because the DPA receives many complaints and breaches. Dutch financial institutions already had to report breaches to financial authorities for many years, so reporting to the DPA was not a big shift. The reporting procedure is reported to be not very practical though.

- The Danish insurance association suggested that the introduction of a de minimis rule would be useful.

- The Spanish DPA has published a guide for the management and notification of data breaches to assist data controllers and data processors in meeting their obligations under GDPR. The guide explains how to notify the breach in practice and it includes a system to assess objectively whether a data breach should be notified to the DPA as well as to the data subjects. This system was reported by companies as very useful.

13. Adequacy decisions and other transfer tools:

a. Do the organisations you represent rely on adequacy decisions for their international transfers and, if so, which are the main "destination" countries/territories to which data is sent using this transfer mechanism?

Insurance Europe's members mentioned the adequacy decisions for Switzerland and Israel. However, not every market relies on these decisions for the transfer of international data.

b. *What is you experience with using adequacy decisions as a mechanism for transferring data? Did you encounter any particular question or concern when relying on any of the adequacy decisions adopted under the 1995 Directive (with the exception of the EU-US adequacy decision which is covered by a separate, and annual, review process)?*

-

c. *Do you have any information on the developments of the data protection system of any of the countries/territories subject to a Commission adequacy decision under the 1995 Directive that you would consider relevant for the Commission's evaluation?*

-

d. *In your view, should any other third country be considered by the Commission in view of a possible adequacy decision?*

Insurance Europe's members mentioned the UK and India, as well as the South American countries (eg Brazil, Chile, Mexico, Colombia, etc.) whose national legislations establish obligations and guarantees for the protection of privacy that are equivalent to the GDPR.

e. *What other transfer mechanisms from the GDPR toolbox should be developed as a matter of priority?*

Standard contractual clauses (SCCs) should be revised in light of the GDPR. Moreover, it would be useful if the EC develops SCCs for the transfer of data between processors.

It would also be useful to develop certification mechanisms so that companies based in countries without an adequacy decision could rely on this mechanism and be considered adequate data importers.