Position Paper

Response to EC stocktaking exercise on application of GDPR

Our reference:	COB-DAT-19-032		
Referring to:	European Commission stocktaking exercise on the application of GDPR June 2019		
Contact person:	Ana-María López-Chicheri Llorente, Policy Advisor, Conduct of Business		
Pages:	15	Transparency Register ID no.:	33213703459-54

Insurance Europe welcomes the opportunity to participate in the European Commission stocktaking exercise on the application of General Data Protection Regulation (GDPR) due in June 2019.

Insurance Europe's responses are based on the preliminary feedback received from fourteen markets (CY, CH DE, DK, EL, ES, FR, IT, MT, NL, NO, PL, SE, HU), based on their experience with the GDPR application over the last 10 months. Therefore, Insurance Europe would provide additional input should new experiences be shared, or further issues arise.

Insurance Europe stands ready to continue engaging with the European Commission and contribute to its stocktaking exercises ahead of the GDPR review.

1. What were the main issues experienced by your organisation in complying with the GDPR (please explain)?

The main issues reported by insurers so far are:

- Difficulties in classifying suppliers as either controllers or processors, difficulties in adapting processor agreements, and allocating liability between the controller and the processor.
- Updating IT systems to ensure compliance (eg, privacy by design and by default, automated deletion of data when data retention periods are met).
- Implementing deletion of data in IT systems. One of the key difficulties observed in this area concerns the decentralisation in the storage of data.
- Non-uniform application of the GDPR across member states regarding issues of high importance for insurers. In particular, there are different legal bases across member states for processing health data in an insurance

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

© Reproduction in whole or in part of the content of this document and the communication thereof are made with the consent of Insurance Europe, must be clearly attributed to Insurance Europe and must include the date of the Insurance Europe document.

context. This situation creates difficulties for insurers that conduct their business in multiple member states to comply with data protection rules.

- Difficulties in complying with transparency requirements vis-à-vis parties that are not contracted with the insurance company (eg, beneficiaries, data subjects whose data is processed in the context of third-party liability insurance).

2. Impact of the GDPR on the exercise of the rights:

a. ***How have the information obligations in Articles 12 to 14 been implemented? Has there been a change of practices in this respect?***

- Insurers have modified their information clauses to add the new information obligations required by the GDPR. In this regard, a number of companies will adopt the layered approach mentioned in the Article 29 Working Party's Transparency Guidelines to provide the information obligations in Articles 12 to 14 GDPR.
- A national insurance association reported having developed and adopted guidelines on personal data processing by insurers, which include recommendations on how to improve transparency (eg, layered information).
- Another market reported that fulfilling the information obligations has required significant efforts and resulted in complex and costly information campaigns for the industry. This is because, although the layered approach and the use of more than one medium are permitted, the national data protection authority (DPA) stated that changing mediums to inform data subjects under the obligations in Articles 12-14 should be avoided when informing data subjects. However, in practice, when, for example, the initial contact with the data subject takes place via telephone, it is necessary to use a different means to inform the individual in more detail. It would be more practical if the information could be given via a short-pre-recorded message which would refer to the fully detailed information on a website. Another solution could be, upon request of the data subject, to provide the detailed information via a letter sent during the following days of the call. Importantly, in this scenario, reinsurers face the additional difficulty of not having direct contact with the insured person, making it very difficult to deliver the information. Therefore, clearer provisions in the GDPR allowing the use of different means of communication in such scenarios, for example, via a reference to websites after a call would be helpful.

b. Is there an increase of requests (where possible provide estimates);

i. to access data?

The reply differs not only among member states, but also among different insurance companies within the same member state. Most markets mentioned that there was no or just a slight increase in the number of access to data requests. Two markets reported that there was an increase in the number of requests around the GDPR application date and afterwards, the number of requests decreased. In limited cases, a high increase of access to data requests was observed. For example, one insurance company in FR noted that the requests received after the GDPR application date tripled in comparison with those received in 2017; some insurance undertakings in IT noticed a 80% increase and some insurance undertakings in HU reported a 150% increase.

ii. rectification?

Most markets mentioned that the number of requests for rectification did not increase. Only one insurance undertaking reported that the requests for rectification received after the GDPR application date were twice as many as the requests received in 2017.

iii. erasure?

Most markets noticed an increase regarding requests for erasure, but few insurance undertakings saw a steep increase regarding such requests. For instance, an insurer in FR received five times as many requests as the requests received before the GDPR application date, mostly submitted by prospects who requested a quote without subsequently concluding an insurance contract, as well as job applicants who were not subsequently recruited.

v. requests for meaningful explanation and human intervention in automated decision making?

Most markets reported that they did not receive any requests for meaningful explanation and human intervention in automated decision-making.

c. Are there requests on data portability?

Most markets reported that they did not receive any requests on data portability. Few insurance companies reported that they received data portability requests with regard to claims history statements in motor insurance.

d. On which rights do these requests mostly relate to?

Most requests relate to the right to access to data and the right to erasure.

e. Are there any difficulties in the application of the rights (by controllers, by DPAs), including for meeting the deadlines for responding to the requests?

Most markets reported that meeting the deadline for responding to the data subjects' requests is challenging for the following reasons:

i) the number of requests received has increased,

ii) sometimes the complexity of the request makes it challenging to meet the deadline,

iii) the consolidation of all data that needs to be provided in case of right to access requests can be time-consuming,

iv) some insurance undertakings do not have in place automated systems to handle these requests and they need to implement them manually,

v) consequently, more human resources need to be allocated for responding to such requests.

In many cases, insurance companies need to prolong the 1-month deadline for responding to data subjects' requests.

Some insurance companies also noticed difficulties in applying data subjects' rights due to decentralised management mode.

f. What percentage of the requests was manifestly unfounded or excessive? Please describe why these requests were unfounded or excessive.

Most insurance companies reported that they did not receive a lot of unfounded or excessive requests. Most unfounded requests concerned the exercise of the right to erasure. For instance, one insurer mentioned that the right to erasure is often exercised for contracts that have just been concluded. Other insurance companies reported that some requests were rejected as unfounded since the individuals that exercised the rights failed to provide information for their identification.

3. Impact of Article 7(4) regarding the conditions for valid consent on your business model/consumers:

a. Are there any issues with the use of consent as legal basis for specific processing operations? (e.g. complaints received)?

One of the main processing operations when insurers need to process sensitive - health - data is for underwriting purposes, as well as for the evaluation and payment of claims. Processing of such data is necessary for the provision as well as fulfilment of several types of insurance policies such as health, life, disability insurance (for more detailed information on the role of health data processing in the insurance context, please read our position paper).

However, different legal bases are being used across member states for processing health data in an insurance context. This situation creates difficulties for insurers that conduct their business in multiple member states to comply with data protection rules.

The following legal bases have been identified for processing health data in an insurance context across member states:

- Consent as a legal basis: In some member states there is no alternative legal bases for processing health data and therefore insurers must rely on consent for processing health data, both at the pre-contractual stage and for the performance of the contract.
- National legislation as a legal basis: Some member states provide insurers with the possibility to process health data without consent both at the pre-contractual stage or for the performance of the contract, by means of an explicit national regulation (Article.9(4)).
- Substantial public interest exemption as a legal basis: In some member states, processing health data in an insurance context is deemed to fall under the substantial public interest exemption (Article. 9(2)(g)).
- Legal claims as a legal basis: In some member states, Article. 9(2)(f) ("establishment, exercise or defence of legal claims") has been deemed the appropriate legal basis at the pre-contractual stage, as well as for the performance of the contract (eg, for handling claims).
- Consent in combination with legal claims as legal bases: In some member states, processing of health data for the performance of the insurance contract is allowed based on Article. 9(2)(f) ("establishment, exercise or defence of legal claims"). In these cases, insurers must rely on the consent of data subjects for processing health data at the pre-contractual stage.
- Social protection as legal basis: In some member states, processing health data in the insurance context is allowed based on Article. 9(2)(b) according to their DPA (ie, for health insurance).

In addition, the following issues have been reported concerning obtaining valid consent under art. 7(4) of the GDPR in an insurance context:

- Insurance undertakings face difficulties in obtaining consent from data subjects that are not directly part of a contract with the insurance company. For instance, it is difficult to obtain consent from a data subject that benefits from an insurance policy in the context of group insurance, as there is no direct contractual

relationship with the insurance company. Similarly, it is difficult to obtain consent from the injured party that is not part of the contract with the insurance company in the context of third-party liability insurance.

- In some member states, there are national provisions that allow transfers and processing of data in a reinsurance context from the insurer to the reinsurer, without obtaining the consent of the insured person. In others, the processing in the reinsurance context is based on the same legal basis as for the insurer. This difference in the conditions for processing data across member states might impose significant restrictions in the reinsurance context as reinsurers conduct their business in more than one member state.
- In some member states, insurers reported that they need to process health data for fraud prevention/detection purposes. Consent is not an appropriate legal basis for processing health data for these purposes. It is not reasonable to ask a person suspected for fraud to provide their consent before proceeding with the processing of their data in the fraud context.

b. When requesting consent, how did individuals respond?

In most cases, individuals respond positively to the requests for consent. However, a few insurance companies reported that some data subjects were unaware of the regulatory requirements for obtaining explicit consent for processing health data and this resulted in data subjects' frustration and late response to such request, which, ultimately, delayed the management of the customer's file.

c. Have you switched the legal ground for processing from consent to another legal ground?

Insurers did not report switching consent to another legal ground. In general, insurers reported that they mostly rely on the legal basis of the performance of the contract, compliance with a legal obligation and legitimate interest for processing personal data of consumers. Consent is used only for processing health data as well as for direct marketing purposes.

d. How are businesses addressing the issue of tied consent? How are they distinguishing between contract as legal basis and consent?

If no direct marketing and/or processing of health data is involved, insurers mainly rely on the contract as legal basis for processing data of consumers. One insurance undertaking mentioned that it is difficult to explain to the data subject why consent is needed for health data that is necessary for entering into/for the performance of the contract (eg, in case of health and/or life insurance).

In member states where national provisions are in place for processing health data in the insurance context, insurers rely on consent only for processing data for direct marketing purposes.

4. ***Complaints and legal actions:***

   a. ***Are there any or is there an increase of complaints to the DPA against your organisation(s)?***

   The majority of insurance companies mentioned that there was no increase in the number of complaints submitted to the DPA against them. Four markets noticed a slight increase in the number of complaints submitted to the DPA.

   b. ***Are there any or is there an increase of court actions against your organisation(s)?***

   None of the markets reported an increase of court actions against them.

   c. ***If so, for which types of infringements of GDPR?***

   The majority of respondents did not indicate the reasons for complaints reported to the DPA. One market pointed out that complaints concern the request by the data controller to identify the data subject before responding to the request.

   d. ***Are there any court actions against decisions, or absence of decisions, of DPAs?***

   - CY, DE and ES reported that they are not aware of any such court decisions.
   - FR reported that since the entry into application of the GDPR, the CNIL (the FR DPA) has not issued any decisions concerning insurers. Moreover, the FR insurers market is not aware of any court actions concerning CNIL's decisions.

   e. ***In all the above cases, please explain what is the matter of the complaint or court action is and for which types of infringements of GDPR?***

   - FR reported that the majority of court decisions concern the security of personal data and/or the insufficient provision of information to the data subject.
   - CY reported a complaint concerning the exposure of personal data on a mailing envelope which contained information relating to the insurance policy of the data subject. The design of the envelope was such that there was a transparent box at the front which revealed the address of the data subject as well as additional personal data which should not have been displayed.
   - DE reported that complaints mainly concerned out-of-court proceedings where the transfer of personal data to service providers or other third-parties had been allegedly transferred without consent.

5. ***Use of representative actions under Article 80 GDPR:***

   a. ***Are you aware of representative actions being filed against your organisation(s) or in your Member State?***

   The respondents are not aware of any representative actions being files against them.

   b. ***What types of representative actions (complaint to DPA or to court, claim for compensation)? In which country/ies?***

   N/A

   c. ***Against whom and for which types of infringements of GDPR?***

   N/A

6. ***Experience with Data Protection Authorities (DPAs) and the one-stop-shop mechanism (OSS):***

a. Are there any difficulties experienced in the dealings with DPAs (by individuals/businesses)?

The responses vary significantly across markets. Four respondents, especially in small markets, pointed out that the DPAs are slow in responding to requests submitted by the industry. One respondent indicated as a reason that their national DPA is understaffed. Three respondents indicated that they do not face any particular difficulties in dealings with their DPAs. One respondent underlined a positive relationship with its DPA made of frequent and constructive exchanges allowing a coherent application of the GDPR on difficult topics.

b. Are there difficulties in obtaining advice or guidance material by the DPAs?

Seven respondents pointed out that they face difficulties in obtaining specific guidance or advice by their DPAs. One respondent mentioned that their experience when dealing with the DPA was very positive, as it provided specific guidance to their issues.

c. Are DPAs following up on each complaint submitted, and in a timely manner?

- CY reported that the DPA is following up on complaints, decisions and where necessary imposing fines. This market is not aware of the timeframe taken by the DPA to examine a complaint. However, and as a general comment, the CY's DPA is consistent and responsive to complaints.
- DE noted that DPA's had reported a significant increase in the number of complaints. Companies do not always receive feedback from their DPA, therefore, it is difficult to assess whether DE DPAs are following up on each complaint and in a timely manner.

d. How many of your business members have declared a main establishment to a DPA and benefit from a Lead Authority? Have they experienced difficulties with the functioning of the OSS?

The majority of respondents indicated that they do not have any evidence on the functioning of the one-stop-shop mechanism. Only one of the respondents mentioned that one of their member-company declared a main establishment to their respective DPA.

f. Are you aware of guidelines issued by national DPAs supplementing or conflicting with EDPB guidelines? (please explain)

- The Spanish DPA (AEPD) has published guidelines supplementing the European Data Protection Board (EDPB) guidelines on the following matters: (i) data breach notifications, (ii) DPIAs and (iii) Transparency.
- The DE DSK, which is a committee composed by the different DPAs of the Federal Government and the Federal States of Germany, publishes guidelines supplementing the EDPB guidelines. Moreover, the DSK has also expressed its views on issues on which no guideline has yet been adopted by the EDPB. Every guideline of the DSK start with a reference such as "this opinion is subject to a future - possibly divergent - interpretation by the EDPB".

7. ***Experience with accountability and the risk-based approach:***

   a. ***What is the feedback from your members on the implementation of accountability? And their experience with the scalability of obligations (eg Data Protection Impact Assessment for high risks etc)?***

Accountability

The feedback consisted of the following comments: The accountability mechanism involves significant documentation effort, and it is a time-consuming process. Despite the risk-based approach, there are difficulties adapting accountability to small-sized companies. Maintaining accountability requires an increase in human resources within the company.

Scalability of obligations (DPIAs, etc.)

The criteria for a Data Protection Impact Assessment (DPIA) are so broad that the rule for insurance companies is to conduct a DPIA especially in the context of health, life and accident insurance. This places an administrative burden on companies which does not necessarily improve the protection of personal data. Moreover, due to different guidelines published at national level (black and white lists), companies that conduct their business in several countries must comply with different set of rules, which proves ineffective and burdensome.

   b. ***What are the benefits/challenges of GDPR in your line of business?***

- One market highlighted as a major challenge data retention policy to be compliant with GDPR. This is because of the difficulty to implement the technical processes and the high costs involved in this process (eg. human resources, hiring of additional technical services etc.). Specifically, it has been proven to be a challenge in terms of data retention:
  - To correctly identify the end of the retention period, considering particular situations which in an insurance context may require longer retention periods.
  - The difficulty to implement data erasure techniques. Normally, databases are centralised, there is no single database for each application, this means that applications have correlated databases and when erasing records, problems may arise from non-matching data bases.
  - The amount of data to be erased. In particular, problems regarding processing capacity and the duration of the process, since the erasure process must necessarily run when the applications are not working.
  - Automatic data matching among different subjects. For example, between undertakings, intermediaries, service firms or other outsourcers, and
  - The need to have historic data for actuarial calculations, this forces a process for data transformation and data saving before it is erased.
- Another market reported that the notion of "freely given" consent and the right to withdraw consent can be challenging in an insurance context when providing the service to the policy holder. Moreover, issues are arising in relation to the classification of suppliers, whether they are considered controllers or processors (for details please see our replies to question 9 in relation to the adaptation of SCCs). These problems arise often in connection to reinsurance companies, external advisors and insurance intermediaries. In general, these entities tend to consider themselves by default controllers.

   c. ***What do you think the overall impact of GDPR will be on your organisation's approach to innovation?***

The following issues have been reported by different markets regarding innovation:

- Innovation is slowed down because the GDPR requirements (eg, privacy by design) need to be integrated in the process.
- Legal uncertainty on the scope of Article 22 of the GDPR (solely automated decision-making, including profiling) stifles innovation in insurance. This is because the GDPR establishes a general prohibition on the use of solely automated decision-making processes, including profiling, that have legal or similar effects on individuals (Article 22(1)). The GDPR provides a number of exceptions to this rule, including the "necessity to perform or enter into a contract" (Article 22(2)(a)). However, the EDPB adopted a narrow interpretation of this exception in its guidelines on automated decision-making and profiling, requiring that "the controller must be able to show that this type of processing is necessary, […]. If other effective and less intrusive means to achieve the same goal exist, then it would not be necessary". Additionally, the high threshold for obtaining valid consent under art. 22(2)(c) and (4) may hinder the design of innovative insurance products. Legal certainty is all the more important as the ePrivacy regulation – currently under discussion within the Council of the EU – will likely impose different rules on several topics than the ones provided by the GDPR.
- The implementation of data minimization and the purpose limitation principle when designing new products may have a negative impact on innovation since the data collected, as well as the purposes for which data will be used, are restricted.
- The implementation of requirements, such as the privacy by design principle, increased the cost of designing innovative products.

One insurer reported that the integration of the GDPR in the innovation process can provide a competitive advantage, as it is an important element of consumer trust.

d. In which area did your organisation have to invest most in order to comply with the GDPR? How useful do you consider this investment for the overall performance of your organisation?

The following areas where organisations must invest most have been reported:

- Software developments and IT solutions in order to implement increased GDPR requirements
- Developing solutions for implementing data retention policies (eg, automated archiving, digital deletion)
- Human resources and training/awareness of staff
- Data management to maintain data quality
- Design of a data breach notification process

e. To which extent could your organisation rely on existing technical and organisational measures or did you establish a new data management system?

Insurance companies mentioned that they mostly relied and adapted accordingly existing technical and organisational measures. Actions taken to adapt existing systems include the designation of a data protection officer (DPO), updating the privacy policies, implementing policies such as incident management policies. Only a limited number of insurance undertakings needed to establish new data management systems.

f. Do your members experience an increase of awareness and of trust of their customers due to the implementation of technical and organisational measures to comply with the GDPR?

The feedback received on this question is limited. Overall it is observed that there is an increase of awareness of data protection rules, but there is no evidence that this increased awareness result in an increase of trust of customers vis-à-vis the industry.

8. Designation of data protection officers (DPO)

a. Did your organisation designate a mandatory DPO pursuant to Article 37(1) GDPR?

All markets participating in this survey confirmed the designation of a DPO, some insurers even referred to the designation of DPO's prior to the GDPR. Larger undertakings highlighted that they had designated a DPO for each market branch. One market reported that, although most insurers had appointed a DPO, some smaller companies operating in niche markets, for example, liability insurance for boats or insurance for horse ownership, do not meet the conditions under Article 37 of the GDPR to designate a DPO.

b. Did your organisation designate a mandatory DPO pursuant to national law implementing Article 37 (4) GDPR?

A few markets reported that they had designated a DPO according to national law, while one market reported that some insurers had designated DPOs according to national law and others had not designated DPOs, or at least not yet. Other markets indicated that this designation was not applicable to their markets.

c. Did your organisation designate a DPO on your own initiative, without being required to do so by the GDPR or by national law?

A number of markets replied that they already had in place a similar figure to the DPO prior to the entry into force of the GDPR. Some of these markets have adapted their DPOs to comply with the new mandatory DPO figure as prescribed in the GDPR. A small number of undertakings indicated that the designation of the DPO was in response to the new regulatory requirements.

d. Did associations or other bodies representing categories of controllers or processors designate data protection officers?

The input received on this question is limited. Four insurance associations confirmed the appointment of a DPO at their organisation.

e. What is your experience with the performance of DPOs?

Overall, the majority of respondents have a positive view and experience regarding the role and performance of the DPO. Moreover, a number of markets see DPOs as a positive structure within insurance undertakings as the DPO (i) contributes towards fostering and building the companies' responsible approach and culture towards the protection of data amongst the different departments which have to handle data, (ii) the DPO becomes the internal point of reference for any requests concerning data, (iii) is involved from a data protection perspective in the design of new insurance products, and (iv) facilitates the process for data subjects to exercise their rights.

ES indicated that it has been feasible to quickly implement the role of DPOs within insurance companies given that the previous Spanish legislation already provided for a similar structure.

A few markets, while sharing their view on the positive value brought by DPOs, noted that their role should be further clarified to prevent the attribution of tasks which could go beyond the intended scope of the DPOs duties.

9. Controller/processor relationship (Standard Contractual Clauses)

a. What is the experience of your members on the adaptation of current contacts?

The majority of markets indicated difficulties on the adaptation of contracts with processors; it has turned out to be a very slow and lengthy process. This is mainly because the contracting parties have had to cope with capacity and organisational issues to be able to carry out the exhaustive technical examinations required for adaptation of insurance contracts. Insurers have had to undertake a lengthy process to review and amend insurance contracts with customer and contracts with suppliers. The following examples reflect some of the main technical difficulties encountered by insurers when adapting contracts to the new GDPR clauses:

- The DE market reported that the opinion of their DPA regarding the requirements for a legal basis under Article 6 or 9 of the GDPR to transfer data from a joint controller to another controller creates difficulties: The German DSK, a committee composed by the independent DPAs of the Federal Government and the federal states of Germany, published an information note about joint controllers (Kurzpapier Nr. 16). The paper says that joint controllers are also recipients within the meaning of Article. 4 (9) of the GDPR and can therefore be subject to information obligations. The transfer of personal data among joint controllers is a processing operation in the sense of Article. 4 No. 2 DS-GVO and as such requires a legal basis.
- Seven markets reported difficulties in establishing whether a joint controller or a controller/processor relation exists. In other words, a repeated issue is the difficulty to understand whether a party qualifies as processor or separate or joint controller. Overall, the main difficulty remains to establish and define the responsibilities and status of each party, in particular concerning the role of the subcontractor (processor) given the broad interpretation provided in the GDPR and the concerns around liability. As a result of this, establishing whether a party within the supply chain is a controller, processor or joint controller remains a challenge, with some firms noting lengthy and protracted negotiations between parts of the supply chain.
- FR insurance companies reported that the effectiveness in the adaptation of contracts depends very much on the level of understanding of the GDPR by the contracting parties. An uneven understanding of the law generally delays the process to amend contracts, and this is often the case when the contracting parties or one of the parties has few resources to be able to respond to the efforts that GDPR implementation requires.
- CY insurance companies are facing many difficulties when classifying suppliers as processors or joint-controllers vis-à-vis their commercial relationship. This is often the case where reinsurance companies, external advisors (eg, legal firms, accounting firms and consulting firms) and insurance intermediaries are involved. These entities tend to categorise themselves by default as controllers and strongly contest any other classification.

ES, NO and PL indicated no major difficulties in the adaptation of contracts. In the case of ES, this is due to the previous legislation which already established a similar relationship between controller/processor, there have been no major changes for suppliers. NO reported a fairly smooth contract adaptation process given that most suppliers were prepared for GDPR. PL has not observed any significant difficulties.

b. Is there a need for the adoption of standard contractual clauses under Article 28 (7) GDPR? Explain what the main reasons are.

There is no clear consensus among the respondents on whether the EC should adopt standard contractual clauses (SCCs) for contracts with processors:

- Four markets and four insurance companies of a fifth market explained that the adoption of SCCs could be useful to (i) standardize the contractual framework for subcontracting while saving time and resources in negotiations with processors, (ii) establish a balance of power where larger organisations with more resources

can request amendments to agreements which could not always be for the benefit of both parties. In this regard, SCCs would be particularly useful for SMEs and intermediaries. Moreover, (iii) SCCs could facilitate contractual negotiations with US service providers, (iv) and could bring clarity concerning questions on liability by establishing that both the controller and the processor are responsible for damages and sanctions.

- Another market reported that SCCs are not needed for larger organisations given the existing expertise; however, SCCs could be helpful for smaller undertakings.
- Another respondent highlighted that if SCCs are adopted under Article 28 (7) of the GDPR, then it must be ensured that these SCCs can be adapted to the different levels of risk processing. It would be concerning if cases with little data processing and of low risk were to meet the same requirements of larger data processing activities with higher risks. This situation could result in an unreasonable administrative and costly burden on insurers.
- Another market and four insurance companies belonging to the same market said they were against the adoption of SCCs. Respondents explained that each contract has its own particularities and therefore SCCs would add further difficulties. In the case of the insurers, it was reported that their DPA has already proposed their own SCCs, which constitute a sufficient reference framework. Other undertakings highlighted that the adoption of SCCs may arrive at a too late stage since companies have already adopted their own into their contracts and therefore, EC SCCs would force insurers to restart the process of contract adaptation.

c. If standard contractual clauses were to be prepared, what elements and specifications should be included? (e.g. auditing, liability allocation, duty of cooperation, indemnification)?

Two markets reported that SSCs *should not* contain elements that are not listed in points 3 and 4 of Article 28. However, a market noted that adding an obligation for the processor to cooperate in case of requests for erasure would be useful to fulfil the requirements of Article 19 of the GDPR. Moreover, the same respondent reported that it would be helpful if the law could clarify that the service supplier has to be subjected to the controls/audits demanded by any supervisory authorities.

d. Do you have suggestions in terms of how to ensure the "user-friendliness" of such standard contractual clauses?

If SCCs are adopted, there should be different clauses depending on the risk and the size of the data processing activities. Minor processing activities with low risk should not have to meet the same requirements than a high-risk processing.

10. Adaptation/further development of Standard Contractual Clauses (SCCs) for international transfers

a. What are your practical experiences with the existing SCCs: Do they serve the purpose? If not, where do you see room for improvements? Have you encounter any problems in using the existing SCCs?

- A national association reported that insurance companies in their market had been frequently confronted with requests to change contractual clauses. The changes were requested in regard to the existing audit regulation in the SCCs, which causes difficulties because some contractual parties request changes due to a deviating regulation. So far, changes requesting audit arrangements have not been accepted. SCCs should therefore include alternatives to choose from.
- A market said that while their insurance market has, so far, not experienced any difficulties with the use of the existing SCCs, they do see room for their adaptation to the new requirements within the GDPR. For example, SCCs should be improved to consider aspects related to the management, functions and identification of the DPO, the management of rights of the data subject or the possibility to collaborate between the contracting parties to demonstrate compliance.
- Another market reported that insurers use SCCs when needed and that these clauses are commonly known among suppliers, therefore there is little discussion about whether the necessity to have them or use them.
- Another market reported that their experience with the use of SCCs is positive and that insurers' distributors appreciate their use. In general, the use of SCCs in this market is preferred to other means such as the Privacy Shield.

b. Do you see a need to adapt the existing SCCs, generally and/or in the light of the GDPR? (eg different structure/design? additional safeguards? combination with Art. 28 standard clauses for processors?)

- A national association reported that the majority of insurers in its market would be in favour of having an Article 28 combination of SCCs. However, another undertaking reported that more time is required to experience the effects of the contractual amendments already made in order to review or adapt SCCs.
- Another respondent reported that the insurers in its market would be in favour of introducing additional safeguards concerning mandatory data and data security concepts. Moreover, this market pointed out that were processing is carried out on behalf of the controller, an additional contract is needed to fulfil the requirements in Article 28. Therefore, it would be helpful if a combination with Article 28 is provided. In this regard, another market reported that its insurance undertakings would also be in favour of adopting SCCs where these helps to adapt to the new GDPR requirements. In a similar line a third market reported that SCCs would be helpful in the relationship between processor-processor.
- Another market reported that they are not ready yet to provide an assessment in this regard, and another respondent expressed that new measures would be unnecessary.

c. Do specific clauses require further clarification (e.g. auditing, liability allocation, duty of cooperation, indemnification)?

One market reported that SCCs should include alternatives in the audit regulation to choose from. The current regulation caused difficulties because some contractual parties requested changes due to a deviating regulation. Consequently, companies were frequently confronted with change requests concerning the contractual clauses.

In these cases, it would be helpful to have alternatives to the current regulation, for example certificates which are recognised in the EU.

d. *Is there a need to adapt the SCCs in light of the Schrems II court case (concerning access by third country authorities), e.g. with respect to monitoring/reporting obligations on the data importer/exporter?*

- A market said that SCCs should not be adapted in light of this particular case, since there are already other mechanisms or legal considerations at national level and within EU law that could cover vacuums caused by the outcome of the ruling. Two other markets reported that they did not see the need for further adaptation of SCCs with regard to the Schrems case.
- In the second annual review of the EU-US Privacy Shield, the EDPB expressed concerns regarding the lack of concrete assurances as to the indiscriminate collection and access of personal data by US Government Agencies for national security purposes. This remains a concern for the EDPB and should be addressed when developing SCCs, therefore, the EDBPS's concerns shall be taken into consideration to ensure that SCCs will be a valid instrument for data transfers between the EU to the US.

Do you have suggestions on ways and means to strengthen the possible control by the data exporter vis-à-vis the data importer and the measures to enforce such control (e.g. not only suspending the transfer of data but actually recalling the data already transferred?)

One market reported that "collective controls" could help in supporting the acceptance of controls between the parties. Also, the involvement of DPAs in the home country of the importer could be helpful, provided that there is cooperation mechanism between the DPAs in the country of the exporter and the country of the importer. For example, the use of recognized certificates for the processing of data by the European DPAs, would allow for easier controls.

e. Is there a need to develop new SCCs, e.g. for the processor/sub-processor relationship, joint-controllership, processor-to-controller relationship or specific processing operations?

- A market reported that SCCs have not adapted to the situation where the data exporter is the processor. This lack of adaptation can be problematic, for example, when an international insurance group has its head office (HO) within an EU country and subsidiaries worldwide.

  A HO normally works for the subsidiaries providing them with different services. In these cases, while working under the instructions of its subsidiaries, the HO is a processor and the subsidiaries are the controllers. In such scenario, the EDPB guidelines on the territorial scope of the GDPR, indicate that the GDPR does not apply to the subsidiaries, but to the HO which are the processors. Moreover, the guidelines provide that the transfer of the "return" data from the processor (HO in an EU country) to the controller (subsidiary in third country) has to be legally framed by SCCs or other exceptions of Article 46-GDPR, which would not apply in this particular case.

  In the above situation, insurers with HOs in the EU are facing the problem of not being able to use SCCs to transfer the "return" data to its subsidiaries (data controllers). This is because SCCs are only applicable when the data exporter is a controller. Furthermore, validation of 'self-made' contractual clauses by DPAs according to Article 46 (3) of the GDPR is not conceivable in practice because of the complexity and the duration of the process; each entity must have its own validated clause.

  Therefore, the transfer of data where the transferring entity is the processor and the receiving entity is the controller should be possible through the use of SCCs. It would be beneficial to develop SCCs to allow international transfers where the processor based in the EU is the data exporter and the controller is based in a non-EU country.
- Another market reported that the establishment of SCCs for the processor/sub-processor relationship is necessary. In case a processor within the EU plans to engage another sub-processor in a third country, the controller itself has to close the contract with the controller in the third country. Currently a contract between

processor and sub-processor is not sufficient. Moreover, a clarification of the necessary content of contractual clauses for joint controllership would be beneficial too.

f. Do you have suggestions in terms of how to enhance the "user-friendliness" of SCCs?

A market replied that user instructions could be helpful, for example, to clarify the fact that the SCCs cannot be changed.

11. 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, etc.)?

- ES highlighted the national legislation implementing the GDPR had been published on December 2018. The national implementing law recognizes and respects the national insurance legislation that regulates data processing in the insurance sector for special categories of personal data. ES has a positive experience on the national implementation process of the GDPR.
- DE highlighted the DSK guideline on the processing of personal data for advertising purposes. The guideline defines additional requirements, on top of the requirements proposed by the EDPB Guidelines, to balance the different interests involved in advertising.

Insurance Europe is the European insurance and reinsurance federation. Through its 34 member bodies — the national insurance associations — Insurance Europe represents all types of insurance and reinsurance undertakings, eg pan-European companies, monoliners, mutuals and SMEs. Insurance Europe, which is based in Brussels, represents undertakings that account for around 95% of total European premium income. Insurance makes a major contribution to Europe's economic growth and development. European insurers generate premium income of €1 200bn, directly employ over 950 000 people and invest nearly €10 200bn in the economy.