Position Paper

Insurance Europe views on EC report on the review of the GDPR

Our reference:	COB-DAT-20-030	Date:	28 April 2020
Referring to:	European Commission consultation on EC report on the review of the GDPR		
Contact person:	Ana-María López-Chicheri Llorente, Policy Advisor, Conduct of Business	E-mail:	llorente@insuranceeurope.eu
Pages:	19	Transparency Register ID no.:	33213703459-54

Introduction

Insurance Europe welcomes the various opportunities offered by the European Commission (EC) to provide input to its report on the evaluation and review of the General Data Protection Regulation (GDPR). Insurance Europe has already responded to the EC stakeholder questionnaires[1] and is now pleased to comment on the EC roadmap consultation on the report of the GDPR. Insurance Europe invites the EC to consider the following aspects:

- **Comments on the form and content of the GDPR review report:**

  - **The EC report should not open the text of the GDPR for amendments in 2020**: Although it contains challenges for business, revising the GDPR after only two years since the Regulation became applicable to introduce amendments would be premature and counterproductive. Like many other sectors, the insurance industry has invested significant resources to understand the Regulation and its implications for our sector and to ensure a proper implementation of the new regime. Opening the GDPR for review at such an early stage would undermine the industry's efforts and investments to comply with the Regulation.

    Instead, Insurance Europe recommends that the EC report focuses on taking stock of the experiences gained since the application of the Regulation in May 2018, and if areas where the GDPR has failed to meet its objectives are identified, considers the development of further or different guidance, together with the European Data Protection Board (EDPB), where relevant.

  - **The EC report should take stock beyond the mandate established in Article 97 GDPR**: Article 97 GDPR mandates the EC to issue a report identifying any issues on the application of the GDPR and instructs the EC to focus the assessment on the international transfer of personal data to third countries and on the adequacy and consistency mechanism (Chapters V and VII respectively). Insurance Europe recommends that the EC takes stock beyond Chapters V and VII of the Regulation and includes the following aspects into the report:

    - The EC, as the guardian of European Law, should include a dedicated section in the report on the role of the EDPB and the impact of its GDPR guidelines on industries. In particular, this section should address the areas where the interpretation of the EDPB, has gone

[1] Insurance Europe is a member of the EC multi-stakeholder group on GDPR and submitted input to the stock-taking questionnaires on the functioning of the GDPR in April 2019 and February 2020.

beyond the political agreement in the text of the GDPR by, for example, creating additional requirements or narrowing the interpretation of a GDPR provision[2].

The EC should use the report on the application of the GDPR to reinforce its role as the guardian of the Regulation and to stress that the EDPB's mandate is subjected to the political agreement in the text of the GDPR.

- In the interest of European consistency in the application of the GDPR, the EC report should consider assessing whether certain national GDPR guidelines have created fragmentation in the application of the Regulation. For example, the guidance on cookies and tracers issued by the Spanish data protection authority (DPA) does not follow the same criteria that is used by the French and UK DPAs regarding the mechanisms to obtain consent from the data subject. These discrepancies at national level have also arisen in guidelines concerning data protection impact assessments or legitimate interest, where DPAs have established differing criteria. It is paramount that the EC pursues a unified approach to the interpretation and application of the GDPR throughout Europe.
- Furthermore, as explained further below, the EC report should assess:
  - The impact of the GDPR on innovation and address any obstacles the regulation may have unintentionally created to the development of innovative and emerging technologies such as blockchain, artificial intelligence, big data or the internet of things. These technologies offer great opportunities for insurers and consumers, but innovation developments could be undermined in the sector if innovation attempts challenge GDPR provisions and/or EDPB guidelines.
  - The interplay between the GDPR and the ePrivacy proposal and propose to align the legal bases provided in both Regulations to process data.
  - The tools for international data transfer, and suggest ways to address any existing insufficiencies to ensure that European companies can rely on the tools provided in the GDPR.
  - Whether DPAs are provided with sufficient resources according to their needs to ensure a European level playing field in the enforcement of the GDPR.

- **Comments on unintended barriers on the development of technology in insurance**:
  - **Blockchain technology and GDPR**: The underlying principles of blockchain technology raise certain questions about compatibility with the GDPR. For example, how to reconcile the GDPR's rights to erasure and to rectification with the fact that blockchain technology is designed to be an immutable and permanent record of all transactions is unclear. This lack of clarity may hinder the development of solutions based on blockchain technology by insurers. The EC should take note that the principle of "technological neutrality" should be preserved in any legislation and guidance.
    Insurance Europe recommends that the EC works closely with the EDPB, to address any necessary clarifications on the interplay between the GDPR and blockchain, and provide the necessary legal certainty to develop solutions based on blockchain technology.
  - **Article 29 Working Party Guideline on automated individual decision-making and profiling**: 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 GDPR). However, the GDPR provides a number of exemptions to this rule, including the "*necessity to perform or enter into a contract*" (Article 22.2 (a) GDPR). Therefore, solely automated decisions, as described, are allowed when they are *necessary* to perform or enter into a contract. This could be the case, as explained by the Guidelines, where the amount of data being processed cannot be treated by humans in a timely manner.

    The barriers for insurers to use solely automated processes comes from the interpretation that the Guidelines give to the threshold that needs to be fulfilled to prove the "*necessity*" of the solely

[2] See the annex to this document: Insurance Europe's table on its key contributions to the EDPB's draft guideline consultations.

automated process to perform/enter into the contract. In this regard, the Guidelines state on page 23 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*".

This narrow interpretation imposes an extremely high burden on insurers, who are forced to prove case by case the "*necessity*" of carrying out the solely automated processes. This situation may create difficulties to offer innovative products based on solely automated techniques, depriving insurers of business opportunities and prejudicing consumers.

For example, an insurance company may offer online motor insurance through a mobile phone app, where the consumer can obtain coverage simply by sending a picture of the car and providing the requested data via an app. The premium is automatically calculated, and the contract is entered into when the payment is effective. In this case, the narrow interpretation of "*necessity*" could prevent insurers from offering a "real time" service because it might not be possible to prove in a timely manner, that the calculation of the premium based on solely automated processing is necessary for the performance of the contract. This situation could be extended to the use of solely automated techniques in claims handling processes or in the offer of online travel insurance.

The Guidelines narrow interpretation of the "*necessity*" threshold in Article 22.1 (a) GDPR may jeopardise the introduction of technological developments in the area of profiling and automated decision-making throughout the insurance value chain. Insurance Europe recommends that the EC addresses this concern and takes action to ensure that insurers can provide innovative products with legal certainty. For this purpose, the narrow interpretation of the "*necessity*" threshold should be deleted from the Guidelines.

- **Absence of an adequate legal basis in the ePrivacy proposal to offer telematics insurance products**: The unclear scope and inflexible approach of the ePrivacy proposal towards innovation would put certain insurance products at risk. This is because, insurers do not know with certainty if insurance telematic products fall under the scope of Article 8 of the proposal. If they did, the insurance industry could not rely with certainty on the legal bases provided under Article 8 to offer, for example, pay as you drive insurance (PAYD).

  Article 8 of the ePrivacy proposal regulates the use of the processing and storage capabilities of terminal equipment, the collection of information from end-user's terminal equipment and the collection of information emitted by the terminal equipment of the end-user to enable it to connect to another device.

  Insurance Europe has worked under the hypothesis that insurance products based on telematics fall under the scope of Article 8. This is because, the dongle installed in a car for the purpose of providing PAYD insurance could be considered terminal equipment under the ePrivacy proposal. The scope of the proposal has been broadened in such manner that almost any device that processes non personal data would immediately be ruled under the new ePrivacy rules. However, it must be noted, that insurance products are not captured by the scope of the ePrivacy Directive.

  Article 8 establishes as a general rule the prohibition of data processing activities unless they fall within one of the exemptions provided in the provision. Therefore, if it is assumed that insurance telematic products are terminal equipment, insurers need to rely on an exemption of Article 8 to be able to offer any product that processes data from an application or dongle that can be defined as terminal equipment.

  The legal bases provided in Article 8 and that could potentially be used by insurers are consent (Article 8.1(b)) and the processing is necessary to provide an information society service requested by the end-user (Article 8.1b(c)). However, insurers cannot rely on either of these solutions:

  - The use of the exemption "*the user has given their consent*": According to the EDPB guidelines on consent, this can only be an appropriate lawful basis if a data subject is offered control and is offered a genuine choice with regard to accepting or declining the terms offered or declining them without detriment. Therefore, if insurers rely on the consent

exemption there is a risk that consent is rendered invalid by the DPA or a court. Moreover, the consumer could withdraw the consent and consequently the insurer would not be able to continue to provide insurance telematics coverage despite the continued existence of a valid telematics insurance contract.

- The use of the exemption *"it is necessary for providing an information society service requested by the end-user".* In light of Directive 98/48/EC and of the European Court of Justice ruling in the Uber case, it is unclear whether insurance telematic products can be categorized as "*information society services*". The Court decided in the Uber case, that the digital platform was not an information society service since Uber's main activity was to provide a transport service. Therefore, insurers cannot rely on this exemption to process data from the terminal equipment.

As a result, the insurance industry lacks a legal basis to process data from the terminal equipment to offer insurance products based on telematics. Therefore, Insurance Europe recommends that the EC supports the deletion proposed and maintained by the last three Council Presidencies, to delete the wording "information society" from Article 8.1b(c) of the proposal and simply keep "*the processing is necessary to provide a service requested by the end-user*". This would provide insurers with a legal basis to offer insurance telematic products.

In addition, Insurance Europe calls upon the EC to support aligning the legal bases to process personal data in the GDPR (Article 6 GDPR) and the legal bases provided in the ePrivacy proposal. In this regard, it is vital for the insurance industry that Article 6.1 (b) of the GDPR – *Processing is necessary for the performance of a contract* – is included in the ePrivacy proposal. The performance of a contract is the most adequate legal basis that insurers can use to process data from the terminal equipment and therefore offer insurance telematics products with legal certainty.

- **Comments on the tools available in the GDPR for international data transfers (Chapter V GDPR):** The GDPR provides different tools and solutions for the international transfer of data. These are EC adequacy decisions, standard contractual clauses (SCCs), binding corporate rules (BCRs), codes of conduct for international data transfers and certification mechanisms. Some of these tools have been inherited from the previous data protection directive, such as the existing SCCs and the majority of the adequacy decisions. However, in practice these tools are not sufficient to cover international data transfers in the insurance sector:

  - Adequacy decisions are the most well-fitting instrument for insurers to transfer data internationally as they provide the most appropriate safeguards for both data controllers and data subjects. So far, the EC has recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the United States of America (limited to the Privacy Shield framework) as providing adequate protection. The only decision signed after the entry into force of the GDPR in May 2018 was the EU-Japan decision.

    The above-mentioned list of countries is not sufficient and falls short to cover data transfers in an environment where the global exchange of data is on the rise daily. The EC should take note of this gap and speed up the processes for adopting adequacy decisions for third countries and territories with adequate level of protection.

  - BCRs only cover intragroup data transfers and therefore insurers cannot make use of them for international data transfers in a broader context.

  - Codes of conduct for international data transfers and certification mechanisms:

    - Articles 46 (2) (e) and 40 (4) GDPR state that codes of conduct together with binding and enforceable agreements can be used as a tool for international data transfers. However, the EDPB has not adopted the guidelines for international codes of conduct nor published the

draft guidelines for public consultation. The absence of guidance on this subject creates uncertainty and adds difficulties for the development of international codes of conduct.

- A similar situation applies to certification mechanisms (Articles 42 and 46 (20 (f) GDPR). Although the EDPB adopted the guidelines on certification mechanisms, this tool in its version for international transfers has not taken off. In this regard, Insurance Europe invites the EC to explore the possibility in the current stocktaking exercise of developing in partnership with the International Organisation for Standardization (ISO) a certification and audit scheme for companies to adhere to. A partnership of this nature could boost the use of certification mechanisms as a means for international data transfers.

- Use of SCCs in the insurance industry:

  - Overall, the insurance market has a positive experience with the use of the existing SCCs for international data transfers. SCCs are, in the absence of adequacy decisions, the preferred tool for international data transfers. However, Insurance Europe recommends that existing SCCs should be updated to be fully in line with the GDPR. For example, SCCs should be updated to consider aspects related to the management, functions and identification of the data protection officer (DPO), the management of rights of the data subject or the possibility to collaborate between the contracting parties to demonstrate compliance.

  - The existing SCCs for international transfers do not cover the situation where a subcontractor relationship is in place. In other words, at present there is no legal scheme for data transfers when a controller who is seated within the EU uses the services of a processor who is also seated within the EU, but *who in turn employs a subcontractor in a third country*.

In view of the above, Insurance Europe recommends that the EC acknowledges in its report the current insufficiencies regarding tools for international data transfers and takes prompt action to address them to ensure that European companies can rely on the tools provided in the GDPR. Moreover, Insurance Europe calls on the EC to acknowledge the existing gap in the available SCCs for international data transfers and develop SCCs for transfers between processors in accordance with Article 46 (2) (c) GDPR.

- **Comments on the level playing field of GDPR enforcement:** Article 52(4) of the GDPR establishes that each Member State shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the EDPB.

  The GDPR determines a legal obligation upon Member States to provide their DPAs with the resources they require to perform their duties. However, Member States do not always provide their DPAs with an adequate budget that matches the amount of resources needed to face the increasing workload of these authorities. This situation is creating an uneven level playing field in the enforcement of the Regulation. While some Member States have established strong DPAs through robust budgets, enabling the authority to duly perform their tasks and impose fines where necessary, other DPAs are poorly equipped and therefore unavoidably perform a lower level of enforcement.

  Insurance Europe recommends that the EC addresses in the report the uneven level playing field in the enforcement of GDPR and initiate infringement procedures where necessary.

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 pay out almost €1 100bn annually — or €2.9bn a day — in claims, directly employ over 900 000 people and invest nearly €10 200bn in the economy.

List of EDPB Guidelines' requirements going beyond the GDPR provisions and Insurance Europe's recommendations

Annex to Insurance Europe's position paper to inform the preparation of the evaluation & review report of June 2020 on the GDPR application

EDPB Guidelines	Guidelines requirements going beyond the GDPR text	Insurance Europe's views	Insurance Europe's recommendations in view of the GDPR evaluation and review report
Guidelines on Data protection impact assessment (DPIA) and determining whether processing is "likely to result in a high risk" (link): ▪ Last revised & adopted on October 2017 ▪ Insurance Europe's position paper	**Mandatory DPIAs**: The Guidelines expands the scope of DPIAs since it recommends carrying out DPIAs even when it is not clear whether the DPIA is required (p.8). **Sensitive data**: The Guidelines includes location data and financial data as "*sensitive data or data of a highly personal nature e*" (p. 9-10).	**Mandatory DPIAs:** The recommendation goes beyond the GDPR requirements, increasing company's burden and causing legal uncertainty. Companies would be forced to carry out DPIAs, where it is not prescribed by the law, out of fear of not being compliant and risk legal claims. **Sensitive data**: The Guidelines treats financial and location data as *sensitive data.* Insurance Europe had cautioned against expanding the scope of Articles 9 and 10 GDPR.	**Guidelines interpretation of (i) mandatory DPIAs and (ii) sensitive data**: The interpretation goes beyond the letter of the GDPR expanding the scope of DPIAs which increases company's burden and causes legal uncertainty (risk of legal claims). It also expands the categories of sensitive data. The Guidelines should be revised to be aligned with the requirements in the law.
Guidelines on personal data breach notification (link): ▪ Last Revised and adopted on February 2018 ▪ Insurance Europe's position paper	**Communication of a personal data breach**: The Guidelines establish that if in doubt of the existence and level of the risk "*the controller should err on the side of caution and notify*" (p. 26) **Obligation to document breaches**: The Guidelines recommends that, in addition to the obligations set in Article 33.5 GDPR, "*the controller also documents its reasoning for the decisions taken in response to a breach"* (p. 27).	**Communication of a personal data breach**: The literal reading of the guidelines forces data controllers to notify the supervisory authority and the data subject to ensure compliance, which goes beyond the obligations established in Articles 33 and 34 GDPR. **Obligation to document breaches**: The recommendation to reason the decisions taken in response to a breach goes beyond the obligations described in Article 33.5 GDPR. The recommendation "*to reason*" should be removed from the Guidelines.	**Guidelines requirements to (i) communicate personal data breaches and (ii) to document breaches:** The Guidelines establish requirements that go beyond the obligations in the GDPR. Therefore, the Guidelines should be revised to align their wording with the GDPR requirements.

EDPB Guidelines	Guidelines requirements going beyond the GDPR text	Insurance Europe's views	Insurance Europe's recommendations in view of the GDPR evaluation and review report
Guidelines on Automated individual decision-making and Profiling (link): ▪ Last revised and adopted on February 2018 ▪ Insurance Europe's position paper	**The "necessity threshold"**: The Guidelines impose a burdensome and narrow interpretation of the threshold to prove the necessity to use (solely) automated decision-making processes for entering/performing a contract (p. 13-23). This narrow interpretation affects (i) automated decision-making processes under Article 6.1 (b) GDPR and (ii) solely automated decision-making processes under the exception in Article 22.2 (a) GDPR.	**The "necessity threshold":** The Guidelines interpretation suggesting that "*the data controller shall take into account whether a less privacy-intrusive method could be adopted to prove that automated-processing is necessary*" is nowhere written or implied in the GDPR provisions. The GDPR simply states that these processes shall be allowed when necessary to enter/perform a contract. Therefore, the narrow interpretation should be removed from the Guidelines.	**The "necessity threshold":** This interpretation has created legal uncertainty in the insurance industry when using automated processes becoming a barrier to innovation. Insurers could risk facing administrative fines and civil litigation. These risks discourage insurers from introducing new techniques for automated processing and profiling throughout the insurance value chain. The narrow interpretation of "*necessity of a contract*" should be removed from the Guidelines.
	The interpretation of consent in Article 22.2 (C): The Guidelines say that "*data controllers relying on consent as a basis for profiling will need to show that data subjects understand exactly what they are consenting to* (p. 12-13).	**The interpretation of consent in Article 22.2 (C):** The obligation to demonstrate that data subjects understand *exactly* what they are consenting to, is disproportionate and cannot be achieved in practical terms. Specially if we bear in mind the information obligations in Articles 13-15.	**The interpretation of consent in Article 22.2 (C):** The adverb "exactly" should be removed from the guidelines and the section revised in line with the obligations established in Articles 13-15.
	Right to access information on the profile: The Guidelines state that, "*according to Article 15.3, the controller has a duty to make available the data used as input to create the profile as well as access to information on the profile and details of which segments the data subject has been placed into"* (p.17).	**Right to access information on the profile**: The GDPR provides data subjects with the right to obtain information on the input and output data, including information about the existence of automated decision-making processes (Articles 13-15 GDPR). However, the GDPR does not impose any obligation to provide information on the profile itself.	**Right to access information on the profile**: The obligation to provide information on the profile itself is not included in the GDPR. Therefore, it should be removed from the Guidelines.
	Algorithmic third-party auditing: The Guidelines includes in p.32 a good practice recommendation to assist data	**Algorithmic third-party auditing**: Although a best practice example:	**Algorithmic third-party auditing:**Third-party auditing is not included in the GDPR, it should be removed from the Guidelines.

EDPB Guidelines	Guidelines requirements going beyond the GDPR text	Insurance Europe's views	Insurance Europe's recommendations in view of the GDPR evaluation and review report
	controllers to meet the requirements of Article 22 GDPR. The good practice involves third party auditing of algorithms (*independent 'third party' auditing where decision-making based on profiling has a high impact on individuals, provide the auditor with all necessary information about how the algorithm or machine learning system works).*	(1) Proposed best practice examples have an effect for the industry as non-compliance can lead to detrimental effects during data protection audits (Art. 58 (1b)). Additionally, noncompliance with proposed good practices can possibly establish liability in civil claims. (2) Third-party auditing is not included in the GDPR. Therefore, this example should be deleted.	
Guidelines on transparency (link): ▪ Last revised and adopted on April 2018 ▪ Insurance Europe's position paper	**Obligation to provide information on the consequences of the processing**: The Guidelines state that, "*as well as providing the prescribed information under Articles 13 and 14, data controllers should also separately spell out in unambiguous language what the most important consequences of the processing will be*" (p.7-para.10). **Article 13 exceptions to the obligation to provide information:** According to Article 13(4) GDPR, a data controller can be exempted from their information obligations "*where and insofar as, the data subject already has the information*". However, the Guidelines proposes in p.27-29 a best practice example which goes beyond the information obligations established in Article 13 ("*…the complete suite of*	**Obligation to provide information on the consequences of the processing:** The obligation to provide additional information (on top of Articles 13 & 14) to the data subject on the *most important consequences of the processing* goes beyond the GDPR requirements. This adds an overwhelming burden on data controllers. Therefore, such obligation should be removed from the guidelines. **Article 13 exceptions to the obligation to provide information:** The proposed best practice goes beyond the GDPR information obligations and increases information fatigue.	**Obligation to provide information on the consequences of the processing:** This obligation goes beyond GDPR requirements and therefore should be deleted. **Article 13 exceptions to the obligation to provide information:** The best practice example should be deleted from the Guidelines.

EDPB Guidelines	Guidelines requirements going beyond the GDPR text	Insurance Europe's views	Insurance Europe's recommendations in view of the GDPR evaluation and review report
	information should be provided to the data subject again…). **"Appropriate measures" to provide information under Articles 13 and 14:** The Guidelines states that "*a notification of changes should always be communicated by way of an appropriate modality (email, hard copy letter etc,) specifically devoted to those changes (eg not together with direct marketing content)* (…)". **Maximum time limit to provide information according to art. 14 (3):** The Guidelines establish in p.15 regarding Article 14(3(b)) that "*if the first communication with a data subject occurs more than one month after obtaining the personal data, then Article 14(3(a)) continues to apply, so that Article 14 information must be provided to the data subject at the latest within a month after it was obtained*". According to the Guidelines, the same rule applies when it comes to Article 14(3(c).	**"Appropriate measures" to provide information under Articles 13 and 14:** The requirement for a "*specifically devoted communication*" goes beyond the GDPR transparency requirements of Article 12 and imposes an unnecessary burden on data controllers. This obligation would also increase information fatigue and confusion among data subjects, which goes against the benefits sought by the GDPR transparency requirements. **Maximum time limit to provide information according to art. 14 (3):** The Guidelines introduce new deadlines to Articles 14.3 (b) and (c) GDPR. According to the Guidelines the obligation to provide information in Article 13 is subjected to time deadlines of one month. This is not in line with the GDPR since the one-month deadline is limited to Article 14(3(a)).	**"Appropriate measures" to provide information under Articles 13 and 14:** Sending a written communication (e-mail, hard copy letter, etc.) to address changes to the privacy notice/statement is sufficient and avoids consumer fatigue and confusion. The requirement for a "*specifically devoted communication*" goes beyond the obligations in GDPR and therefore should be deleted. **Maximum time limit to provide information according to art. 14 (3):** The additional time limits introduced by the Guidelines go beyond the established in the GDPR. Therefore, the general one-month limit in relation to Article 14 (3(b)) and Article 14(3(c)) should be removed from the Guidelines.
Guidelines on consent (link) ▪ Last revised and adopted April 2018 ▪ Insurance Europe's position paper	**Freely given consent in the insurance context**: The Guidelines do not explicitly mention that consent for the processing of sensitive data in the insurance context is freely given. However, they did clarify a number of	**Freely given consent in the insurance context:** The Guidelines interpretation of "freely consent" remains problematic. Insurers can face the situation where consent is regarded as not freely given if the data subject has no free choice or is	**Freely given consent in the insurance context:** A further revised version of the Guidelines should include a reference to the insurance sector to mention that *consent in the insurance context is freely given.*

EDPB Guidelines	Guidelines requirements going beyond the GDPR text	Insurance Europe's views	Insurance Europe's recommendations in view of the GDPR evaluation and review report
	aspects which lead to the conclusion that consent is not the appropriate legal basis when the data processing is necessary for the performance of the contract. In these cases, the Guidelines clarify that performance of the contract is the appropriate legal bases (p.8-9 and footnote 23). The Guidelines also acknowledged that consent is the only lawful basis to process sensitive data when none of the possibilities in Article 9.2 (b-j) apply (p.19).	unable to refuse or withdraw consent without detriment. In this scenario, not obtaining a contract or being proposed a higher premium could be interpreted as 'detriment', rendering consent invalid. This leaves insurers with no legal basis.	The following example could be included: *"An insurance company asks consumers for consent to use their health data for assessing the risks to be covered and for calculating the related insurance premium of a long-term care insurance policy. This processing of health data is necessary for entering into the insurance contract and thus consent shall be considered freely given. The company also asks for consumers' consent to process their health data for evaluating and paying out claims as provided for in the insurance policy. This processing of health data is necessary for the performance of the long-term care insurance contract and thus consent shall be deemed freely given".*
	Refusal and withdrawal of consent without detriment: The Guidelines explains in p.10-11 and example 8 that when the user of an app withdraws consent which leads to the downgrading of the service and where the data was not necessary to deliver that service, then there is detriment and thus consent is invalid.	**Refusal and withdrawal of consent without detriment:** According to example 8, insurers could argue that there is *no detriment* (consent is valid), when the user of an insurance app withdraws consent for data that is *necessary* for the delivery of the service/performance of the contract. However, this is an interpretation of the example which does not provide sufficient legal certainty for insurers.	**Refusal and withdrawal of consent without detriment:** The Guidelines should include examples (preferably related to insurance) explaining that there is no detriment (consent is valid) when the service is suspended because the user withdrew consent to process data that is necessary for the controller to provide the service/perform the contract.
	Consent on behalf of third parties in the insurance context: The Guidelines do not clarify whether a policy holder (parent) can consent on behalf of third parties (family	**Consent on behalf of third parties in the insurance context:** (1) The absence of an example/clarification in the Guidelines causes legal uncertainty. In this scenario insurers would have to seek	**Consent on behalf of third parties in the insurance context:** The Guidelines should include an example recognising that the obtention of consent by a policy holder on behalf of third parties is common practice in the insurance industry. For example, travel

EDPB Guidelines	Guidelines requirements going beyond the GDPR text	Insurance Europe's views	Insurance Europe's recommendations in view of the GDPR evaluation and review report
	members) to obtain for example travel insurance.	direct consent from all third parties to provide them with coverage. (2) Consumers will not be able to obtain insurance coverage for families in a quick way (online product). (3) It will be extremely burdensome for insurers to obtain and demonstrate that they have obtained direct consent from the third parties including existing contracts.	insurance/health insurance policies are taken out by a parent for the entire family. In these cases, consent given on behalf of third parties should be valid.
	Obligation to name third-party organisations: The Guidelines state that "(..)*to comply with Articles 13 and 14 of the GDPR, controllers will need to provide a full list of recipients or categories of recipients including processors* (p.13)".	**Obligation to name third-party organisations:** (1) The requirement to provide *full lists* goes beyond the information obligations established in Articles 13.1(e) and 14.1 (e). (2) Unachievable requirement: Insurance companies may need to send personal data to many service providers, therefore, the list of recipients can be very long or unknown at the moment of collection of the data subjects' data. For example, a travel insurance company is not be able to provide the names of the foreign medical experts or repatriation service providers to whom it may need to transfer personal data if an insured person has an accident.	**Obligation to name third-party organisations:** The Guidelines should not create additional obligations. Therefore, the wording *full lists* should be removed from p.13.
	Consent through electronic means: The Guidelines reflect on consent in the digital context: data subjects receive multiple consent requests which cause click fatigue. In these situations,	**Consent through electronic means:** (1) The Guidelines wording goes beyond the GDPR controllers' obligations: The GDPR does not place any obligations	**Consent through electronic means:** The Guidelines should be modified and include to be in line with the GDPR, for example, the following phrase "*the GDPR*

EDPB Guidelines	Guidelines requirements going beyond the GDPR text	Insurance Europe's views	Insurance Europe's recommendations in view of the GDPR evaluation and review report
	consent questions are no longer read. In this scenario, the Guidelines say that "*the GDPR places upon controllers the obligation to develop ways to tackle this issue*" (p.17). **Refreshing consent:** The Guidelines recommend in p.21 to refresh consent at appropriate intervals since providing all the information again helps to ensure the data subject remains well informed about how their data is being used and how to exercise their rights.	on controllers to ensure that data subjects read consent questions. (2) Disproportionate obligation (it is the data subjects' responsibility and not vice versa). **Refreshing consent:** The GDPR does not include any provisions which suggest that consent should be refreshed. The Guidelines recommendation goes beyond the requirements introduced in the GDPR. (1) Recommendation beyond GDPR text (2) No proven benefits, however, it increases controllers' burden and consumers' information fatigue. (3) Legal uncertainty: What happens if the consumer ignores the request to refresh consent but does not withdraw consent? Does consent remain valid?	*encourages controllers to find solutions to tackle this issue*". **Refreshing consent:** The recommendation in p.20 to refresh consent should be deleted.
Guidelines on codes of conduct and monitoring bodies (link) ▪ Final version adopted on June 2019 ▪ Insurance Europe's position paper	**Lack of economic viability to meet the accreditation requirements for monitoring bodies**: The Guidelines suggest unaffordable accreditation requirements. Very few organisations would be able to face the recurring costs of the requirements proposed in the Guidelines. For example: (1) To demonstrate independence: separate staff and management, separate budget and accountability. (2) To avoid conflicts of interest: to hire separate staff for the monitoring body	**Lack of economic viability to meet the accreditation requirements for monitoring bodies**: Codes of conduct are an instrument of self-regulation and therefore the Guidelines should consider feasible solutions in line with the GDPR for the monitoring of compliance of codes of conduct. Specially, codes of conduct should, as stated in the Guidelines, be "*a beneficial tool for both SME and micro enterprise business by providing a mechanism which allows them to achieve data protection compliance in a more cost-effective manner*".	**Lack of economic viability to meet the accreditation requirements for monitoring bodies**: Codes of conduct should serve their purpose which is to help an economic sector to comply with the GDPR. Therefore, excessive accreditation requirements should not prevent the adoption of codes of conduct. The Guidelines should be revised to propose economically viable requirements.

EDPB Guidelines	Guidelines requirements going beyond the GDPR text	Insurance Europe's views	Insurance Europe's recommendations in view of the GDPR evaluation and review report
	(3) The criteria to demonstrate the expertise of the body is also unachievable since there is no prior experience with a body of this nature and there is a shortage in the market of data protection experts. **The lack of possibility to present amendments to a draft code during the approval phase:** The Guidelines establish that once a code has been accepted for approval phase* the code can still be rejected by the DPA. This triggers reinitiating the whole administrative process of (i) submission, (ii) acceptance and (iii) approval. *At this stage the DPA has checked that the draft code does not present fundamental flaws.	**The lack of possibility to present amendments to a draft code during the approval phase:** The Guidelines introduces unnecessary burden and cost in the approval process of a code of conduct. The process should be effective, allowing the dialogue between the DPA and the drafting code owners. Cooperation should be encouraged through consultations or questionnaires from the DPA to the code owners when further clarifications or amendments are needed.	**The lack of possibility to present amendments to a draft code during the approval phase:** The approval of a code of conduct should be more effective and avoid unnecessary administrative burden and costs. The Guidelines should introduce the possibility of consultations between the DPA and the code owners to provide during the approval phase, if needed, amendments to the content of the draft code.
Draft guidelines on Article 25 Data Protection by Design and by Default (link) ▪ Version published for public consultation November 2019 ▪ Insurance Europe's position paper	**Definition of "state of the art":** The EDPB notes in footnote 6 and pages 7-8 that "*state of the art" can be identified as the technology level of a service or technology product that exists in the market and is most effective in achieving the objectives identified*". Moreover, the draft guidelines mention that "*neglecting to keep up to date with technological changes could therefore result in a lack of compliance with Article 25 GDPR*"	**Definition of "state of the art":** The EDPB statements and its economic implications go beyond the political agreement in Article 25 GDPR, where "state of the art" should be assessed together with other elements such as the cost of implementation. Moreover, even if data controllers have the obligation to stay up-to-date with technological developments, that does not imply an obligation to always update their systems, with the consequent organisational and financial burdens.	**Definition of "state of the art":** The EDPB should clarify in the final guidelines that its interpretation of "*state of the art*" does not imply the obligation for controllers to constantly update their systems to the latest DPbDD technology. In other words, instead of requiring a technology level that is the "most" effective in achieving the objectives identified, any effective technology level should suffice.

EDPB Guidelines	Guidelines requirements going beyond the GDPR text	Insurance Europe's views	Insurance Europe's recommendations in view of the GDPR evaluation and review report
	Interpretation of the "cost of implementation": The draft guidelines state in page 8 that the "*the controller shall plan for and expend the costs necessary for the effective implementation of all the principles*" and that "*incapacity to bear the costs is no excuse for non-compliance with the GDPR*".	**Interpretation of the "cost of implementation":** Nowhere in the GDPR, is stated or implied, as the EDPB suggests, that data controllers shall expend excessive resources to achieve a marginally higher level of DPbDD. It is more likely, that the legislators' intention was to propose a proportionality test including all the elements mentioned in Article 25 GDPR – *taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing* (…). Therefore, these elements should not be assessed in isolation, but as a whole.	**Interpretation of the "cost of implementation":** The EDPB should redraft the section in the guidelines on cost of implementation and propose a new chapter where all the aspects mentioned in Article 25 GDPR are analysed in the form of a proportionality test and follow a risk-based approach, and not in isolation as currently proposed in the draft guidelines. This approach would be in line with the spirit of the GDPR and in particular with the letter in Article 32 and recital 83.
	The balancing of interests in the section on lawfulness (page 15): The draft guidelines state that where Article 6 (1) (f) – legitimate interest - is the legal basis used for the processing of data, the controller should disclose the assessment of the balancing of interests. The draft guidelines also state that the controller must carry out an *objectively* weighted balancing of interest.	**The balancing of interests in the section on lawfulness** (page 15): The measure proposed by the EDPB goes beyond the requirements of the GDPR. Articles 13-15 GDPR clearly establish that, when processing data on the basis of legitimate interest, the controller shall simply disclose the information concerning the legitimate interests pursued. Moreover, the criteria of *objectivity* is not mentioned in Article 6 (1) (f) and so goes beyond the requirements of the GDPR.	**The balancing of interests in the section on lawfulness** (page 15): The final guidelines should be aligned with the GPDR with respect to the balancing of interests.
	Example on lawfulness (pages 15-16): The draft guidelines state that when the controller uses Article 6 (1) (b) GDPR – performance of a contract	**Example on lawfulness** (pages 15-16): The draft guidelines establish a principle which is not intended nor included in the GDPR, and that is to oblige controllers to	**Example on lawfulness** (pages 15-16): The example on pages 15-16 should be amended to be aligned with the principles established in the GDPR on the lawfulness of processing.

EDPB Guidelines	Guidelines requirements going beyond the GDPR text	Insurance Europe's views	Insurance Europe's recommendations in view of the GDPR evaluation and review report
	– as the legal basis to process data, then all data must be collected directly from the data subject, and in the case where some data needs to be collected from a third party then the only appropriate legal basis to do so would be Article 6 (1) (a) GDPR – consent.	always collect data directly from the data subject. This creates an uncertainty of the application of the legal bases included in the GDPR and risks diverging application.	
Draft guidelines on processing personal data in the context of connected vehicles and mobility related applications (link) ▪ Version published for public consultation February 2020 ▪ Insurance Europe's position paper	**Interplay between the ePrivacy Directive and the GDPR:** According to the ePrivacy Directive access to information that is stored in terminal equipment does not require consent if one of the exemptions in Art.5(3) of the Directive applies. However, the draft guidelines suggest in para.18 that in cases where an exemption of the Directive applies "*the processing of personal data including personal data obtained by accessing information in the terminal equipment is based on one of the legal bases as provided by Art.6 GDPR* ". **Remarks on consent:** ▪ **Quality of the user's consent**: Para.46 notes that "*data controllers need to pay careful attention to the modalities of obtaining valid consent from different participants, such as car owners or car users*". However, the EDPB acknowledges, in para.49, that in practice consent might be	**Interplay between the ePrivacy Directive and the GDPR:** The EDPB statement in para.18 creates a new obligation for data controllers. Following para.18, a legal basis under Art.6 GDPR would be required in cases where an exemption under Art.5(3) of the ePrivacy Directive applies to process data from the terminal equipment. The creation of such obligation is contrary to recital 173 and Art.95 GDPR. **Remarks on consent:** ▪ **Quality of the user's consent:** To save the hurdle created in para.46, the guidelines should stress that other legal bases under Art.6 GDPR can be considered as an alternative to consent. Furthermore, the guidelines should clarify that consent should not be required from passengers if they cannot be identified. In this context, it	**Interplay between the ePrivacy Directive and the GDPR:** The EDPB should clarify that para.18 explains that only further processing after gathering the data from the terminal equipment requires a legal basis under Art.6 GDPR. Insurance Europe recommends the following wording in para.18: "*In such cases, if there is **further processing** of personal data that has been obtained by accessing information in the terminal equipment, one of the legal bases as provided in Art.6 GDPR should apply* ". **Remarks on consent:** The EDPB should revise the draft guidelines to ensure that the final text recognises the existence and practical use of all legal bases in Art.6 GDPR to process personal data from connected vehicles. In particular, Insurance Europe calls the EDPB to acknowledge that in the context of motor insurance telematics, the most adequate legal basis to process personal data is Art.6(1) (b) GDPR– performance of a contract

EDPB Guidelines	Guidelines requirements going beyond the GDPR text	Insurance Europe's views	Insurance Europe's recommendations in view of the GDPR evaluation and review report
	difficult to obtain for drivers and passengers who are not related to the vehicle's owner. ▪ **Further processing of personal data – telemetry data**: The guidelines state in para.52 that "*telemetry data collected for maintenance purposes may not be disclosed to insurance companies without consent for the purpose of offering behaviour-based insurance policies*". ▪ **Transmitting personal data to third parties**: The EDPB recommends in para.95 that "*the data subject's consent be systematically obtained before their data are transmitted to a commercial partner acting as a data controller*". **Geolocation data-incompatibility of the guidelines with insurance**	would be impossible to obtain consent. ▪ **Further processing of personal data – telemetry data:** The statement in para.52 is correct, however, the EDPB should clarify that telemetry data which is necessary for the performance of a telematics insurance contract can be processed on the grounds of Art.6(1) (b) GDPR. Otherwise para.52 may be misunderstood in a way that the processing of telemetry data in the context of driving behaviour-based insurance policies always requires consent. ▪ **Transmitting personal data to third parties:** The recommendation in para. 95 is in practice unfeasible, moreover it is contradictory to the EDPB's statement in in para.93, where the guidelines note that "*the data controller may transmit personal data to a commercial partner, to the extent that such transmission is based on one of the legal bases stated in Art.6 GDPR*". **Geolocation data-incompatibility of the guidelines with insurance telematics:** The principles suggested in	**Geolocation data-incompatibility of the guidelines with insurance telematics:** The EDPB should revise the principles

EDPB Guidelines	Guidelines requirements going beyond the GDPR text	Insurance Europe's views	Insurance Europe's recommendations in view of the GDPR evaluation and review report
	telematics: The draft guidelines note in para.61 that the collection of geolocation data is subject to compliance with principles, such as (i) geolocation activation only when the user launches the functionality that requires the vehicle's location to be known and not to activate geolocation by default and continuously when the car is started. The EDPB also suggests (ii) the option to deactivate geolocation at any time. **Hybrid processing**: The draft guidelines state in para. 75 that "*while it is not always possible to resort to local data processing for every use-case, hybrid processing can often be put in place*". Moreover, para.75 notes that the data is to be processed inside the vehicle or by the telematics service provider, generating scores that should be transmitted to the insurer at predefined intervals, ensuring compliance with the principle of data minimization.	para.61 are contrary to the principle of fairness in insurance telematics and incompatible with national contractual law (see Insurance Europe's position paper page 3). **Hybrid processing:** To ensure an adequate performance of PAYD policies, it must be possible to transmit the score to the insurance undertaking at shorter intervals. Importantly, being able to transmit at short intervals means that the driver can see how they have driven after each ride, something that has a positive impact on road safety. Also, it is unclear in para.75 who can be considered a telematics service provider. It is currently not apparent, if the term "*telematics service provider*" encompasses vehicle manufacturers or the providers of the electronic communication services through which the data are transmitted. It might also mean that according to the EDPB the telematics infrastructure must be provided by an independent third party, which is not always possible. Unless the	suggested in para.61 of the draft guidelines and propose recommendations compatible with the principle of fairness in telematics insurance and with national contract law and sectorial mandatory guidance concerning telematics insurance**.** **Hybrid processing:** The EDPB should clarify that short transmission intervals are allowed between the data score and the insurer. This will enable the customer to see how they have driven after each ride. Moreover, the EDPB should introduce a more flexible approach to data minimization, allowing a better understanding of who can be the processor of the data originated in the telematics device.

EDPB Guidelines	Guidelines requirements going beyond the GDPR text	Insurance Europe's views	Insurance Europe's recommendations in view of the GDPR evaluation and review report
	Limitations to access raw data: The draft guidelines recommend limiting insurers' access to raw data in para.108 to prevent the creation of precise profiles of the driver's movements. This limitation is also suggested in para.74.	EDPB clarifies who can be considered a telematics service provider, companies might not be able to properly conduct "*hybrid processing*" as envisioned by the EDBP. **Limitations to access raw data:** Insurers understand the concerns raised by the EPDB in paras. 74 and 108, however, access to raw data remains essential to provide fair pricing for PAYD insurance. More importantly, the insurer needs access to at least one identifier (eg name, VIN) to be able to provide the insurance cover. Furthermore, the EDPB's interpretation on insurers' access to raw data can have a serious negative impact on competition and innovation in the motor insurance market, and impact insurers' ability to comply with regulatory requirements (see page 7 of the position paper).	**Limitations to access raw data:** The EDPB should provide further guidance in the final guidance on the bases to grant access to raw data from the telematics device used to offer PAYD. Moreover, the final guidelines should acknowledge that insurance companies need access to at least one identifier to know to which policyholder and the data score is being referred to, in order to be able to deliver the service and charge the correct individual. Finally, the EDPB should acknowledge that insurance companies also need access to raw data to ensure competition in the market and to comply with different legal obligations.