Position Paper

Insurance Europe's contribution to the Article 29 Working Party consultation on draft guidelines on transparency

Our reference:	COB-DAT-18-015	Date:	23 January 2018
Referring to:	Article 29 Working Party public consultation on the draft guidelines on transparency		
Contact person:	Georgia Bakatsia, Policy Advisor, Conduct of Business William Vidonja, Head of Conduct of Business	E-mail:	bakatsia@insuranceeurope.eu vidonja@insuranceeurope.eu
Pages:	5	Transparency Register ID no.:	33213703459-54

Introduction

Insurance Europe welcomes the Article 29 Working Party's (WP) draft guidelines on transparency under the General Data Protection Regulation (GDPR) and the fact that:

- The draft guidelines recognise the risk of information fatigue and provide for layering information as a way to mitigate such a risk in an online environment.
- The draft guidelines acknowledge that any potential development of a system of icons would have to follow an evidence-based approach, including extensive research to be conducted in conjunction with businesses and the wider public. Insurance Europe agrees that before developing any icons, their objectives should be clarified and their added-value for data subjects should be evidenced. Business representatives and other relevant stakeholders should be consulted before the development of standardised icons to avoid any potential unintended consequences. Standardised icons are already used for transparency purposes in various sectors, including the insurance sector, and therefore there is a risk of misleading consumers by using similar icons for different disclosures, as well as a risk of "icon fatigue".
- The draft guidelines clarify that inferred and derived data are excluded from the scope of Articles 13 and 14.

However, Insurance Europe is concerned that the draft guidelines go beyond the Level 1 GDPR requirements and it therefore invites the WP to provide the following clarifications.

Guidelines going beyond the Level 1 GDPR text

- **Layered approach** Insurance Europe welcomes the proposed layered approach to disclosures. However:

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

- The draft guidelines state on p.17 para. 30 that "*the WP recommends that layered privacy statements/notices **should** be used to link to the various categories of information which must be provided to the data subject, rather than displaying all such information in a single notice on the screen (…)*".

  The use of "should" in the proposed wording suggests that a layered approach is compulsory, while the GDPR Level 1 text does not impose such an obligation on data controllers.

  Insurance Europe believes that the guidelines should not prescribe or limit the forms and means of disclosure that data controllers can use. Instead, the guidelines should give flexibility to the data controller to use the most appropriate forms and means, including for instance a layered approach, depending on the circumstances of the case.

  Recommendation Para. 30 on p.17 should be amended as follows: "*layered privacy statements/notices **could** be used to link to the various categories of information (…)*". The use of "could" instead of "should" would clarify that a layered approach is an option, not compulsory. It would ensure that the guidelines do not go beyond the GDPR Level 1 requirements.

- Insurance Europe believes that the possibility to adopt a layered approach should not be limited to a digital context only, as suggested by the draft guidelines (p.17). The layered approach could also support transparency in paper-based and oral contexts, where administering the volume of information in a consumer-friendly manner, and thus avoiding information fatigue, remains a challenge. The layered approach should therefore be promoted, regardless of the medium or environment in which the information is given.

  For example, in an insurance context, where an injured party contacts their insurer by phone to request services, the controller, following a layered approach, could brief the consumer on the most relevant sections (eg the sensitive data that would be required and processed) while for details referring to the specific sections layered in the privacy statement. The full privacy statement could be then accessed online and/or be sent directly to the consumer by email. If, on the other hand, the controller had to provide all the information orally, consumers would be easily overwhelmed by such a volume of information. They would not understand their rights and how to make use of them if needed, which would defeat the transparency objectives of the GDPR.

  Recommendation The guidelines should explicitly refer to the fact that data controllers can also adopt a layered approach to disclosures in a non-digital/off-line context.

- **Reminders of privacy notices and statements** The draft guidelines state on p.16 para. 28 that "(…) where data processing occurs on an ongoing basis, in order to ensure fairness of the processing, the controller **should** reacquaint data subjects with the scope of the data processing, for example by way of a reminder of the privacy statement/notice notified at appropriate intervals".

  Articles 13 and 14 of the GDPR establish an extensive list of requirements, providing data subjects with high protection and knowledge of their rights and the data that will be processed. At the same time, data controllers face the complex challenge of complying with all the obligations established in those provisions. Therefore, introducing an additional requirement, as proposed on p.16 para. 28 of the draft guidelines, for controllers to re-notify the data subject with the information in Articles 13 and 14 would impose an unnecessary burden and go beyond the Level 1 GDPR text.

  Recommendation Insurance Europe suggests that the WP delete the requirement to re-notify privacy notices and statements as it goes beyond the Level 1 GDPR text.

- **Obligation to provide information on the consequences/effects of the processing** The draft guidelines state on p.8 para. 9 that, as a best practice, "*controllers should not only provide the*

prescribed information under Articles 13 and 14, but also separately spell out in an unambiguous language what are the most important consequences of the processing". In other words, the data controller should inform the data subject about the *effects* that the data processing, as described in the privacy notice, would have on them.

Moreover, the draft guidelines establish that "*the description of the effects should not simply rely on innocuous and predictable best-case examples of data processing*". With this obligation, the draft guidelines introduce an additional requirement to the requirements in Articles 13 and 14, going beyond the Level 1 GDPR text.

Furthermore, the requirement in the draft guidelines to provide an explanation of the effects of the processing through complex case studies would impose on data controllers an overwhelming burden that would be extremely difficult to implement.

Recommendation The obligation to provide information to the data subject on the consequences/effects of the processing, while not simply relying on innocuous and predictable best-case examples of data processing, goes beyond the GDPR requirements. It would add an overwhelming burden on data controllers. Therefore, Insurance Europe suggests deleting such an obligation from the guidelines.

- **Article 13 exceptions to the obligation to provide information** According to Article 13(4) of the GDPR, a data controller can be exempted from their information obligations under Article 13 "*where and insofar as, the data subject already has the information*". Therefore, a data controller will only be required to supplement previously given information, as stated in the draft guidelines (p.24 para. 49), to ensure that the data subject has a complete set of the information listed in Articles 13(1) and 13(2). Insurance Europe supports this approach, as it avoids overloading the data subject with information already provided.

  However, the proposed example on pp.24-25 suggests that "*as a matter of best practice however, all of this information* (ie both Articles 13(1) and 13(2), including already provided information) *should be provided to the data subject again*". Given the explanation above, the WP's proposed best practice goes beyond the GDPR actual information obligations and would only increase information fatigue.

  Recommendation Insurance Europe proposes the deletion of the proposed best practice example on pp.24-25.

- **"Appropriate measures" to provide information under Articles 13 and 14** Recital 58 and Article 12(1) of the GDPR establish that the principle of transparency requires the controller to take "appropriate measures to provide the information referred to in Articles 13 and 14 in a concise, transparent, intelligible and easily accessible form, using clear and plain language (…)".

  The draft guidelines establish on p.13 para. 22 that where the privacy notice/statement is changed, the controller should communicate these changes in such a way as to ensure that most recipients will notice them. Moreover, the draft guidelines suggest 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) (…)*".

  Insurance Europe regards the WP's suggested example of a "specifically devoted communication", as going beyond the GDPR transparency requirements of Article 12, imposing an unnecessary burden and costs on data controllers that would increase information fatigue and confusion among data subjects.

  Insurance Europe believes that sending a written communication (e-mail, hard copy letter, etc.) to address changes to the privacy notice/statement together with the regular contractual communications (which are different from marketing communications) would be in line with the GDPR transparency requirements ("concise, transparent, intelligible and easily accessible form, using clear and plain language"), provided that it is made clear where the privacy notice/statement starts and ends.

Recommendation Insurance Europe suggests the deletion of the words "*specifically devoted to those changes*".

- **Information obligations related to further processing** Article 6(4) of the GDPR allows further processing of personal data for purposes that are "compatible" with the original purposes for which the data was collected. To ascertain whether further processing is compatible with the original purposes, Article 6(4) establishes an obligation on the controller to run a compatibility test, which shall take into account, among other things, the parameters described in paragraphs (a), (b), (c), (d) and (e).

  Nevertheless, according to Articles 13(3) and 14(4), the data subject must have been previously informed about the possibility that further processing for other compatible purposes may take place. As the draft guidelines explain (p. 20 para. 38), this is to ensure that the data subject understands at the moment of collection of the data that further processing for a particular purpose may take place.

  The WP states on p. 21 para. 40 that, in the framework of further processing, "*controllers should provide data subjects with further information on the compatibility analysis carried out under Article 6.4 (…), (in other words an explanation as to how the processing for the other purpose(s) is compatible with the original purpose)*". Insurance Europe believes that the WP's position imposes on controllers a burden that goes beyond the obligations established in the GDPR and, in particular, against the obligations established in Recital 63, Articles 6(4), 13 and 14. Moreover, an obligation to reveal "further information"*,* could increase information fatigue among data subjects and ultimately force controllers to reveal business secrets.

  Recommendation Insurance Europe suggests that the WP clarify that "further information on the compatibility analysis" would not in any case entail revealing further information than the obligations established in Recital 63 and Articles 13 and 14. In other words, the controller should only provide information useful to the data subject to understand the purposes for which the data would be further processed.

- **Recipients or categories of recipients of the personal data** The draft guidelines state on p.32 that, for Articles 13(1)(e) and 14(1)(e), "*the default position for the controller should be to provide information on the actual (named) recipients of the personal data*" and that "*where the controller opts to provide the categories of recipients, the controller must be able to demonstrate why it is fair for it to take this approach*".

  Recital 63 explains that the controller has an obligation, among other things, to provide information regarding the recipients of the personal data. Articles 13 and 14 further clarify and establish that the controller shall provide information about the recipients or categories of recipients of the personal data (if any). Therefore, the GDPR does not impose, as suggested by the WP, a default option or preference to provide the data subject with the (named) recipients rather than the categories of recipients. Consequently, establishing a default option in favour of providing the (named) recipients would go beyond what is prescribed by law. Moreover, Insurance Europe's position is that, in many cases, the actual naming of all recipients would contradict the requirement of providing information in a concise and transparent way. For instance, the actual naming of IT service providers — who might frequently change — would have no benefit for the data subject and would easily lead to fatigue. In certain cases, it is not even feasible to disclose the names of all third parties. For instance, in the context of travel insurance, an insurer is not able to provide the names of the foreign medical experts to whom it may need to transfer personal data if an insured person has an accident while travelling abroad.

  Recommendation Insurance Europe suggests that the WP delete its proposal for a default option in favour of providing information on the actual (named) recipients, re-establishing the equal footing given in the GDPR to both options (to provide information on the recipients or on the categories of recipients of the personal data).

- **Information on the balancing test when legitimate interest is a legal basis** On p.31, the draft guidelines state that where legitimate interest is the legal basis for the processing "*as a matter of best practice, the data controller should also provide the data subject with the information from the balancing test, which should have been carried out by the data controller to allow reliance on Article 6.1(f) as a lawful basis for processing, in advance of any collection of data subjects' personal data*". The requirement to provide information from the balancing test is not listed in the GDPR and goes beyond the Level 1 text. Articles 13(1(d)) and 14(2(b)) of the GDPR require that the data controller inform the data subject of the legitimate interests, without any reference to information/result of the balancing test.

  Recommendation Insurance Europe suggests that the WP delete the best practice on the disclosure of the balancing test, since it goes beyond the Level 1 GDPR text.

- **Maximum time limit according to Article 14(3)** On p.15, the draft guidelines state that the maximum time limit within which Article 14 information must be provided to a data subject is one month. However, Article 14(3(b)) states that when personal data is to be used for communication with the data subject, the information shall be provided at the latest at the time of the first communication to that data subject. Similarly, Article 14(3(c)) states that when a disclosure to another recipient is envisaged, the information shall be provided at the latest when the personal data is first disclosed. Articles 14 (b) and (c) introduce new deadlines and do not refer to the maximum time limit of one month.

  The draft guidelines therefore go beyond the Level 1 GDPR text as, regarding Article 14(3(b)), it is mentioned 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 WP, the same rule applies when it comes to Article 14(3(c)).

  Recommendation Insurance Europe suggests that the WP delete the general one-month limit in relation to Article 14 (3(b)) and Article 14(3(c)) as it goes beyond the Level 1 GDPR text.