Position Paper

# Insurance Europe contribution to Article 29 Working Party guidelines on DPIAs

| | | | |
|---|---|---|---|
| Our reference: | COB-DAT-17-043 | Date: | 23 May 2017 |
| Referring to: | Article 29 Working party guidelines on data protection impact assessments (DPIAs) | | |
| Contact person: | Lamprini Gyftokosta, Policy Advisor, Conduct of Business | E-mail: | Gyftokosta@insuranceeurope.eu |
| Pages: | 3 | Transparency Register ID no.: | 33213703459-54 |

## Introduction

Insurance Europe welcomes the Article 29 Working Party's (WP) guidelines on the Data Protection Impact Assessment (DPIA) and the intention to help stakeholders to determine whether processing is "*likely to result in a high-risk*" for the purposes of Regulation 2016/679.

Insurance is a highly-regulated sector, and the General Data Protection Regulation (GDPR) is one of the many new EU regulations that insurers have to comply with by 2018. For example, insurance consumer protection rules will change as a result of the Packaged Retail and Insurance-based Investment Products Regulation (PRIIPs) and the Insurance Distribution Directive (IDD), which are both to be completed by additional Level 2 and Level 3 measures in the following months.

For the new regulatory framework to be successful, it is crucial to ensure that stakeholders have sufficient time to provide input and that the industry has sufficient time to prepare for implementation. The technical work for new consumer protection rules mentioned above therefore always goes through an appropriate consultation process as part of a dialogue with stakeholders and the European Insurance and Occupational Pensions Authority (EIOPA).

Similarly, it is important for the WP to continue the dialogue with stakeholders on the implementation of GDPR. Insurance Europe welcomes the decision of the WP to extend the consultation period to six weeks instead of four, but still believes that consultation periods of at least three months and ongoing opportunities to contribute to the process as part of a dialogue will help ensure that European insurers and consumers fully benefit from a high-quality new regulatory framework.

## Guidelines should respect Level 1 GDPR text

Insurers recognise the importance of data protection, since data processing lies at the very heart of their business. Insurers collect and process data to analyse the risks that individuals wish to cover and this allows them to tailor products accordingly. Data processing is also an essential part of evaluating and paying policyholders' claims and benefits, and the detection and prevention of fraud.

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 guidelines would provide insurers with an important clarification tool enhancing legal certainty when implementing and interpreting the GDPR provisions. However, the WP guidelines should not go beyond the Level 1 text of GDPR, as agreed by the EU co-legislators. This is extremely important: although these guidelines are non-binding, they may be introduced as compulsory requirements at national level. A great deal of responsibility and importance is, therefore, attached to the quality of these guidelines.

For instance, on page 7 of the guidelines, the WP refers to Article 35(1) stating that "the carrying out of a DPIA is only mandatory where a processing *is likely to result in a high risk to the rights and freedoms of natural persons*". At the same time, the WP recommends that a DPIA should also be carried out in cases where it is not clear if the processing operations are likely to result in a high risk. The WP advises that in these cases a DPIA is a useful tool and demonstrates compliance with the rules.

Following a strict and literal reading of the guidelines, data controllers would have to carry out DPIAs to ensure that they are compliant. As a consequence, the scope of the DPIAs is significantly broadened, going beyond the political agreement in the Level 1 text.

Similarly, on page 8 of the guidelines, the WP significantly broadens the definition of sensitive data, by including location and financial data. This expands considerably the scope of mandatory DPIAs and goes beyond the scope of sensitive data in Articles 9(1) and 10 of GDPR.

Additionally, on page 12, the WP suggests that the DPIAs are reviewed every three years, despite the fact this is not foreseen by GDPR. Insurance Europe believes that such a recommendation goes beyond Level 1 text and suggests that such a review should be left at the discretion of the data controller.

Finally, on page 17, the WP acknowledges that the GDPR does not require publishing a DPIA, however, such practice is strongly encouraged. For reasons explained earlier regarding the strict and literal interpretation of the guidelines by national DPAs, insurers are concerned that such a publication would de facto become an obligation and would not be left up to controllers to decide, despite this being allowed under GDPR.

There are already several requirements in place that can demonstrate accountability and transparency in the insurance sector, including provisions in the Insurance Distribution Directive and Solvency II Directive. This recommendation to publish DPIAs should not be included in the guidelines, as it goes beyond the Level 1 text, or at least its scope should be narrowed down to cases where a public authority carries out a DPIA.

## DPIAs in the insurance context

Based on Article 35(3)(a) of GDPR, insurers would be obliged to conduct a DPIA because they systematically and extensively evaluate personal aspects relating to natural persons based on automated processing, including profiling.

Similarly, Article 35(3)(b) of GDPR and the recently adopted WP guidelines on the Data Protection Officer (DPO), indicate that an insurance company must conduct a DPIA because it processes data on large-scale as part of the regular course of its business. In both cases, the processing operations described are considered of "high risk" by default.

Insurance Europe would like to raise the following insurance specific concerns over the interpretation and application of the DPIAs guidelines and provide some recommendations.

- **Non-retroactive application of DPIAs**

Insurance Europe welcomes the clarifications on the non-retroactive application of DPIAs provided on page 11 of the guidelines, which confirm that "*the requirement to carry out a DPIA applies to processing operations meeting the criteria in Article 35 and initiated after the GDPR becomes applicable on 25 May 2018*".

To avoid implementation issues stemming from a narrow interpretation of the WP's recommendation to carry out DPIAs for processing operations already underway prior to May 2018, the WP should delete the sentence in page 11 stating *"WP29 strongly recommends carrying out DPIAs for processing operations already under way prior to May 2018"* from the final guidelines.

- **Broad definition of "vulnerable subjects"**

The WP provides a list of non-exhaustive examples of "vulnerable subjects" that could fall under Recital 75 of GDPR, including employees. This is a very broad definition, that includes a wide range of data subjects that may not carry the same degree of vulnerability. As a consequence, the scope of the DPIA is also broadened.

However, it is crucial to reiterate that a party in a disadvantaged position does not automatically fall under the vulnerable subject definition. In almost every relationship one party could be in a disadvantaged position. This does not constitute a relevant basis to assign it a vulnerable character. Vulnerability should be determined by using a more pragmatic approach and context.

For instance, employees may be considered to be in a disadvantaged position in the employment relationship. However, they should not automatically fall under the criteria for vulnerable subjects, when the processing of employees' data takes place in the context of staff administration only (payment of wages, social rules, reimbursement). This is a distinctly different situation from processing operations where the employees' data could be used to evaluate and assess performances (profiling).

Therefore, the WP should adopt a more pragmatic approach to the definition of vulnerable subjects, especially when it comes to employees' data.

- **Data subject representatives**

Article 35(9) states that where appropriate, controllers should be seeking the views of data subjects' representatives on the intended processing. However, in page 13 of the guidelines, there are no examples illustrating when this could be "appropriate" and it is also not clear who falls under the "data subject representatives" category.

In some cases, it could prove problematic for insurers to involve data subject representatives in the review of processing operations, especially if the same representatives are involved in reviewing processing operations of other insurers in the same sector, as this would raise competition concerns or could give away trade secrets or commercially sensitive information.

It is also important to remember that insurance is a heavily regulated and supervised sector. Therefore, data subjects' views are upheld by the supervisory authorities, including the WP and the European Insurance and Occupational Pensions Authority (EIOPA). Consequently, an additional layer of the data subject involvement would create an additional burden for data subjects and insurers, without adding any value.