European Payment Institutions Federation aisbl

23 MAY 2017

EPIF RESPONSE TO THE ARTICLE 29 WORKING PARTY GUIDELINES ON DATA PROTECTION IMPACT ASSESSMENT (DPIA)

ABOUT EPIF (EUROPEAN PAYMENT INSTITUTIONS FEDERATION)

EPIF, founded in 2011, represents the interests of the non-bank payment sector at the European level. We currently have over 190 authorised payment institutions and other non-bank payment providers as our members offering services in every part of Europe. EPIF thus represents roughly one third of all authorized Payment Institutions in Europe. Our diverse membership includes a broad range of business models, including:

- 3-party Card Network Schemes
- Acquirers
- Money Transfer Operators
- FX Payment Providers
- Mobile Payments
- Payment Processing Service Providers
- Card Issuers
- Third Party Providers
- Digital Wallets

EPIF seeks to represent the voice of the PI industry and the non-bank payment sector with EU institutions, policy-makers and stakeholders. We aim to play a constructive role in shaping and developing market conditions for payments in a modern and constantly evolving environment. It is our desire to promote a single EU payments market via the removal of excessive regulatory obstacles.

We wish to be seen as a provider for efficient payments in that single market and it is our aim to increase payment product diversification and innovation tailored to the needs of payment users (e.g. via mobile and internet).

EPIF RESPONSE TO CONSULTATION

- **General comments**
  - The approach taken in the Guidelines will result in making a DPIA mandatory for the majority of all data processing activities pursued, in particular if global players like EPIF members are involved. Whereas the **DPIA** has been designed as an **exceptional instrument in the GDPR**, a DPIA will become the rule according to the Guidelines.
  - The Guidelines focus on "when a DPIA is required". They say hardly anything about when a DPIA is not required which even fosters the "DPIA as a rule" instead of "DPIA as an exception". In other words, in cases where it is not clear whether a DPIA is required, the WP29 recommends that a DPIA is carried out nonetheless, as a DPIA is a useful tool to help data controllers comply with data protection law. This widens the net significantly and may result in companies committing scarce resources to a DPIA **when it is not in fact needed, just because companies do not have clarity on what is required**.
  - The GDPR requires a DPIA if the processing is "likely to result in a high risk to the rights and freedoms of natural persons". The "two criteria approach" of the Art. 29 Working Party might help as a first step for the sorting of "high risk processing activities". However, it is much too schematic. The assessment whether a processing activity entails a "high risk" must at the end of the day always be assessed based on a proper risk quantification, taking into account the specific technical and organizational measures taken by the controller.
  - Art 29 Working Party says that in cases where it is not clear whether a DPIA is required, the WP29 recommends that a DPIA *is carried out nonetheless*, as a DPIA is a useful tool to help data controllers comply with data protection law. The WP29 recommendation goes beyond the legal scope of the primary legislation, as the legislation says that a DPIA is not required in all circumstances, only where there is high risk. The question is **what 'high risk' means to the regulators and to companies**. **Companies need legal certainty** of how the rules will be applied. The uncertainty of interpretation will be problematic and could have a chilling effect on European innovation, if companies need to carry out unnecessary DPIAs. We call on regulators to give guidance on their interpretation of high risk or offer an open door policy while they develop their thinking. We advocate an approach where the company records the detailed reasons why a DPIA is not required, after a thorough assessment. The assessment would need to show that processing is not likely to result in high risk. We would advocate an approach where the assessment can be discussed with the relevant regulator prior to the processing, if the situation is unclear. If the regulator does not yet have the resources to deal with many inquiries from companies, then companies should be allowed to continue once a specified period for the response has elapsed eg one month. It would not serve EU commerce to have a regulatory bottle neck. Regulators should quickly publish & update guidelines on what constitutes high risk. We support guidelines that take a results

based approach and set out results based criteria to determine what is considered high risk, to encourage a consistent approach.

- **Specific comments (Pages 7, 8 and 5)**
  - "**Evaluation**" is too broad as a trigger criterion for DPIA. The focus should be on the (intended) use of the evaluation or scoring and whether that use will likely result in high risks to the rights and freedoms of natural persons.
  - It is unclear what the concept of "**monitoring**" shall encompass. It should be clarified if it is only about physical monitoring (e.g. via CCTV) or also IT based control (e.g. web usage monitoring, keyword filtering, etc.).
  - "**Sensitive data**"
    - "Sensitive data" should not be a stand-alone trigger criterion, as the GDPR requires "processing on a large scale of special categories of data". The large scale of the processing should be added to avoid a limitless DPIA increase.
    - A whitelist for the processing of "sensitive data" in the employment context is urgently required because otherwise most of employers' data processing activities will require a DPIA (sickness data in personal files, sickness data in personal administration tools, union membership and church membership in payroll systems, etc.)
  - **Data processed on a large scale**: the GDPR does not define what constitutes large-scale, though recital 91 provides some guidance. In any event, the WP29 recommends that the following factors, in particular, be considered when determining whether the processing is carried out on a large scale

    a. the number of data subjects concerned, either as a specific number or as a proportion of the relevant population;

    b. the volume of data and/or the range of different data items being processed;

    c. the duration, or permanence, of the data processing activity;

    d. the geographical extent of the processing activity.

    Comment: These factors (a-d) are not particularly helpful, some more concrete examples would be more helpful to determine how to assess what they mean by large scale.

- **Specific comments (Pages 9 and 13)**
    - "**Vulnerability**" needs to be assessed on a case-by-case basis and should not be assumed, in particular in employment relationships or for candidates as it depends on the type of processing and the specific processing situation whether there actually is an imbalance of power between the employer and the employee or candidate.
    - "**Innovative use or applying technological or organizational solutions**": New technology does not automatically lead to a high or increased risk to the rights and freedoms of natural persons. This is a technophobic approach that casts an air of general suspicion over new or innovative uses of technology.
    - **Data transfer outside of the EU** should not be a trigger criterion for DPIA. The "risk" related to such a transfer is already mitigated through the "appropriate safeguards" (Chapter 5 of the GDPR) that need to be put in place by a controller sharing data across EU-borders.

- It is stated that the controller must "seek *the views of data subjects or their representatives"* (Article 35(9)), "where *appropriate".* The WP29 considers that those views could be sought through a variety of means, depending on the context (e.g. an internal or external study related to the purpose and means of the processing operation, aformal question to the staff representatives or trade/labour unions or a survey sent to the data controller's future customers);if the data controller's final decision differs from the views of the data subjects, its reasons forgoing ahead or not should be documented; the controller should also document its justification for not seeking the views of data subjects, if it decides that this is not appropriate.

  Comment: "Where appropriate" is a particularly unhelpful criteria, and examples of what the WP29 would find appropriate are necessary. Also, practically speaking, the feasibility and benefit of doing this in a corporate environment, where there are commercial pressures to roll out systems, products, by defined timeframes, is questionable. It will take a disproportionate amount of time to canvas the views of data subjects, analyse that data and document it. The views of data subjects may vary widely in terms of how they view particular processing. If the organisation is carrying out a DPIA done by qualified individuals, DPO's, lawyers, etc. to determine the risk, based on the overall regulation, this should be enough. There is ample allowance for data subjects to exercise their rights through complaints to organisations and regulators.