To:

Article 29 Working Party

JUST-ARTICLE29WP-SEC@ec.europa.eu
presidenceg29@cnil.fr

EUROPEAN BANKING FEDERATION'S COMMENTS ON THE ARTICLE 29 WORKING PARTY GUIDELINES ON DATA PROTECTION IMPACT ASSESSMENT (DPIA) - WP248

EBF Key points:

- **Data Protection Impact Assessment (DPIA) should be based on a risk-based approach:**

  We understand that the Article 29 Data Protection Working Party (WP29) intends to recommend a risk-based approach, but this can be clarified and strengthened in the guidelines.

  - **No mandatory DPIA for data processing requested by legal requirements:**

    A DPIA is intended to produce protection and privacy-friendly solutions where a data processing is likely to result in a high risk. If, however, a bank is subject by law to certain data processing requirements (e.g. monitoring payments to combat money laundering and fraud, processing employee data to comply with statutory tax and social security provisions), the legislator has already decided that such processing is legitimate. The bank has no discretion as to whether it performs the processing called for by the legislator or not.

  - **Scope:**

    The Guidelines provide a very large scope of criteria (listed on page 7-9) which are not adapted to the banking practice. An application of the current Guidelines would mean that each processing of financial data on a large scale would be considered as "likely to result in a high risk" under Article 35 (3). This will require banks to conduct a DPIA for most of their day-to-day operations/activities which would be disproportionate to the low risk of most bank data processing. Most routine data processing by banks is highly regulated, well controlled and well understood, and will not pose a high risk to data subjects.

European Banking Federation aisbl

Brussels / Avenue des Arts 56, 1000 Brussels, Belgium / +32 2 508 3711 / info@ebf.eu
Frankfurt / Weißfrauenstraße 12-16, 60311 Frankfurt, Germany
EU Transparency Register / ID number: 4722660838-23

www.ebf.eu

- **The "high risk to the rights and freedoms of natural persons" should be the deciding factor to conduct a DPIA:**

  While it is, in principle, helpful to provide examples of cases in which a DPIA should be conducted, an obligation to carry out a DPIA should not automatically be inferred from these examples. Instead, the "*high risk to the rights and freedoms of natural persons"* threshold should be the deciding factor to conduct DPIA. The 'criteria' for high risk should be reframed as 'factors' for controllers to consider when determining high risk. Factors that suggest that processing is 'low risk' should also be added and should include in particular the presence of other relevant regulation that protects data subjects.

- **The WP29 Guidelines on DPIA requirements should not go beyond the scope defined by the GDPR:**

  The Guidelines in many ways will be of help for the companies in their work with Data Protection Authorities. However, we observe that certain provisions go beyond the General Data Protection Regulation (GDPR). Helping interpretation of the text is useful, but seemingly, expanding the requirement to carry out a DPIA beyond the provisions of the GDPR should be avoided. This would pose unmanageable challenges to companies and also be at odds with the risk-based approach of targeted use of limited resources for particularly important cases ("be selective, be effective").

- **DPIA for existing processing operations:**

  The Guidelines strongly recommend to carry out DPIAs for processing operations already underway prior to the entry into force of the GDPR. It seems rather burdensome to expect organisations to assess all of their existing processing operations as if they were already subject to DPIA. The Guidelines should be aligned with the scope defined by the Level 1 GDPR text, and not go beyond.

  We propose to omit such a recommendation in view of the fact that the requirements for the future are already very challenging.

EBF Response:

GENERAL COMMENTS

The European Banking Federation (EBF) welcomes the possibility to provide comments on the Guidelines prepared by the Article 29 Data Protection Working Party on the Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 adopted on 4 April 2017.

The EBF supports the objectives of the Guidelines, DPIAs are indeed useful tools which are linked to the privacy-by-design principle and have been used in several countries where they are reasonably consolidated. It is in essence a data protection risk analysis exercise in relation to a system, product or service. It allows the identification of possible risks in advance (before launching the product or service) and measures to mitigate risks.

Yet, we believe it is important to take into account the fact that many industries process personal data to a certain degree. In addition, there are significant differences between sectors, in terms of the types of data stored and collected, the purposes of processing and the quantity of regulation that surrounds and controls the processing.

The banking sector processes data primarily to execute transactions, detect and prevent financial crime, and comply with other regulatory requirements. Banks are subject to significant regulatory requirements to manage risks and ensure security. For example the Anti-Money Laundering (AML) Directive imposes Know Your Customer requirements and requires customer due diligence to prevent banks services from being used for money laundering or terrorist financing. The DPIA for the processing of data for AML and fraud prevention purpose should not necessarily be mandatory. The legislator has already decided that such processing is legitimate. The bank has no discretion as to whether it performs the processing called for by the legislator or not. The personal data processing, in this case, is based on compliance with legal obligations, and the broader public interest of this processing overrides the interests of individual data subjects.

We observe that the Guidelines and lists of high-risk processing inadvertently, target very different types of processing from various industries. A proportionate and nuanced approach should be adopted to avoid creating false equivalence between, for example, tracking transactions for marketing purposes and those to detect fraud which will give rise to different issues. For this reason, the purpose of the processing should be taken into account when deciding whether a DPIA is needed or not.

Similarly, the existence of other relevant regulations and laws should be taken into account. In the banking sector, significant regulation exists already to protect consumers and employees. Firms should be able to take these protective measures into account when making an initial risk assessment.

Putting prescriptive lists of criteria in guidance risks would lead firms to conduct DPIAs when not necessary. This can lead to firms overlooking other instances of risk not covered by the list of criteria, meaning other processing, which should be subject to a DPIA, is not.

DPIAs may be taken into account to evaluate the due diligence of the controller in the implementation of measures to comply with legal requirements. However, each organisation, depending on its needs, culture and structure may adapt the orientation of DPIA. Companies (or even sectors) may have their own privacy risk policies as long as they consider the main aspects covered by a DPIA.

It is therefore important to ensure that the final guidelines avoid prescriptive rules and closed lists of high-risk activities. Instead, they should aim for high-level guidelines, proposing factors for firms to consider in assessing risk and examples, while acknowledging the relevance of differences between industries and businesses. In addition, the Guidelines should be aligned with the scope defined by the Level 1 GDPR text, and not create new obligations.

Paragraph A. What does a DPIA address?

(See page 6 of the WP29 guidelines)

Assessment of multiple processing operations

According to Article 35 (1) "*Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks"*.

We understand that a single DPIA could be used to assess multiple processing operations that are similar in terms of existing high risks. To this aim, the Article 29 Data Protection Working Party ("WP29") recommends that the specific nature, scope, context and purposes of the processing shall be taken into account.

We would however welcome further clarifications on whether a single DPIA could be used to assess multiple processing operations (similar in terms of existing risks) when only one of the criteria mentioned above (namely: nature, scope, context and purpose of processing) is similar to the different operations or whether all four criteria shall necessarily be similar occur.

In our views, some flexibility should be provided to the controllers to include different types of processing activities under a single DPIA, when appropriate.

Paragraph B. Which processing operations are subject to a DPIA?

(see page 7 of the WP29 guidelines)

a) When is a DPIA mandatory? (see page 7 to 11 of the WP29 guidelines)

A DPIA is only mandatory under Article 35 of the General Data Protection Regulation (GDPR) where a processing is "likely to result in a high risk to the rights and freedoms of natural persons". This makes it clear that a DPIA is by no means an instrument intended for regular or even blanket use. The DPIA should be conducted only where there are special risks.

There is no definition of what "high risk" means, but it likely corresponds to the extent and frequency of processing which may adversely affect or otherwise interfere with the rights and freedoms of the data subject.

The Article 35 (3) of the GDPR provides a non-exhaustive list of examples of processing "likely to result in high risk" which require a DPIA.

In order to define more concrete set of processing requiring a DPIA, the WP29 Guidelines set out specific criteria, which include "*evaluation or scoring, including profiling; automated decision-making; systematic monitoring of individuals; processing sensitive data; processing data on a large scale; matching or combining datasets; processing data concerning vulnerable data subjects; innovative use or application of technological or organizational solutions; data transfer across borders outside the European Union and processing which in itself prevents data subjects from exercising a right or using a service or a contract"*.

The WP29 Guidelines also remain unclear when mentioning that *"as a rule of thumb, a processing operation meeting less than two criteria may not require a DPIA due to the lower level of risk"* and at the same time stating that *"in some cases, a processing meeting only one of the criteria will require a DPIA"*.

In our views the criteria listed by the WP 29 Guidelines are very broad as, in practice, they risk forcing banks to conduct a DPIA for many kinds of activities that do not pose genuine high risks to data subject (instead of dedicating the necessary resources to genuinely risky processing activities). It is particularly the case when the WP29 Guidelines states that "*if the controller believes that despite the fact that the processing meets at least two criteria, it is considered not to be "likely high risk", he has to thoroughly document the reasons for not carrying out a DPIA*".

While it is, in principle, helpful to provide examples of cases in which a DPIA is to be conducted, an obligation to carry out a DPIA should not automatically be inferred from these examples. The purposes, context, and wider controls relating to a processing operation are all relevant.

Instead, the "*high risk to the rights and freedoms of natural persons*" threshold should be the deciding factor to conduct a DPIA. The 'criteria' on pages 7-9 should be reframed as 'key factors for controllers to consider', or similar. As outlined below, the 'criteria', while helpful for some types of processing, miss important factors relevant to banking (and potentially also other industries).

WP29 should amend the '*rule of thumb*' to clarify that where two or more factors are present, a DPIA will "*often* be required" (top of page 10).

In our view, a risk-based approach should be reinforced and a non-exhaustive list of factors and examples that imply low risk should be provided as well.

This list should include in particular other regulation in place which protects the data subjects' rights and interests. For example, in the context of the banking sector, there is extensive regulation in place to protect customers who wish to borrow money (for example, the Mortgage Credit Directive).

Please find below more specific comments on the criteria proposed by the WP29 Guidelines, to help highlight the fact that there are other relevant factors, meaning a risk based approach should be favored:

- **Point 2. Automated decision making with legal or similar significant effect:**

  We would welcome further clarifications in the upcoming Guidelines on profiling and automated decision making, of the meaning of *"legal"* or *"similar significant effect"* on the data subject. Moreover, there is also a need to clarify the extent of human intervention in case the data subject asks for it.

- **Point 4. Sensitive data:**

  The Guidelines refer to *"personal data relating to criminal convictions or offences"* and more particularly to *"electronic communication data, location data and financial data (that might be used for payment fraud)".*

  In our views, the list of sensitive data provided by the Guidelines is very broad and could concern any of the bank's activities. The banking sector processes data primarily to execute transactions, detect and prevent financial crime, and comply with other regulatory requirements. Banks are subject to significant regulatory requirements to manage risks and ensure security. For example the Anti-Money Laundering (AML) Directive imposes Know Your Customer requirements and requires 'customer due diligence to prevent banks' services from being used for money laundering or terrorist financing. In line with Article 35 (10) of the GDPR which provides an exemption, we believe that when the processing of data is compliant with existing legislation, the DPIA should not be necessarily mandatory.

  Moreover, Article 9 of the GDPR referring to *"processing of special categories of personal data"* already provides an exhaustive list of personal data processing[1]. Only the data mentioned in Article 9 (and potentially Article 10) of the GDPR are considered to be sensitive and no other type of data (e.g financial data) can have this consideration. The Guidelines should not go further than the definition of the GDPR, as in this case, the list provided by the Article 9, is not a non-exhaustive list but clearly a closed exhaustive list.

  Care is needed to protect some types of financial data, but the level of risk will depend on the exact data and the nature of the processing. For example, online banking credentials or other information that can be used to identify a customer require greater care than a bank statement. Similarly, data held internally within a bank's systems may pose lower risks than when this is shared with (perhaps unregulated) third parties. A blanket suggestion, that such data pose similar levels of risk as data under Article 9 and Article 10, is therefore not appropriate.

  It would have been useful to have further justifications from the WP 29 regarding the choice of such examples as electronic communication, location data, and financial data.

- **Point 5. Data processed on a large scale**:

  According to the definition of *"data processed on a large scale"* provided by the Guidelines, particularly given the inclusion of 'large scale', it is likely that nearly every processing operation by a financial services firm would require a DPIA.

  However, the amount of data or the number of data subjects concerned ("large scale") are, on their own, not a sufficient or determining measure of a high risk. This is shown by the handling of payments in the banking sector, covering billions of transactions annually and millions of data subjects. This processing is tightly controlled and regulated, and there is no evidence of any high data protection risks.

[1] *"Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited (…)".*

We believe that a risk-based approach should be adopted and that Guidelines should instead provide examples of large-scale processing activities that do not require a DPIA.

- **Point 7. Data concerning vulnerable data subjects (Recital 75):**

  Member State law or collective agreements, including 'works agreements', may already provide for specific rules on the processing of employees' personal data in the employment context, in particular for the conditions under which personal data in the employment context may be processed on the basis of the consent of the employee, the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, and for the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship (see recital 155 and Article 88 of the GDPR already covering those provisions).

  Application of the *'vulnerable data subjects'* criteria to the processing of employee data is therefore in our view inappropriate because it would mean that every employer might be required to conduct a DPIA in the area of human resources management. As such, the Guidelines should include a specific reference to the fact that processing of employee data in the employment context does not fall under these criteria.

- **Point 9. Data transfer across borders outside the European Union**

  The GDPR already requires firms to put in place safeguards to protect data subjects when personal data is transferred outside of the EU. Where an adequacy decision is in place, or where safeguards such as model contracts or Binding Corporate Rules are in place, firms should be able to rely on these.

- **Point 10. When the processing in itself "prevents data subject from exercising a right or using a service or a contract":**

  It is important to recall that the purpose of the impact assessment is to assess the particular likelihood and severity of the high risk, taking into account the nature, scope, context and purposes of the processing and the sources of the risk. That an impact assessment should include, in particular, the measures, safeguards and mechanisms envisaged for mitigating this risk, ensuring the protection of personal data and demonstrating compliance with the GDPR. It should not be deflected from its primary objective and used to assess whether the data subject was able to access a service or enter into a contract. Several pieces legislations already prevent unfair practices. For example, the performance of credit worthiness assessments is already strictly regulated under European consumer credit/mortgage credit directives, in order to protect data subjects.

  This point is also relevant in the context of criteria 1 and 2.

  Thus, these last criteria should be removed and properly analysed in the upcoming WP29 Guidelines on Profiling.

Paragraph c) What about already existing processing operations? *(see page 11 to 12 of the WP29 guidelines)*

- The Guidelines note that the requirement to carry out a DPIA applies to processing operations initiated after the GPDR becomes applicable on 25 May 2018.

  However, the Guidelines strongly recommend carrying out DPIAs for processing operations already underway prior to the entry into force of the GDPR. This goes beyond the requirements of the GDPR Level 1 text.

  Furthermore, the word 'underway' is unclear as it is not clear which period banks would have to consider.

  We propose to omit such a recommendation in view of the fact that the future requirements are already highly challenging. It is appropriate to review processing, and potentially to carry out a DPIA, when risks change significantly, but the Guidelines should not suggest this as a systematic practice.

  It seems rather burdensome to expect organizations to assess all of their existing processing operations as if they were already subject to DPIA. The Guidelines should be aligned with the scope defined by the Level 1 GDPR text, and not go beyond.

- The Guidelines provide further requirements regarding the review of the impact assessment compared to the GDPR (Article 35 (11)). They particularly mention that "*As a matter of good practice, a DPIA should be continuously carried out on existing processing activities. However, it should be re-assessed after 3 years, perhaps sooner, depending on the nature of the processing and the rate of change in the processing operation and general circumstances. Such assessment is also recommended for data processing which have taken place before May 2018 and where therefore not subject to a DPIA, to make sure that 3 years after this date or sooner, depending on the context, the risks for the rights and freedoms are still mitigated*".

  We believe this new requirement is disproportionate and not in line with Article 35 (11) of the GDPR which states that "*Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations*".

  Rather than setting one-size-fits-all approach and imposing obligations which are too prescriptive, we believe the decision to review the impact assessment should be left to the controller as stated in the GDPR, under a risk-based approach. Controllers should continuously monitor risk, and should be prepared to carry out a new DPIA when risks change. Where risks remain static, however, a DPIA will not contribute to the protection of data subjects' interests.

Paragraph C How to carry out a DPIA?

(see page 13 to 14 of the WP29 guidelines)

Paragraph b) Who is obliged to carry out the DPIA? The data controller, with the DPO and the data processor(s) *(see page 13 of the WP29 guidelines)*

According to Article 35 (9) of GDPR, "*Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing*".

Consequently, given the wording of Article 35 (9), collecting the data subjects' views should not be mandatory. The Guidelines should be aligned with the scope defined by the Level 1 GDPR text, and not go beyond.

This being said, it would be useful to clarify in the final Guidelines that consulting data subjects is **not** appropriate in certain situations. In particular:

- when doing so would compromise the confidentiality of firms' business plans;
- when doing so would be disproportionate or impracticable, such as when contact details are not held, or data subjects are too numerous.

Illustrative practical advices and instructions on this matter should be useful given that, in the Guidelines, the WP29 recommends that the controller should also document its justification for not seeking the views of data subjects, if it decides that this is not appropriate.

Paragraph d) Should the DPIA be published *(see page 17 of the WP29 guidelines)*

As rightly stated by the Guidelines *"publishing a DPIA is not a legal requirement of the GDPR and it is left upon the controller's decision".*

The EBF believes that it should be up to the controller to decide whether the DPIA should be published and in which format.

The Guidelines go beyond the requirements imposed by the GDPR by providing some recommendations encouraging the controllers to publish their DPIA or part of their DPIA or providing recommendations about the content of the DPIA which should be published (for example the published DPIA does not need to contain the whole assessment nor provide a summary of the main findings, especially when the DPIA could present specific information concerning security risks for the data controller or give away trade secrets or commercially sensitive information).

In addition, it is important to stress that the customer is already informed about the data processing by other means.

Such recommendations should be avoided.

For more information contact:

Noémie Papp,
Senior Adviser Digital & Retail

n.papp@ebf.eu
+32 2 508 37 69

About EBF

The European Banking Federation is the voice of the European banking sector, uniting 32 national banking associations in Europe that together represent some 4,500 banks - large and small, wholesale and retail, local and international - employing about 2.1 million people. EBF members represent banks that make available loans to the European economy in excess of €20 trillion and that securely handle more than 300 million payment transactions per day. Launched in 1960, the EBF is committed to creating a single market for financial services in the European Union and to supporting policies that foster economic growth.

www.ebf.eu @EBFeu

For more information contact:

Noémie Papp
Senior Adviser Digital & Retail
n.papp@ebf.eu
+32 2 508 37 69