57.

afme/ Finance for Europe

bba

Article 29 Working Party Guidelines on Data Protection Officers, Lead Authorities & Data Portability – Joint BBA and AFME Response

31 January 2017

Overview

The Association for Financial Markets in Europe[1] and the British Bankers' Association[2] welcome this opportunity to comment on the Guidelines issued by the Article 29 Working Party in relation to: data protection officers, data portability and identification of lead authorities. We have set out our comments below, along with comments on approaches to consultation.

By way of general overview, these Guidelines display a number of positive attributes. In particular, we think that the use of worked examples and 'frequently asked questions' are excellent mechanisms through which to facilitate understanding by stakeholders of how Article 29 Working Party Guidelines will operate in practice.

Having said this, certain sections of the Guidelines could be improved. In particular, the Guidelines are not always calibrated in a way that captures the realities of European businesses operating in *global markets*. This is particularly evident in the provisions on data protection officers – these appear to treat data protection officers as a single person rather than a team – and in the provisions for identification of lead authorities, which potentially result in the existence of multiple lead authorities and in doing so, arguably undermine the One Stop Shop principle.

Similarly, the Guidelines do not always align with practices in the financial services' sector. In particular, whilst the Guidelines on data portability provide useful detail on how this new right is to be implemented, we have identified several areas of uncertainty, and we propose some clarifications. In particular, we note that the success of data portability will require industry-level solutions, given the differences between different sectors.

We note that the Guidelines are not in draft, but we trust that our comments will be helpful in any future enhancements or additions to the FAQs.

1. General approach to consultation and communication with stakeholders

We commend the Article 29 Working Party's recognition of the importance of stakeholder engagement for the purposes of producing sound and workable guidance, in particular through its invitation to stakeholders to provide comments in relation to its recently adopted Guidelines and through the use of its 'Fab Lab' sessions.

Having said the above, we feel that the consultation procedure for these Guidelines could have benefitted from the provision of a more extensive timeframe in which stakeholders could respond to the Article 29 Working Party's output[3] and indeed for *draft Guidelines* to have been the subject of consultation as opposed to Guidelines that have already been adopted. Indeed, this is the norm in the case of analogous European policy advisory bodies – in the

[1] The Association for Financial Markets in Europe (AFME) represents a broad range of European and global participants in the wholesale financial markets. Its members comprise pan-EU and global banks as well as key regional banks and other financial institutions. AFME advocates stable, competitive and sustainable European financial markets, which support economic growth and benefit society. AFME is listed on the EU Transparency Register, under ID number 65110063986-76.

[2] The BBA is the leading trade association for the UK banking sector with 200 member banks headquartered in over 50 countries with operations in 180 jurisdictions worldwide. Eighty per cent of global systemically important banks are members of the BBA. As the representative of the world's largest international banking cluster the BBA is the voice of UK banking. The BBA is listed on the EU Transparency Register, under ID number 5897733662-75.

[3] The Guidelines were issued for consultation on 16.12.16 – over the Christmas period.

field of financial services, for example, ESMA consults on its *draft* technical guidelines whilst also providing stakeholders with longer (though varying) timeframes in which to respond to its consultations.

In the longer term, it would be positive if the Article 29 Working Party, and in due course its successor, the European Data Protection Board, could seek to better reflect established EU norms for stakeholder engagement in relation to policy making. The European Supervisory Bodies in the field of financial services, for example, tend additionally to make use of open hearings and consultative working groups made up of market participants. Given sectoral specificities, we would encourage the establishment of a distinct consultative group comprised of financial services' data protection experts. This group could provide advice and industry insights and act as an appropriate mechanism for consultations. This would be conducive to developing workable and user friendly Guidelines.

2. Guidelines on the right to data portability

General comments

- The Guidelines provide a useful explanation of how to interpret various elements of this new right. However, most of the examples involve customers having at least partial access to datasets relating to them online. Applying this new right in the context of systems that are not connected to the internet poses a greater challenge. Similarly, where data is held in legacy systems it may not be possible to amend these to enable data portability in the manner contemplated by the Guidelines.

Scope, and data in the context of financial services

- The inclusion of 'observed data' under the Guidelines gives a wider scope to this right than expected and may not always be appropriate or simple to implement. We recognise that the Guidelines intend to make a distinction with 'observed data', but identifying data that is 'knowingly provided' may not be straight forward as the controller cannot know the mind of the data subject and this could be disputed. It should be clarified in the guidelines that it is up to the controller to make this determination, in a reasonable manner.

- Also, footnote 12 states that 'all data observed' about a data subject would be in scope such as 'transaction history, access logs, etc.' In the context of financial services, extracting and providing this data, particularly where it is historic, is likely to be very difficult within one month (see also comments on legacy systems).

- There can even be circumstances where it is not legally permissible to provide such observed data to the user. For example, in the context of anti-money laundering this could result in the commission of a "tipping-off" offence.

- More broadly, the distinction between personal data "generated by and collected from the activities" of the user, as opposed to data 'derived' or 'inferred' from the data provided by the data subject may not be clear, and may overlap in practice. These concepts could usefully be further developed. For example, it should be clarified that even if all the personal data was provided directly by the user, there may be circumstances where the totality or the specific selection and display of the provided data within a data set

can provide additional information or context. Providing such a data set in its specific format should be considered to fall under the category of "derived" data and not subject to this new right.

- In addition, while it is helpful that it is made clear that the portability right does not include the disclosure of information covered by trade secrets or intellectual property, this requires further thought. This right may impact upon, for example, database rights, where a large sample of separate data subjects' data may together compromise the intellectual property of the data controller.

- Finally, financial services firms often collect photos and images, for example a scan of a passport provided by a customer for identification purposes. We do not think that such images would be considered to be in 'machine readable format', but this could helpfully be clarified.

Industry solutions

- Given the specifics of each industry, including financial services, we agree that for data portability to ultimately be successful in fully achieving the aims set out in the Guidelines, industry standards will need to be developed. This is a complex task (particularly if standards between different industries are contemplated) involving not just data standards but also technical standards to enable portability. There are important crossovers with competition principles, as well as data protection, so care is needed in this kind of standard setting.

- In the United Kingdom, significant work is underway by a number of financial services firms, government bodies and Fintech businesses to develop 'Open Banking', being a framework through which customers can transfer their current account transaction data from their bank to third party service providers. This is closely related to the requirements under the Revised Payment Services Directive. The Article 29 Working Party might wish to refer to this work in the Guidelines or elsewhere as an example of industry level implementation of a data portability system.

Scope - Personal data under business contracts

- The Guidelines are clear that the right applies where the condition for processing is consent or based on a contract that the individual is party to. However, does this apply in business-to-business environments where a large amount of an individual's personal data may be processed, but they are not 'party' to the contract? This could include for example data relating to company directors processed for AML purposes. Given the wording in Article 6(1)(b), we consider that such personal data is not in scope, but this should be made explicit in the Guidelines. It should similarly be made explicit that this right does not apply in other situations where personal data processing is necessary for the execution of a contract, but to which the data subject is not a party. This can include for example secondary named card holders, or family members who use a product but are not party to the contract.

Security

- It is welcome that the Guidelines recognise the importance of security, which is of particular importance to the financial services sector. It is helpful that section 4 clarifies that strong authentication procedures are needed. Data portability will allow the downloading of potentially vast and sensitive data sets and

companies will have to make sure that the identity of the requester has been positively established to help prevent ID theft, fraud and other misuse of data.

- We do also note, however, that there are risks around how customers use and share their ported data, as noted on page 15 of the Guidelines. It would therefore be useful for data protection authorities to engage in public education on how to use this right securely.

- The Guidelines helpfully state on page 5 that controllers are not responsible for processing by the new controller or the data subject after the data has been ported. It would be useful to repeat at the end of page 15 following the guidance on security that the sending controller is not responsible / liable for breaches caused by the data subject after the data has been received by the data subject or new data controller.

Controller obligations

- The Guidance under section 2 regarding the responsibilities of the transferring and receiving data controllers is helpful. However, certain specific details could be further clarified.

- The Guidelines should acknowledge that while the recipient service provider should certainly aim to only use data as needed, this needs to be done in a proportionate manner. Where large, complex data sets are involved, an assessment on a case by case, data element by data element basis, would create significant administrative burdens and costs. Imposing such a granular approach risks discouraging service providers from accepting ported data.

- Similarly, on page 10, the Guidelines state that controllers (both 'sending' and 'receiving') should build tools to enable data subjects to select / exclude other data subjects' data, but this may not always be practicable. To build on the example of transaction history data used in the Guidelines, it would be difficult for a financial services firm to construct an effective screening mechanism of this kind. Porting this data would often involve very long transaction histories and customers would be unlikely to effectively go through each transaction line to identify potential third party personal data. Similarly, implementing a tool to enable third party data subjects to consent to the porting of their data would often be impracticable. Neither the sending nor the receiving controller would necessarily have a means of contacting the counterparties identified in the transaction history. These kinds of mechanisms would be helpful where they can realistically be built, but the Guidelines should make clear that this is not a requirement and amounts, instead, to best practice that can be implemented when feasible.

- The Guidelines should also acknowledge that in some cases the recipient provider will have to use the data for legal and regulatory purposes. For example, a financial services provider would have to use the data also to detect and prevent money laundering and other financial crimes.

- Building on the above, we note that the receiving controller cannot necessarily decide what data the data subject is going to port. A data subject could even in principle port data to a receiving controller without having any prior relationship in place. In this situation, the receiver might not be able to readily meet its accountability and transparency obligations in respect of data received. The scale of this challenge will depend on the nature of any industry solutions and standards put in place.

- As noted in the Guidelines, Article 20(3) and Recital 68 exclude certain bases for processing from the right to data portability, but footnote 9 on page 7 states that portability would be good practice where processing is based on legitimate interests. However, this will sometimes be inappropriate, for example when processing is to prevent fraud and other financial crime (see also comments above). Therefore, it should be made clear that this is only good practice in situations where portability would be appropriate, given the purposes of the processing.

Further issues

- The Article 29 Working Party should also give consideration in due course to the possibility of 'forced' data portability requests, where companies make the provision of services conditional on the individual exercising his/her right of data portability to extract data from a service (s)he currently uses, and to have that data transferred to the new provider. This could include for example data regarding the data subject's financial transactions, fitness, health activities, etc.

- Under section 5, it should be clarified that if there is no current compatible format for a whole data set, then companies could instead use one or several available formats to achieve the purpose of data portability, to the extent possible.

3. Guidelines on Data Protection Officers

General comments

- A key concern is that aspects of the Guidelines do not always reflect the way in which multinational companies operate within global markets and that they expand the role of the DPO at the expense of their independence. Specifically, our observations in relation to the Guidelines are as follows:

    - While a DPO team is referred to in para. 3.2 of the Guidelines, the Guidelines would, in most instances, appear to proceed on the basis that the DPO is one person. If this is the intention, this is inconsistent with the way in which large multinational organisations operate in practice in global markets given that there is instead likely to be a DPO/CPO team rather than a single DPO.

    - Similarly, in many larger organisations there are various functions that support the overall privacy lead e.g. there may be a privacy legal function, operational functions that deal with data breaches, in-business teams that support subject access requests and cross-border data transfer teams etc. In many companies, there will also be a network of privacy champions/officers who help ensure compliance within a specific department. Indeed, this will be more relevant under the GDPR given the significant list of explicit responsibilities and enhanced documentation and accountability requirements. Given the extensive range of responsibilities it is crucial that the DPO can rely on other stakeholders to support him/her. The Guidelines could therefore better reflect this and allow companies flexibility to develop and implement the most appropriate model for their circumstances. In some organisations, the DPO sets the model or framework for compliance but does not implement activities to achieve compliance (which is done by the operational part of the business). This distinction is important to maintain independence of the DPO who can then enforce

compliance to the framework. In this regard the GDPR suggests that the DPO has more of a monitoring (or second line) role as opposed to an implementing role.

- For the same reason, whilst the DPO should be the contact person to enable breaches to be escalated to the supervisory authority, in most multinational organisations the DPO is not individually involved in remediation and management of each breach and each data protection issue.

- Section 3 (position of the DPO) notes that organisations must ensure that the DPO is involved in all issues relating to data protection at the earliest stage possible, and that the DPO's primary concern should be enabling GDPR compliance of the organisation. This is not the norm in large organisations operating in global markets where guidance has been provided to businesses on day to day matters, and a DPO/CPO team operates. A preferable and alternative approach would be to require businesses to operate in a privacy compliant way that entails the escalation of salient issues and queries to the DPO. Also, the DPO's tasks are primarily to act as a single point of contact internally and externally, manage the data protection risk framework, advise on and monitor compliance to that framework. The GDPR does not imply that the DPO is involved in all data protection issues.

- Similarly, the wording in section 4.4 relating to the DPO and specifically retention of records could, perhaps, be read as providing implicit encouragement for an approach that requires the DPO to retain records of processing activities. Whilst we agree that ensuring *a firm* maintains these records should indeed be part of the DPO's role, retention by a DPO of such records would be problematic for a large multinational company operating in global markets.

- The requirement in section 2.3 that the DPO should communicate with local regulators and customers in their language will be challenging to implement for multinational companies who may well have a presence in each/most Member States as it would entail the installation of DPOs with linguistic skills in each and every one of those locations. This could also undermine the concept of an EU wide DPO for a group of undertakings. The Guidelines could better achieve the desired objective through adopting a more proportionate and practical approach which would enable the group-wide DPO to utilise local colleagues (e.g. local senior management, customer service, local Legal etc.) to facilitate the communication with local supervisors and individuals, or local language services, which is an approach commonly used.

- In short, the DPO needs to support a framework for compliance with the GDPR by the organisation, but the DPO cannot be individually accountable for all the data protection activities of an organisation particularly as many of these are operational in nature.

Proposed Frequently Asked Questions

We would suggest addition of the following question (and corresponding answer): in relation to the necessary skills and expertise of data protection officers, the Guidelines include: 'expertise in national and European data protection laws and practices including an in-depth understanding of the GDPR', could this be achieved through the availability of resources to the DPO through the team they manage who have knowledge of the national laws and practices? Or is it intended that this expertise is possessed by the individual DPO?

4. Guidelines for Identifying a Controller or processor's lead supervisory authority

General comments

- The key general concern is that the Guidelines do not always reflect the reality of European businesses operating in global markets. We have the following specific comments to make:

  - The approaches to assessing the main establishment for groups of companies on pages 5/6 are not fully consistent. On page 5 it is suggested that the main establishment for each individual processing activity should be assessed separately. This is further explained with example 2 on page 6 which uses a group of undertakings scenario. However, in the following section on group of undertakings, it is stated that the undertaking with overall control should be the main establishment. We agree with the latter approach and would suggest that even if there is no clear undertaking / legal entity with overall control, that the overall decision making centre for the group should be the (single) main establishment for the group of companies. Assessing the main establishment for each legal entity/processing activity could undermine the One Stop Shop principle and instead lead to a situation where a group of undertakings has multiple lead establishments or no lead establishment and is consequently required to appoint a number of DPOS in various jurisdictions to allow supervisory authorities to have an entry point into the company. The effect of this would be to make it more difficult for a group of undertakings to have a strong central DPO team with oversight over all aspects of the group and to manage the relationship(s) with the lead supervisory authority/authorities. It would also arguably create inconsistency with Recital 122 of the GDPR.[4]

  - It would also make it more challenging for supervisory authorities to engage with a group of undertakings where a data protection issue spans across several business activities/legal entities. The suggestion that decision making powers are concentrated in a single location for data protection purposes is not realistic or feasible given the many factors that multinational financial services firms and other companies need to take into consideration when determining their locations e.g. fulfilment of regulatory capital requirements, legal restrictions – a branch could not accept liability for a subsidiary, talent, infrastructure, registrations, approvals, etc.

  - We agree with the recommendation on page 7 that groups of undertakings with no central administration in the EU should identify and justify where they determine their main establishment is located. Given that this is still part of the group of undertakings section, it should be clarified that this applies for groups of undertakings, not just to an individual data controller as currently stated (second paragraph on page 7).

  - It is unclear who would be expected to take the lead in the case of complaints, in cases where a supervisory authority may be concerned. This potentially presents problems for customers/data subjects wishing to make complaints as they will be unaware of precisely which supervisory authority

4.'Each supervisory authority should be competent on the territory of its own Member State to exercise the powers and to perform the tasks conferred on it in accordance with this Regulation'.

they should submit complaints to. It will also be problematic for organisations for the purposes of breach reporting.

- Regarding the reference to "supervisory authority concerned", as per para. Iii, p.8, we suggest that there should be a minimal threshold for complaints to be considered by that supervisory authority.

5.Closing comments

We would welcome clarification and resolution by the Article 29 Working Party of the foregoing points to ensure that the Guidelines are as effective as possible and facilitate timely implementation of the General Data Protection Regulation. We would be happy to meet with its Members or its secretariat to discuss these issues in further detail.

Contacts

[redacted]
BBA
[redacted]

[redacted]
AFME
[redacted]