AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Our position

Working Party 29 Draft Guidelines on Personal data breach notification

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate US investment in Europe totalled more than €2 trillion in 2016, directly supports more than 4.5 million jobs in Europe, and generates billions of euros annually in income, trade and research and development.

American Chamber of Commerce to the European Union
Speaking for American business in Europe

Avenue des Arts/Kunstlaan 53, 1000 Brussels, Belgium • **T** +32 2 513 68 92
info@amchameu.eu • amchameu.eu • European Transparency Register: 5265780509-97

Executive Summary

AmCham EU welcomes that guidance on data breach notification is provided by the Article 29 Working Party. While we agree with many of the points, we believe additional clarifications are needed in order to bring the guidelines on Personal data breach notification under Regulation 2016/679 in line with the reality of data breach situations faced by both data processors and controllers. Our recommendations address key aspects of the guidelines with the aim of ensuring a predictable, uniform and proportional application across Europe.

Main points which should be improved in the draft guidelines are:

1. The awareness of a breach by the processor and by the controller is a two-step process and should not be considered to occur concurrently. The point at which a processor and a controller become aware of a breach should be clarified.
2. The guidelines should set out an adequate timeframe for the investigation between the time of "an initial alert" and becoming aware of the personal data breach.
3. The guidelines should clarify that breach notification requirements are not expanded to include availability in situations that do not meet the definition of "personal data breach".
4. The guidelines should provide more concrete examples in order to be effective.

Contents

Key Issues

1. Notification and Awareness (draft guidelines, p. 9-11)

Awareness of a breach by the processor and awareness by the controller are two separate things - they are treated as such by Article 33 paragraphs (1) and (2) respectively - and should not be considered to occur concurrently. Instead, it would be appropriate to only consider a controller 'aware' once the controller has sufficient information to determine with 'a reasonable degree of certainty that a breach has occurred', whether that information comes from the processor or from the controller's own investigation.

The GDPR specifically refers to a notification 'without undue delay' in Article 33(2). The use of the word 'undue' here is crucial and reflects the practical need for an appropriate amount of time to 'take into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject', as provided for under Recital 87 of the GDPR. The interpretation provided in the draft guidelines undermines the intent and practical application of the Regulation.

The controller should not, as the guidelines suggest, be considered aware at the precise moment as the processor is considered aware: controller and processor are distinct parties, as clearly acknowledged in the differing notification timeframes imposed on them under paragraphs (1) and (2) of Article 33 respectively, and the mere fact that a controller 'uses' a processor is an insufficient legal ground to determine joint knowledge. A controller should not be considered to be 'aware' of a breach initiated with the processor until the controller is able to determine with 'a reasonable degree of certainty that a breach has occurred.'

The guidelines should highlight that a phased notification by a processor to a controller would enable the controller to participate in or oversee the processor's initial investigation.

The point at which a controller and processor respectively become aware of a breach should be clarified. It would be appropriate if the point at which a controller is considered to become aware is related to the awareness of the controller's investigating team and should be defined as the point when the investigating team recognizes that the breach impacts the controller's data.

The guidelines accord the controller a short period of time to investigate once informed of a potential breach in order to arrive at a reasonable degree of certainty on whether a breach occurred or not – during that time the controller is not considered to be 'aware'. It should be spelled out when a processor is considered to be 'aware' of a potential data breach.

The guidelines should clarify that the processor is entitled to conduct an initial investigation to establish a reasonable degree of certainty whether an incident has led to personal data being compromised, before either party is considered to be 'aware' of a breach. The guidelines already provide that the controller is not considered to be aware of a breach until it has 'a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised.' The same principles should apply for processors.

A processor may be carrying out processing on behalf of several controllers. When a processor investigates a potential data breach the investigating team needs to first establish which specific controller is impacted. The point at which the investigating team recognizes that the data of a specific controller has been impacted is the point which should be defined as the point when the controller becomes 'aware'.

A processor may not always have sufficient information to determine whether a breach under the GDPR has occurred, and the controller may need to conduct an additional initial investigation of the processor's report before it has the requisite 'reasonable degree of certainty.' The guidelines should therefore also clarify that the controller is not necessarily 'aware' of a breach simply because it has received a report from the processor. Rather, depending on the circumstances of the breach and the quality of the information from the processor, the controller might reasonably decide it does not yet have 'a reasonable degree of certainty' that a breach has occurred and that it needs to conduct its own initial investigation, in addition to the information provided by the processor.

For example, a processor may discover what it suspects is a data breach under the GDPR. However, the processor may not have access to certain key facts relevant to the analysis, such as whether the data in fact pertains to persons within the EU or is otherwise subject to the GDPR (the processor may have little to no visibility into the circumstances under which the data was collected by the controller), whether the data is real data or only test data not pertaining to real people, etc. In such a case, while the processor may consider itself to be 'aware' of a GDPR breach, the controller receiving the processor's report may reasonably decide that some additional investigation is needed before it can determine whether a breach has in fact occurred. The controller should not be considered 'aware' of the breach under the GDPR merely because the processor determined itself to be 'aware' based on the limited facts available to it.

The guidelines should set out an adequate timeframe for the investigation between the time of 'an initial alert' and becoming aware of the personal data breach. The guidelines should also clarify what constitutes an 'initial alert'.

The draft guidelines acknowledge that some level of investigation needs to occur between the time of 'an initial alert' and becoming aware of the personal data breach, at which point the 72 hour timer to notify the supervisory authority begins.

The guidance only gives one concrete timeframe as an example and that is 24 hours. The remaining text refers to terms like 'short' and 'brief', which does not provide actual guidance. This does not necessarily seem like an adequate time to determine what happened. Further, the importance of notifying without undue delay might be emphasized in other ways without unrealistically asserting that all initial investigations of security incidents will be 'short'.

Even in a seemingly obvious case like a lost CD, some time for investigation is necessary to discover the facts necessary to make a determination of 'notifiability'.

The language of the opinion also states in a broad manner that 'it should be clear that there is an obligation on the controller to act on any initial alert and establish whether or not a breach has, in fact, occurred.' It is not clear what would constitute an 'initial alert'. Many systems and technology components have extensive 'alerting' or logging functionalities. Leaving the language as broad as in the draft guidelines may result in companies disabling logging which could run counter to increasing security and data protection. Additionally, raw alerts may not be meaningful by themselves and may need to be correlated with other data to be meaningfully investigated, which may take additional time and significant resources.

We recommend adjusting the examples in line with the above by considering to:

- Update the first example in the box on page 9, by replacing the lost CD with a lost USB key or adding the latter to the example, to align it with current practices.

- Clarify the process in the example in the box on page 10 by inserting the phrase 'and determines that there is likely risk to individuals' at the end of the second sentence, to read: 'The controller conducts a period of investigation, identifies an intrusion into their network and evidence of unauthorised access to personal data, and determines that there is likely risk to individuals'.

- Delete the sentence that makes up the second paragraph at the top of page 10: 'In most cases the preliminary actions should be completed soon after the initial alert –it should take longer than this only in exceptional cases'.

2. The guidelines should clarify that breach notification requirements are not expanded to include availability in situations that do not meet the definition of 'personal data breach' (draft guidelines, p.12)

The guidelines appear to expand breach notification requirements to include availability in situations that should not rise to meet the definition of 'personal data breach'.

The GDPR defines a 'personal data breach' as 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.' [Article 4(12)] It foresees a requirement to provide notice to the regulator [Article 33] upon a certain harm threshold and then an obligation to inform individuals upon a second harm threshold being met [Article 34]. However, the GDPR also requires documenting security breaches even if a harm threshold is not met, Article 33(5) states 'the controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken'.

The guidelines explain that breaches can be considered in three categories, which are respectively breaches of confidentiality, availability and integrity. This is consistent with other information security views. The guidelines acknowledge that availability may be "less obvious". However, they then do not limit breaches of availability that would qualify as a personal data breach to those that would be permanent losses of availability (or otherwise tied to the definition of personal data breach). This becomes most apparent in example iii, which is '[a] brief power outage lasting several minutes at a controller's call centre' and while the guidelines indicate that notification is not required (to either the supervisory authority or the data subjects) they go on to note that this is not a notifiable personal data breach, but still a recordable incident under Article 33(5). It is difficult to understand how a 'brief power outage lasting several minutes' would trigger the definition of personal data breach.

If personal data breach were to include all impacts of availability, this could result in significant and burdensome overhead for reporting and tracking incidents that would not negatively impact the data subjects, such as routine software maintenance.

We recommend to modify language and examples - notably example box on page 7 - to reflect that where a temporary unavailability of data is involved this may constitute a security incident but not an Article 4(12) data breach. We also suggest to modify [example iv] on page 28: In the answer to question of notifying the supervisory authority, change 'potential' to 'likely'. In the answer to the question of notifying the data subjects, change the language to include assessing the likelihood of risk, to read: 'Yes, report to individuals, depending on the likelihood of the lack of availability of the personal data having serious consequences for individuals.'

3. The guidelines should provide more concrete examples in order to serve as effective guidance (draft guidelines, pp. 27-30)

The examples, in many cases, fail to provide additional guidance as they are often qualified with 'if' and 'depends': 'depending on the nature of the personal data' and 'if the risk is not high' [example ii], 'depending on the nature of the personal data affected' [example iv], 'if there is a high risk' [example v], 'if there is likely no high risk' [example vii].

For [example vi] on page 29 we recommend to reference both the likelihood and severity of consequences. The advice on notifying the supervisory authority could read: 'Report to lead supervisory authority, because the cyber-attack indicates intention to harm, thus creating likelihood, and adverse consequences cannot be adequately mitigated.' The advice on notifying to data subjects could read: 'Communicate to data subjects because there is both likelihood and, depending on the specific data involved, severity of consequences. In any case, inform data subjects about changing their account credentials.' The notes could advise on mitigation actions the controller may take.

We recommend that for [Example ii] on page 27 the term 'potential' be deleted and a consideration of the factor of likelihood be added. The advice on notifying the supervisory authority could read: 'Report to competent supervisory authority if adverse consequences to individuals are likely.' The advice on notifying the data subject could read: 'Communicate to individuals if there is a likelihood of severe adverse consequences.' The notes section could also be changed to acknowledge consideration of the likelihood factor.

Additional Comments

4. The guidelines should clarify when the loss or theft of a device may and may not lead to a 'confidentiality breach' (draft guidelines, pages 5-7)

The guidelines state that 'an example of loss of personal data can include where a device containing a copy of a controller's customer database has been lost or stolen. A further example of loss may be where the only copy of a set of personal data has been encrypted by ransomware, or has been encrypted by the controller using a key that is no longer in its possession.'

In addition to discussing the circumstances under which the loss or theft of a device might lead to an 'availability breach', the guidelines should clarify when the loss or theft of a device may and may not lead to a 'confidentiality breach.'

We recommend adding examples of situations where the loss or theft of a device might not be considered a confidentiality breach: where controls exist on the device (for example, strong password protection, full-disk encryption and remote wiping technologies) such that, when taken together with the other circumstances of the incident, the company has no reasonable basis to suspect that the device has been or will be compromised and therefore no reason to suspect 'an unauthorized or accidental disclosure of, or access to, personal data.'

5. The guidelines should clarify when a processor may notify on behalf of the controller/s. The guidelines should also clarify the notification obligations which apply where there is co-controllership or joint controllership of personal data (draft guidelines, page 11)

The guidelines note that the processor could make a notification on behalf of the controller if there are contractual arrangements reflecting this delegation. We recommend the guidelines clarify that any such arrangement must be mutually and explicitly agreed to by the parties.

The guidelines should also clarify co-controllership (and at a lesser extent, joint controllership) and related notification obligations if the breach impacts only one controller. We suggest adding more examples of situations where the processor can notify on behalf of the data controller and further clarify to which extent – in these situations – 'the legal responsibility to notify remains with the controller':

- Company A is a global IT provider serving multiple customers acting as data controllers. If company A experiences a breach affecting personal data collected by its customers it may be better placed to address the breach and to determine whether or not it is required to notify the authorities (and potentially the affected individuals), given its full visibility of the breach.

- Company A and company B share a database with consumers' personal data and act as joint data controllers. If the database is hacked, a notification should be jointly submitted by companies A and B.

The guidelines should add a recommendation that joint controllers should contractually provide for notification responsibilities in the case of a personal data breach affecting a jointly managed system.

In case the same companies act as co-controllers, i.e. do not determine jointly the purpose/s and means of processing personal data, and a breach takes place, a case-by-case assessment should be carried out based on the type of breach and the contractual demarcation of roles and responsibilities.

6. The guidelines should clarify contractual requirements between controllers and processors (draft guidelines, page 11)

The guidelines state that controllers are required to specify how the requirements expressed in Article 33(2) should be met in their contract with their processors. The guidelines should indicate how processing contracts that accompany framework agreements for services might be drafted. A consistent contractual approach will facilitate the conclusion of agreements between controllers and processors and provide clarity on the rights and obligations of both parties. It will equally facilitate any required review of the agreements by supervisory authorities.

We recommend changing the world 'immediate' to 'prompt' in the second sentence of the third paragraph in Section II.A.3 on page 11.

We recommend instead of the second sentence in paragraph 2 of Section II.A.3 on page 11: 'The controller uses the processor to achieve its purposes; therefore, in principle, the controller should be considered as "aware" once the processor has become aware' with a statement of a controller's discretion to contractually prescribe the practices its processors must follow in notifying the controller of a potential personal data breach detected by the processor, with notification of the controller required to occur no later than when a processor has become 'aware' of the breach (i.e., has conducted an initial investigation and found that the may pose a risk to individual rights and freedoms).

7. The guidelines should advise that controllers and processors consider, during the contracting phase, circumstances under which the controller might name the processor and to incorporate these considerations into the relevant contractual terms (draft guidelines, page 12)

The guidelines state that as part of its notification to the supervisory authority, a controller may find it useful to name its processor if the processor is at the root cause of a breach, particularly if this has led to an incident affecting the personal data records of many other controllers that use the same processor. The guidelines should advise that controllers and processors consider, during the contracting phase, circumstances under which the controller might name the processor and to incorporate these considerations into the relevant contractual terms. For example, agreements on advance notice of the controller's intention to name the processor in its notification to a supervisory authority.

8. We suggest adding a number of additional examples of situations that do not trigger notification, particularly where there is no 'high risk' to individuals. The final guidelines should equally make clear that these are examples only, rather than an exhaustive list (draft guidelines, page 15 & Annex)

The guidelines contain numerous examples of situations that require notice to a regulator or individuals. These examples are meant to help determine whether notice is required in different personal data breach scenarios, and to help distinguish between risk and high risk to the rights and freedoms of individuals. However, there is only one example of a situation where it is considered that notice would not be required.

In order to help with the assessment, we suggest adding more examples - while making clear that these are not intended as an exhaustive list of situations that do not trigger notification, particularly where there is no 'high risk' to individuals, such as:

- A sales representative for a company that sells building materials sends an email to 100 contacts, but places their email addresses in the 'cc' field, rendering them visible to all recipients.

9. The guidelines should specify that where the controller (or processor) determines that the incident is 'unlikely to result in a risk to the rights and freedoms of natural persons' and where there is no reason to suspect any change to that risk over time, that there should not be a requirement to re-evaluate risk to data subjects (draft guidelines, page 19)

The guidelines mention that situations where notification may initially not be required - if there is no risk to the rights and freedoms of natural persons - may change over time, requiring re-evaluation of the risk. The guidelines should clarify that the risk to data subjects resulting from a security incident only needs to be re-evaluated where the controller (or processor) has reason to suspect that the degree of risk has changed. Where the controller (or processor) determines that the incident is 'unlikely to result in a risk to the rights and freedoms of natural persons', and where there is no reason to suspect any change to that risk over time, there will be no reason to re-evaluate the risk resulting from the incident.

The guidelines should be in line with the one-stop-shop principle and unequivocally confirm that the obligation of Article 33(1) is deemed as discharged as soon as the lead supervisory authority has been notified.

The sole requirement of the GDPR is for the controller to notify its lead authority, as indicated in the body of the draft. The flowchart in the annex wrongly suggests that the authorities of each jurisdiction impacted by the breach be notified. While nothing prevents the controller from notifying any or several supervisory authorities, the one-stop-shop principle should clearly be recognized in the final guidelines. The guidelines could highlight that a controller that does not have an establishment in the EU may notify the supervisory authority where its representative is located, in addition to the authority where the breach occurred.

We recommend modifying the Flow Chart in Annex A on page 26: In the box in the left column on notifying the supervisory authority, delete the second sentence (on notifying authorities in all Member States) and change the first so that it reads: 'Notify competent supervisory authority(ies)'.

10. The guidelines should clarify how additional actions 'to ensure that the communication is accessible in appropriate alternative formats and relevant languages' can be deployed by the controller (draft guidelines, page 18).

The guidelines accord the controller a short period of time to issue the notification, which naturally constrains a controller's ability to release 24 different versions of the notification in EEA native languages. Also, it is unclear what alternative formats are.

We suggest adding examples that help clarify how requirements concerning language can be reasonably operationalized considering the timeframes, e.g., notifications can be sent in one official language as long as the means to request a translation in native language are available and such translations are provided promptly. Further, we suggest adding examples of alternative formats.