Position Paper

Bitkom views on Article 29 Working Party Draft Guidelines on Personal Data Breach Notification

27/11/2017

Bitkom represents more than 2,500 companies of the digital economy, including 1,700 direct members. Through IT- and communication services only, our members generate a domestic turnover of 190 billion Euros per year, including 50 billion Euros in exports. Members of Bitkom employ more than 2 million people in Germany. Among the members are 1,000 small and medium-sized businesses, over 400 startups and nearly all global players. They offer a wide range of software technologies, IT-services, and telecommunications or internet services, produce hardware and consumer electronics, operate in the sectors of digital media or are in other ways affiliated to the digital economy. 80 percent of the companies' headquarters are located in Germany with an additional 8 percent each in the EU and the USA, as well as 4 percent in other regions. Bitkom supports the digital transformation of the German economy and advocates a broad participation in the digital progression of society. The aim is to establish Germany as globally leading location of the digital economy.

Federal Association
for Information Technology,
Telecommunications and
New Media

Susanne Dehmel
Managing Director
Law and Security
P +49 30 27576 -223
s.dehmel@bitkom.org

Rebekka Weiß, LL.M.
Data Protection &
Consumer Law
P +49 30 27576 -161
r.weiss@bitkom.org

Albrechtstraße 10
10117 Berlin
Germany

President
Achim Berg

CEO
Dr. Bernhard Rohleder

1. Introduction

Bitkom welcomes the opportunity to comment on the Art. 29 Working Group's (WP29) draft opinion on **personal data breach notifications** (WP 251). We believe that more cooperation and exchange between data protection authorities and practitioners is needed to translate the legal text of the GDPR into practice.

In addition to many other provisions of the GDPR, **Art. 33 and 34** must be implemented until May 2018 not only by the digital economy, but also by all other sectors.

The aim of this position paper is to draw attention to difficulties in interpreting and implementing the law. **Chapter 2** addresses general remarks on data breach notifications, whereas **Chapter 3** deals with specific aspects of the draft opinion and comments on concrete statements of the text based on the structure laid down in the WP29 draft guidelines.

2. General Remarks

The Bavarian data protection authority recognized in a short paper on Articles 33 and 34 that the **requirement to report each and every data protection breach could prove to be a major challenge in the day-to-day life of a company**, since it cannot be ruled out that a risk exists in most cases. The authority further states that 'it is therefore expected that supervisory authorities will consult each other in order to clarify the criteria for risk assessment and when notification is required.'[1]

From Bitkom's point of view, a **proportionate interpretation** would be desirable in order to reduce legal uncertainty of companies and to further advance the implementation of the GDPR. A **risk-based approach, which runs systematically throughout the GDPR**, should be applied with regard to breach notifications. In this context, it should be **evaluated in a case-by-case analysis** which risk is tolerable and when the threshold is exceeded. A notification of each and every breach would lead **to a flood of information which would undermine the purpose of the provisions,** namely to raise security in data protection. Last but not least, the **principle of proportionality** needs to be taken into account.

Service disruptions by post: Regarding the notification of data breaches under current data protection law,[2] questions arose with regard to service disruptions by post as the services of some data processors not only include processing of personal data but also printing, putting documents in an envelope, hand it over to postal service providers[3] and document the pick-up. The content of such mail may include highly sensitive data e.g. financial data and pay slips subject to professional secrecy.

Examples:

- Customer informs company that the addressee has not received the mail. Usually the mail is delivered delayed in the following days. In rare cases, the mail will never arrive.
- Customer informs company that the mail arrived damaged/opened.
- Postal service provider informs company that mail has been stolen.
- Customer complains about missing delivery and it turns out that postman dumped the mail.
- Recipient informs company that mail was mistakenly sent to him/her and he/she opened/not opened the mail.
- Recipient informs data processors that mail was mistakenly sent to him/her an opened/not opened it.

With regard to these examples, it should be clarified **whether and under what conditions a personal data breach needs to be notified**. In this context, following questions arise:

- **Does it make sense to notify the supervisory authority** when, for example, the data protection breach occurs at a service provider who is not a data processor and who is already subject to certain regulations?

- **In case a notification is deemed necessary, when does the 72 hour period start?** An investigation by post takes between 4 and 8 weeks, until (in the worst case) it is clear that the item could not be found.

[1] Umgang mit Datenpannen, see https://www.lda.bayern.de/media/baylda_ds-gvo_8_data_breach_notification.pdf.
[2] § 42 a of the Federal Data Protection Act (BDSG).
[3] Postal service providers are generally regulated by German law and are subject to specific confidentiality requirements.

- **In case a notification is deemed necessary, what does the supervisory authority do with the findings?**

In relation to the volume of mail sent by companies, these incidents are rare, but without legal certainty they will lead to considerable effort and documentation. For example, the service provider must inform his client that he/she has received a notification in accordance with Art. 33 but cannot itself influence improvement measures. This is because he/she can only document that the mail has been sufficiently stamped and correctly addressed, but he/she has no other means of influencing the internal processes of a postal service provider.

From Bitkom's perspective:

- **A notification in such cases according to Art. 33 GDPR** does neither help the company, the data subject nor the supervisory authority (that might not have the data protection oversight over the postal company and cannot influence any changes in the event of fundamental shortcomings).

- **A notification in such cases according to Art. 34 GDPR** needs to be evaluated on the basis of whether there are any other data subjects affected, the content of the mail and whether the notification might violate professional secrecy obligations.

Bitkom asks the WP29 for clarification in order to ensure early legal certainty for the parties involved and to avoid a disproportionate amount of documentation. Among other things, it should be clarified that the assignment of postal service providers with postal services does not constitute data processing on behalf of a controller according to Article 28 GDPR.

3. Concrete comments on the text

I. Personal Data Breach Notification under the GDPR

A. Basic Security Considerations

- *'Example: 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.'* p. 5

  Confidentiality Breach: In addition to discussing the circumstances under which the loss or theft of a device might lead to an 'availability breach' **the draft guidelines should evaluate when the loss or theft of a device may or may not lead to a 'confidentiality breach'.**

  In particular, **the guidelines should advise that the loss or theft of a device might not be considered a confidentiality breach where controls exist on the device** (e.g. strong password protection, full-disk encryption and remote wiping technologies) so 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.'

B. What is a personal Data Breach?

- *'The question may be asked whether a temporary loss of availability should be considered as breach and, if so, one which needs to be notified.' p. 7*

  Temporary losses of availability: Temporary losses of availability of data, such as service outages, should not qualify as data breach that needs to be recorded. It is, for example, more common for service unavailability to result from a software issue rather than a data breach. Furthermore, cloud service providers do not have perfect knowledge about how controllers are using their services. This makes it difficult to determine at the time of service unavailability whether that event should be reported as an incident and may result in over-reporting.

II. Article 33 –Notification to the supervisory authority

A. When to notify

2. When does a controller become aware?

- *'WP29 considers that a controller should be regarded as having become 'aware' when that controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised.' p. 9*

  Reasonable degree of certainty by the investigating team: The 72 hour timeline for notification of breaches to the supervisory authority **should not begin until the 'investigating team' of the controller has a reasonable degree of certainty** that a data breach that affects personal data, and is likely to result in a risk to the rights and freedoms of natural persons, has in fact occurred.

3. Processor obligations

- *'Article 33(2) makes it clear that if a processor is used by a controller and the processor becomes aware of a breach of the personal data it is processing on behalf of the controller, it must notify the controller 'without undue delay'. 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****. The obligation on the processor to notify its controller allows the controller to address the breach and to determine whether or not it is required to notify the supervisory authority in accordance with Article 33(1) and the affected individuals in accordance with Article 34(1).'* p. 11

- *'The GDPR does not provide an explicit time limit within which the processor must alert the controller, except that it must do so 'without undue delay'. Therefore, WP29 recommends an* ***immediate notification by the processor to the controller****, with further information about the breach provided in phases as information becomes available. This is*

important in order to help the controller to meet the requirement of notification to the supervisory authority within 72 hours.' p. 11

- **Ascribing processor's awareness to the controller: The controller should not, as the guidelines suggest, be considered 'aware' at the precise moment as the processor is considered 'aware.'** Controllers and processors are distinct parties and the mere fact that a controller works together with a processor is an insufficient legal ground to determine joint knowledge. Instead, the controller should be only considered 'aware' if he/she has received sufficient information from the processor to provide him/her with 'a reasonable degree of certainty that a breach has occurred'.

  The interpretation of the WP29 is also lacking evidence and seems to contradict the intent of the EU legislators which would have certainly referred to such circumstances in the legal text if they wanted the controller's time frame to run from the moment its processor become aware of the breach. Instead, the GDPR drafters have established two different regimes to govern the notification obligations by controllers and processors respectively, with the controller's obligations only being explicitly linked to processor's obligations via Art. 28(3)(f) GDPR which merely requires that the processor 'assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor'.

  Furthermore, this interpretation could also lead to unworkable situations in practice where large processing chains exist. Example: In some supply chains, which could have four of five layers, this will not be a simple exercise and it will take time for the information to reach the data controller. Indeed, Art. 33 (2) is clear that a controller is not aware until they are notified.

- **Immediate notification to the controller:** The draft guidelines also state that notification by the processor to the controller must be 'immediate.' **However, this does not reflect the provisions of the GDPR, which specifically refer to 'without undue delay'.** The use of the word 'undue' is crucial and reflects the practical need for an appropriate amount of time to 'tak[e] 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. The interpretation provided in the draft guidelines undermines the intent and practical application of the Regulation.

  In addition, it is also **not realistic from an operational perspective** as it disregards the need for a processor (or any organization) to gather the facts, prepare the notification, obtain approvals from relevant stakeholders, create the list of recipients, and send the notification. Processors (just like controllers) should be afforded the opportunity to investigate potential data breaches.
  The guidelines should therefore:

  - **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. Taking away the time to properly investigate, could lead to erroneous notifications

which would create unnecessary concerns and undermine public trust in the digital economy. The guidelines already provide that the controller is not considered to be aware of a breach until he/she 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.

- **Recognize that the processor needs a certain time** to gather facts, prepare notification, obtain approvals from relevant stakeholders, etc.

- **Recognize that a processor may not always have sufficient information to determine whether a breach under the GDPR has occurred**, and that the **controller**, depending on the circumstances of the breach and the quality of the information from the processor, **may reasonably decide to conduct an own investigation on top of the processor's report** before he/she has a 'reasonable degree of certainty.'

  For example, if a processor discovers that he/she has accidentally destroyed data appearing to pertain to individuals within the EU, he/she might reasonably suspect that an availability breach has occurred under the GDPR. However, the processor may not have access to certain key facts, such as whether the controller has backups of the data, whether the data in fact affects data subjects within the EU, under which circumstances the data was collected by the controller, etc. In such a case, while the processor may reasonably 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 he/she 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 him/her.

- *'A processor could make a notification on behalf of the controller, if the controller has given the processor the proper authorization and this is part of the contractual arrangements between controller and processor. Such notification must be made in accordance with Article 33 and 34.' p. 11*

  Notification on behalf of the controller: We recommend that the WP29 clarifies that any **such arrangement must be mutually and explicitly agreed to by the parties**, and that the processor can in no way be compelled by the controller to notify the supervisory authority.

- *'As is explained above, **controllers are required to specify how the requirements expressed in Article 33(2) should be met in their contract with their processors**.' p. 11*

  Data processing contracts: To ensure consistency in agreements between controllers and processors, **the guidelines should include an annex with a template of recommended terms/model clauses to be included in the contract** e.g. the type of information to be provided. 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.

- *'Example: As part of its notification to the supervisory authority, **a controller may find it useful to name its processor if it 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.' p. 12*

Name processor in notification breach: 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.

B. Providing Information to the supervisory authority

2) Notification on Phases

The guidance raises the concept of controllers providing phased notifications to the supervisory authority and supplementing later with more complete information. Given the risk that would arise if incomplete information about a data incident is leaked/revealed, **it is recommended that there should be a mechanism through which companies can ask to keep information confidential until the investigations are complete.**

III. Article 34 – Communication to the data subject

A. Informing Individuals
B. Information to be provided
C. Contacting individuals
D. Conditions where notification is not required

- *'It should be borne in mind that while notification may initially not be required if there is no risk to the rights and freedoms of natural persons, this may change over time and the risk would have to be re-evaluated.' p. 16*

Re-evaluation of incidents: It is **not reasonable to expect controllers to re-evaluate the incident for an indefinite duration**. 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. However, **if the WP29 expects an ongoing re-evaluation it should be at least clarified and confirmed which maximum period of time companies would have to adhere to.**

IV Assessing Risk and High Risk
A. Risk as a trigger for notification
B. Factors to consider when assessing risk

V Accountability and Record Keeping

A. Document Breaches

It would be helpful to have guidance on the retention periods of such records. Are controllers and processors expected to keep such records indefinitely, or can records be deleted upon expiration of a certain time limit, as most companies would do in accordance with internal policies?

B. Role of the Data Protection Officer

VI Notification Obligation under other legal instruments

VII Annex Flowchart showing notification requirements

- *'This means that whenever a breach affects the personal data of individuals in more than one Member State and notification is required, the controller will need to notify the lead supervisory authority.' p.15*
- *'If the breach affects individuals in more than one Member State, notify each competent supervisory authority accordingly.' p. 26*

Affected data subjects in more than one Member State: When a data breach affects data subjects in more than one Member State, controllers are only required to notify the lead supervisory authority. The flowchart in the guidance says that each supervisory authority should be notified, but the text of the guidance says otherwise.