November 2017

ETNO comments on Article 29 Data Protection Working Party's Guidelines on Personal data breach notification under Regulation 2016/67

On 3 October 2017, the Article 29 Working Party (WP29) adopted a set of Guidelines on Personal data breach notification under Regulation 2016/67 and invited interested stakeholders to present comments. ETNO welcomes this opportunity to comment on WP29's draft guidelines and would like to stress the importance of legal certainty for individuals and data subjects as well as for organisations.

European telecommunications providers have a long-lasting experience in complying with EU legislation on data breaches, stemming from specific security provisions under Directive 2002/58/EC (ePrivacy Directive, as modified by Directive 2009/136/EC) and the subsequent Regulation 611/2013/EC. Indeed, in 2009 the ePrivacy Directive introduced for the first time some obligations on security and notification of security breaches. The GDPR has extended the scope of the new rules on security to all sectors with the primary aim to have a comprehensive, technologically neutral set of rules on security of processing and data breach notifications. Therefore, we welcome the GDPR in that it attempts to establish a regulatory baseline for all sectors for the handling and notification of personal data breaches across Europe.

The GDPR rules on personal data breach notifications will be all the more crucial for the telecoms sector as the EU co-legislators are updating the ePrivacy Directive into a new ePrivacy Regulation, which seeks alignment with the GDPR. The current proposal repeals the ePrivacy Directive provisions relating to personal data breach notifications, since they are already addressed by the GDPR[1]. A fair, coherent implementation of the GDPR is consequently crucial for ensuring that the personal data of customers of electronic communications services are adequately protected.

For ETNO members is it absolutely necessary to clarify the interplay between GDPR rules and current sector specific rules (ePrivacy Directive and Regulation 611/2013/EC), especially in the transitory period when the GDPR will be applicable, but the future ePrivacy Regulation will not yet be adopted and in force. We do not think that the current ePrivacy Directive and its rules on notification of personal data breaches should be considered *lex specialis* to the GDPR in the same way the ePrivacy Directive was considered *lex specialis* to the former Data Protection Directive 1995/46/EC. It is crucial to ensure legal certainty for e-communications service and network providers, which are currently covered by the ePrivacy Directive and its rules on notification of security breaches, but will also be obliged to comply with the new rules set by GDPR as of 25 May 2018. Having two different set of applicable rules will imply additional complexity for telecom operators and competent authorities.

[1] A remaining provision on security still appears in Art. 17 of the proposed ePrivacy Regulation. ETNO would suggest that also this legacy provision is deleted from the future Regulation as it is questionable whether an additional information obligation related to a security risk is necessary. In addition, the provision in its current form is highly problematic in terms of its practical implementation, as it lacks a clear definition of "particular risk".

Based on telecommunication providers' experience in implementing EU-wide obligations on personal data breach notifications, ETNO would like to provide some comments in order to improve the Article 29 Working Party's draft guidelines and to facilitate a smooth, coherent implementation of the GDPR obligations.

NOTIFICATION TO THE SUPERVISORY AUTHORITY. TIMING OF THE NOTIFICATION

One of the critical issues is to define the timing of the notification and when a controller can be considered to be "aware" of a personal data breach, triggering then its obligation to notify. ETNO would like the WP29 guidance to be more specific on the 72 hour deadline for notification, and more specifically on when the 72 time period starts.

- As regards the data controller, the draft guidance paper states that a controller should be regarded as having become aware of a data breach "when that controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised". ETNO appreciates the acknowledgement that, when a controller is informed about a possible data breach and decides to carry out a preliminary investigation, the controller may not be regarded as being "aware" until this first investigation is completed. As WP 29 recognises, depending on the circumstances of the specific breach, in some cases, it will be relatively clear that there has been a breach, whereas in others, it may take some time to establish if personal data have been compromised. It is equally important to stress that Article 33(1) refers to "without undue delay, where feasible". Therefore, we would suggest that the guidelines further clarify that awareness arises only after it obtains the forensic reports of the alleged breach.

- Regarding the role of the data processor, ETNO is concerned with WP 29's interpretation with regard to the processor's obligation. As per Article 33 GDPR, the data controller is bound by a requirement to notify the supervisory authority "without undue delay", which means "not later than 72 hours". The processor assists the controller in ensuring compliance and has a supporting obligation to notify the controller, also "without undue delay" but with no specific hour marker.

- However, WP29 guideline is suggesting that the controller's 72 hours actually beings when the processor becomes aware of the data breach. This seems impractical: the processor should be bound by a certain time, giving then the controller additional time thereafter. The proposed method could put the controller under considerable time pressure, forcing the controller to blindly accept the processor's determination that a breach has, in fact, occurred and how/where to make notice or risk infringing GDPR (with associated fines up to 10 million Euro or 2% of the total worldwide annual turnover).

- In addition, WP 29 recommends that the processor shall notify immediately. GDPR does not refer to an "immediate notification", on the contrary it makes a difference between controllers' and processors' obligations and while setting an explicit 72-hour time limit for controllers, only refers to a notification without undue delay for processors. A quick reaction of the processor to alert the controller might be welcome so that all actors involved can take the necessary measures, but that should not be at the cost of unrealistic time frames. Even if done as soon as possible in practice breach notification takes time,

especially when data is processed in different environments and processing involves different actors. Requirement of "immediate notification" without any further guidance puts pressure on processors to rush notification and this might result in situation where controller is obliged to act on notification which does not provide sufficient information necessary to fulfil GDPR obligations. This does not lead to greater accountability and stronger protection of rights of data subjects.

Therefore, ETNO urges WP29 to take a more balanced approach as regards the definition of the timing of the notification of any data breach. Putting pressure with unrealistic time frames will not help controllers and processors to handle a breach in an effective manner. Both controllers and processors do not have any interest in delays that might result in significant fines in case of infringement of the rules and in reputational damages.

COMMUNICATION TO THE DATA SUBJECT

ETNO would like to comment on the proposed guidance for contacting individuals, and notably on the suggestion that "communication in the native language of the recipient will help to ensure their understanding of the nature of the breach and steps they can take to protect themselves".

We agree that communication in the native language of the recipient is helpful. Nevertheless, at present it is technically hardly possible to determine the native language of an individual. For example: if an individual, who is not an operator's customer, is affected by a data breach because of his communication with the customer leaks, the operator will not be able to contact that individual in his native language.

Furthermore, the processing of data relating to a subject's native language contravenes the principle of data minimisation as it is not necessary for business needs. The processing of these data would represent an onerous burden on data controllers.

NOTIFICATION OBLIGATIONS UNDER OTHER LEGAL INSTRUMENTS

Besides the GDPR, other EU legislative instruments introduce obligations to notify security breaches:

- current ePrivacy Directive,
- Telecom Framework Directive (Directive 2009/140/EC, currently being reviewed into a new European Electronic Communications Code which will also maintain some specific security obligations and notification requirements),
- NIS Directive (Directive 2016/1148/EC).

The electronic communications service and network providers are thus confronted to multiple legislations with different material and subjective scopes, different obligations, possibility of fines and different competent Authorities. A single incident might trigger various notifications to

various Authorities. This adds complexity und legal uncertainty instead of simplification. Going beyond the remit of these guidelines, it is an issue of utmost importance for ETNO members that legislators and policy makers should take into account to avoid duplication and overlaps.

CONCLUSION

ETNO thanks the Article 29 Working Party for this opportunity to provide comments on these important issue and calls for WP29 to take a balance and pragmatic approach when adopting its final Guidelines on Personal data breach notification.

ETNO calls for legal certainty in the transitory period between the moment when GDPR will be applicable and the moment when the current ePrivacy Directive will be repealed.

ETNO is looking forward to providing additional input in the future in light with the practical application of the GDPR and the new technological developments.

ETNO (European Telecommunications Network Operators' Association) represents Europe's telecommunications network operators and is the principal policy group for European e-communications network operators. ETNO's primary purpose is to promote a positive policy environment allowing the EU telecommunications sector to deliver best quality services to consumers and businesses.

For questions and clarifications regarding this paper, please contact Paolo Grassia, grassia@etno.eu