DIGITALEUROPE

DIGITALEUROPE response to public consultation on Article 29 Data Protection Working Party draft guidelines on personal data breach notification under Regulation 2016/679

Brussels, 24 November 2017

EXECUTIVE SUMMARY

In responding to the public consultation, DIGITALEUROPE seeks to provide feedback on both the legal interpretation of various provisions in the legislation and the practicalities of implementing the guidelines. The main issues we raise are:

- **Temporary losses of availability of personal data by data subjects should not be considered breaches by that measure alone**. In terms of the overarching public policy goal, relevant outages are best served by the incident notification regime under the Network and Information Security (NIS) Directive.
- **Clarification would be welcome that the 72-hour timeline for notification of breaches** to the supervisory authority begins when the *investigating team* of the data controller becomes aware of the breach.
- **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 examples of scenarios where a **delay in notification** could be justified should be expanded.
- **The default authority to which breaches should be notified** for controllers that are established in more than one Member State, or offer services and goods in more than one Member State, **should be their lead authority**, regardless of whether the breach impacts individuals in one Member State or more.
- It is impractical to expect controllers to reassess breaches against compromises of technical protection measures in the future in order to determine whether the breaches are notifiable. Instead, **assessment should be based on information available to the controller at the point in time at which the breach occurs.**
- Responsible competent/supervisory authorities under the various legal instruments that establish notification regimes should **coordinate and refrain from penalising good faith notifications made under one or the other regimes**.

DIGITALEUROPE
Rue de la Science, 14 - 1040 Brussels [Belgium]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Transparency register member for the Commission: 64270747023

INTRODUCTION

DIGITALEUROPE welcomes the opportunity to comment on the draft data breach notification guidelines published by the Article 29 Working Party (WP29). It is essential that the guidance published by the WP29 accurately reflects the scope of the data breach articles in the General Data Protection Regulation (GDPR). DIGITALEUROPE engaged closely in the legislative debate and worked closely with policy makers in shaping the text, giving us insight into the intentions behind specific provisions. Our members include digital companies with significant European presence and European national trade associations, representing large, medium and small companies in the technology sector from across the continent. We have experience with the 60+ mandatory data breach regimes at national and state level around the world.

As such, we would like to provide our feedback on our interpretation of the legal provisions in the GDPR but also our practical experience from existing regimes. For many sections of the guidance, we are comfortable with the interpretation provided by WP29. In the interest of providing focused feedback, however, we have chosen to largely limit our comments to topics where we have concerns or would like additional clarification.

PERSONAL DATA BREACH NOTIFICATION UNDER THE GDPR

1. Types of personal data breach

In terms of the scope of incidents that can be considered to be personal data breaches under the GDPR, we agree with WP29 that breaches that impact personal data confidentiality and integrity should be covered. It also makes sense for a security breach leading to any permanent loss of data to be considered an availability breach. In line with Article 4(12), "accidental or unlawful […] loss […] of […] personal data" should be considered a personal data breach, where it results from a breach of security.

We do not agree, however, that *temporary* losses of *availability*, by themselves, amount to a breach. According to the draft guidance, all such losses of availability are recordable events and, depending on whether they are likely to result in a risk to the rights and freedoms of natural persons, may also be reportable. The WP29 guidance interprets the definition as covering "accidental or unlawful loss of access to […] personal data". The actual definition, however, covers "accidental or unlawful […] loss […] of […] personal data" or "accidental or unlawful […] access to personal data", where caused by a breach of security. The concepts of loss and access are not combined. Crucially, the agent who is accessing data in the definition is not the data subject but an unauthorised third party (hence "accidental or unlawful", and the prior "breach of security"). As such, the definition of "personal data breach" has nothing to do with a loss of access to the data by the data subject, unless this is on a permanent basis (i.e. the data is actually lost, following a security breach).

If the current WP29 guidance on the scope of availability breaches is maintained, there are pragmatic concerns on top of the legal arguments above. It is impractical to record all such incidents where personal data would be unavailable to a data subject. Even more so if there are no thresholds regarding the significance of the loss of availability. Routine database, software or service maintenance would qualify, alongside a host of other mundane activities, including the fairly innocuous example given by WP29 of a customer call centre power outage for a few minutes. It is not efficient to dedicate resources of data protection staff to logging such events in a central register. In addition, where availability is an

DIGITALEUROPE
Rue de la Science, 14 - 1040 Brussels [Belgium]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Transparency register member for the Commission: 64270747023

important part of a service, business customers will generally require service level commitments from suppliers, giving those customers remedies in respect of periods when data is unavailable.

In terms of the overarching public policy goal, we would also suggest that the security incident reporting mechanism under the EU Network and Information Security (NIS) Directive would be more appropriate for recording relevant outages. Over and above the likelihood of double reporting, the NIS Directive is more suited to identifying incidents according to the risks presented. It focuses on higher risk scenarios by covering critical (and digital) services, while including thresholds that determine whether an incident is substantial.

ARTICLE 33 – NOTIFICATION TO THE SUPERVISORY AUTHORITY

1. When to notify

In the WP29 guidance, the point at which the controller is "aware", and hence the point at which the 72-hour clock for notification starts ticking, is when there is a reasonable degree of certainty that a breach has occurred.

It is not explicitly stated whether this awareness correlates to the person in the controller's organisation who first realises that a breach may have occurred through their own rudimentary assessment (e.g. an individual employee who first fields a communication from a customer or researcher claiming that data has been breached) or whether awareness begins once a potential breach has been subjected to an initial assessment by the team responsible for investigating and addressing incidents. It can be inferred from the paragraphs in the text concerning the period of investigation and the internal processes in place to detect and address breaches that awareness begins once the investigation team is aware. We would appreciate it, however, if this was explicitly stated, subject to the incident having been communicated through the appropriate channels in a timely manner.

Under the GDPR, the processor should notify the controller about a breach "without undue delay" after becoming aware of a data breach. Following the processor's notification, once the controller assesses that a breach has likely occurred, it should then within 72 hours (where feasible) notify the supervisory authority. This is a two-step process, and WP29 draft guidance should not conflate the two steps into one. Otherwise, it runs counter to the clear drafting and intent of the GDPR legislators.

Under the draft guidance, where the controller is initially informed of a possible breach *other than* via a data processor, awareness begins when the controller's investigation team believes that a breach has occurred with a reasonable degree of certainty. If the initial information source is a processor, however, under the draft guidance awareness begins before the controller has even been told that an incident may have occurred – i.e., when the processor becomes aware. This is somewhat contradicted by example vii) in the table in the Annex, which indicates that the controller becomes aware once *notified* by the processor. Primacy, however, is likely to be given to the main text of the guidance.

The WP29 guidance treats breaches identified by the processor as inherently different than those from another source. It states that the processor is different because the controller uses the processor to achieve the controller's purposes. It also recommends that the processor notifies the controller immediately, with additional information provided in phases. The issue here is that this approach differs from the letter of the law and is problematic in practical application.

If this were the intent of the policy makers crafting the legislation, and the legislators enacting it, why separate out controller awareness and processor awareness, and the associated timelines for making either the supervisory authority or controller aware, into separate provisions? Why not explicitly state that the controller is deemed to be aware when the processor is aware of a breach?

We understand that the WP29 may be trying to guard against controllers giving themselves additional breathing space for notification by 'outsourcing' breach identification to processors. But to conflate the two steps in the process would fail to take into account:

a) that processors do not themselves have free rein in choosing when to inform controllers as they are still subject to the requirement to notify controllers of breaches "without undue delay".

b) the fact that, if a potential data breach occurs at a processor, the processor's investigating team must first assess which customers may be involved. For example, the processor may see an unusually large set of data being exfiltrated from a data centre to a suspicious range of IP addresses and hence suspect a breach. They may not immediately know, however, which customers may have been affected. Which begs the question as to how "immediate" notification could occur?

c) that it is reasonable for the processor's investigating team to want to have a rough handle on the impact of a specific incident before alarming customers. There is a risk that requiring "immediate" notifications from processors leads to erroneous notifications that unnecessarily create concerns. Additionally, processors should not be required to notify when the breach is solely caused by the controller's (or its end users') negligence (e.g., lost credentials) and not by systems managed by or otherwise controlled by the processor.

d) that the information a processor can provide after it becomes aware of and investigates a breach does not necessarily provide the controller with the information the controller needs to understand the impact of the breach on its own organisation. As such, it does not make sense for their timelines to work in parallel. For example, after investigation, a processor may discover that a network administration account associated with a number of specific data controllers has been infiltrated. They may not be able to tell, however, what further access a malicious individual who hacked the initial account gained in the networks of the different controllers - it may require further investigation by the controllers affected to determine this.

2. Providing information to the supervisory authority

In describing possible delays beyond the 72-hour notification deadline, the WP29 guidance qualifies that this should not be something that regularly takes place. The sole example of justifiable delay given, however, is where notification is more meaningful in a group due to multiple similar confidentiality breaches, with possibly different causes, occurring over a short time period.

While we appreciate the example, we note that delay is even more likely to stem from a complex breach that takes a while to unpack. One example could be a sophisticated attack (Advanced Persistent Threat) where (a) malicious attacker(s) do not stop at the point of initial infiltration but seek to undermine multiple systems or accounts, all the while covering their tracks. It could also stem from a range of other factors: the nature of the initial point of attack; the number and type of different customers involved;

the complexity of the supply chain; or initial uncertainty over the protections in place (and hence whether the breach amounts to a risk to individuals).

3. Breaches affecting individuals in more than one Member State

The draft guidance helpfully clarifies that when a breach affects the personal data of individuals in more than one Member State the controller should notify the lead supervisory authority. We would like to point out that the flowchart in the Annex appears to contradict this position by stating that each competent supervisory authority should be notified if a breach affects individuals in more than one Member State. This should be rectified.

DIGITALEUROPE would further like to make the case that the nature of cross-border processing of data is broader than the given example. The first part of the definition of cross-border processing in Article 4(23) covers processing that takes place in the context of activities in more than one Member State (where the controller or processor is established in more than one Member State). It is reasonable to posit scenarios whereby processing relates to activities in a number of Member States but only data subjects in one Member State are affected. For example, a human resources recruitment tool may be centralised across the region (or globally) but a specific breach may have only related to candidates for a specific job local to one Member State, and hence only impacted data subjects from that Member State.

The same could be true across different types of operations, tools or physical storage infrastructure. In fact, we would argue that it is standard for processing to be cross-border for controllers and processors operating on a cross-border basis, even if a particular incident could be local.

As a result, if the data controller is established in more than one Member State (or is offering goods or services in multiple Member States), their responsibility should be to notify the lead supervisory authority, even if the breach only affects individuals in one Member State. It would thus be the responsibility of the lead supervisory authority to forward the information to authorities in other Member States in a timely fashion.

An advantage of presuming notification to the lead supervisory authority is that it would speed up notification, by not requiring controllers to have to identify the right contact points in various data protection authorities. It would also take advantage of the relationship already established between the lead authority and the controller – giving the lead authority a better grasp of the technical and organisational set-up of the controller for subsequent investigation or recommendations.

4. Conditions where notification is not required

As the guidance reiterates, notification is not required to the supervisory authority (but a breach should nonetheless be recorded) where it is unlikely to result in a risk to the rights and freedoms of individuals. We welcome the examples given of publicly available information and encrypted/unintelligible data. The conditions attached to the latter example also seem appropriate: that confidentiality of the key or other protection mechanism remains intact, there is an adequate back-up and availability is restored in a reasonable timeframe.

While we understand the reasoning behind the additional qualification that notification could still be required in the future if the technical protection measure was no longer adequate, DIGITALEUROPE questions whether this is a feasible requirement in practice. The example given is the subsequent exposure of a vulnerability in the encryption software. While controllers will be tasked with keeping records of breaches, it is unrealistic to expect them to cross-check this record every time any one of tens of thousands of vendors discloses a vulnerability - especially as the vulnerability might correlate not only to current vendors but also to legacy ones who may previously have been used.

Indeed, the information that controllers are expected to keep in the internal register of breaches would not be sufficient to do such a cross-check or make a notification. It would need to include the precise details of the versions of the software and hardware used to protect both the data and the multiple systems that data may have touched. Moreover, in order to facilitate possible communication to the data subjects, it would require contact details for data subjects potentially affected by breaches initially classified as low risk to be maintained long after they may have ceased to have an active relationship with the data controller.

A more appropriate recommendation would be for the application of technical protection measures to be considered to reduce the risk to individuals only where, according to the best knowledge available to the controller, such measures are not compromised at that point in time.

NOTIFICATION OBLIGATIONS UNDER OTHER LEGAL INSTRUMENTS

As the WP29 draft guidance recognises, the same incident may result in the need to notify multiple authorities under different legal instruments. Above and beyond the NIS Directive, Citizens' Rights Directive and eIDAS Regulation, controllers may also have to notify incidents under sectoral legislation, like the Payment Services Directive 2.

As a result, we would like to see guidance on such notification requirements reflect the existence of the other legal instruments and avoid double notification to the extent possible. We also call on the various competent/supervisory authorities involved to coordinate among themselves to better understand the equivalent instruments and to forward incidents as appropriate (subject to appropriate application of data protection law). We call on them to avoid penalising entities who notify an incident through one or the other of the mechanisms in good faith but fail to re-notify through other instruments.

--

For more information please contact:
Iva Tasheva, DIGITALEUROPE's Policy Manager
+32 493 40 56 12 or iva.tasheva@digitaleurope.org

DIGITALEUROPE

ABOUT DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE's members include in total 25,000 ICT Companies in Europe represented by 61 corporate members and 37 national trade associations from across Europe. Our website provides further information on our recent news and activities: http://www.digitaleurope.org

DIGITALEUROPE MEMBERSHIP

Corporate Members

Adobe, Airbus, Amazon, AMD, Apple, BlackBerry, Bose, Brother, CA Technologies, Canon, Cisco, Dell, Dropbox, Epson, Ericsson, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, HP Inc., Huawei, IBM, Intel, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Panasonic Europe, Philips, Pioneer, Qualcomm, Ricoh Europe PLC, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Sony, Swatch Group, Tata Consultancy Services, Technicolor, Texas Instruments, Toshiba, TP Vision, VMware, Western Digital, Xerox, Zebra Technologies.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Bulgaria: BAIT
Cyprus: CITEA
Denmark: DI Digital, IT-BRANCHEN
Estonia: ITL
Finland: TIF
France: AFNUM, Force Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: TECHNOLOGY IRELAND
Italy: ANITEC-ASSINFORM
Lithuania: INFOBALT
Netherlands: Nederland ICT, FIAR
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS, APDETIC
Slovakia: ITAS
Slovenia: GZS
Spain: AMETIC
Sweden: Foreningen Teknikföretagen i Sverige, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT UKRAINE
United Kingdom: techUK

DIGITALEUROPE
Rue de la Science, 14 - 1040 Brussels [Belgium]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Transparency register member for the Commission: 64270747023