DIGITALEUROPE

2 MARCH 2021

Response to draft EDPB Guidelines on examples regarding data breach notification

Executive summary

DIGITALEUROPE is pleased to provide its comments on the European Data Protection Board's (EDPB) draft Guidelines on examples regarding data breach notification. The draft Guidelines provide timely guidance that will help data controllers in handling data breaches and conducting risk assessments.

In our response, we put forward the following recommendations for EDPB consideration:

- **Proportionality and an acknowledgement that this is a developing area of law.** Data breaches can present unprecedented questions and challenges, and this is a fast-flowing area of law. The draft Guidelines emphasise that data controllers should act in a reasonable and proportionate manner as relevant under each specific circumstance.
- **Further practical guidance and case studies.** We recommend that the final Guidelines include additional case studies, which could focus on decentralised, multistakeholder models and scenarios that include multiple data controllers and processors.
- **Notification thresholds.** It is important to ensure that the final Guidelines set out clear notification thresholds.
- **Action by supervisory authorities.** There is currently substantial divergence between interventions by various supervisory authorities, with many often contacting data controllers on behalf of data subjects for incidents which are not notifiable in the first place. We recommend that the final Guidelines address this divergence.

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

Table of contents

Proportionality and an acknowledgement this is a developing area of law

It is important to note that data breach notification and reporting requirements are still a relatively new area of law and that the landscape is constantly evolving. This evolution is due to multiple factors, notably the emergence of, and complexities created by, new technologies and services and the fact that malicious actors are themselves evolving in their breaching capabilities. The final Guidelines could better recognise the realities faced by data controllers, and ultimately better align to the GDPR principles of reasonableness and proportionality when mitigating the effects of a data breach.

The draft Guidelines state that a supervisory authority 'can use its corrective powers and may resolve to sanctions if a data controller self-assesses the risks [associated with a data breach] to be unlikely, but it turns out that the risk materialises.'[1] However, if a data controller correctly assessed the risks for data subjects as being unlikely, it would have fulfilled its obligation under Art. 33 GDPR even where those risks later materialise.

In practice, many organisations make these self-assessments on a regular basis and have invested in carefully developed protocols to triage decision-making. These organisations take the decision as to whether to notify on the basis of information available to them at the time. If the suggestion is that these contemporaneous risk assessments will be reviewed with the benefit of hindsight, this will result in many more notifications where the risks to data subjects are remote.

The need for a more proportionate and flexible approach is also evident in the draft Guidelines' description of security measures.[2] The description of security measures within the draft Guidelines does not reflect the GDPR, which requires data controllers to implement 'appropriate' technical and organisational security measures, taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing. Under the GDPR, then, appropriate technical and organisational security will not completely extinguish all vulnerabilities in a system – and breaches will not always be indicative of a system weakness, nor should they lead to systematic enforcement, most of all for those controllers and processors acting with full accountability.

[1] See p. 10 of the draft Guidelines.

[2] See para. 8 ibid.: 'data breaches are problems in and of themselves, but they are also symptoms of a vulnerable, possibly outdated data security regime, [and] thus indicate system weaknesses to be addressed.'

Further practical content and case studies

The draft Guidelines provide a series of case studies which focus on the differing approaches data controllers may take addressing various data breach situations. Further practical guidance would be welcome in particular with regard to when data controller become 'aware' of a breach, for example the reasonable expectation of a practical delay between the first time an employee within the data controller becomes aware and a 'person in charge' of data protection is made aware. In most situations organisations are unlikely to know immediately whether or not a breach or incident has resulted in a compromise of personal data.

It would also be interesting to clarify how, following the point of awareness, controllers can balance the obligation to notify data breaches within certain timeframes with the obligation to carry out proper diligence and what constitutes reasonable and proportionate remedial actions. A summary of 'study cases' on more complex scenarios, involving multiple stakeholders, would also help controllers and processors.

The draft Guidelines explore the complexities of the chronology of an investigation. However, they do not properly acknowledge the detailed forensic analysis that is often required before a data controller can make risk assessments in practice.[3] Significant forensic examination is often a pre-requisite to determining seriousness, which is particularly required for complex scenarios. These investigations may take several weeks before facts and comprehensive conclusions can be provided. DIGITALEUROPE would welcome some additional case studies that explore notification timelines taking into consideration such complex investigative processes.

In addition, case studies that provide more context with regard to situations where a data controller can both end data breach investigations and begin to draw conclusions. For example, one of the case studies provided in the draft Guidelines indicates that a data controller must mitigate all potential and theoretical risks, going against the GDPR provisions.[4] Investigations cannot

[3] See para. 9 ibid.: 'controllers should make this assessment at the time they become aware of the breach … [and] not wait for a detailed forensic examination.'

[4] See case study 2: 'even after a thorough investigation that determined that the personal data was not exfiltrated by the attacker… the likelihood of a confidentiality breach cannot be entirely dismissed.' Meanwhile case study 1 states that an internal investigation…determined with certainty that the perpetrator only encrypted data, without exfiltrating it, but goes on to say that the data controller should evaluate the potential risk of exfiltration without leaving a trace in the logs of the systems.

continue assessing indefinitely and data controllers must eventually draw conclusions and make decisions with a 'reasonable degree of certainty.'[5]

Finally, further insight and case studies that highlight the complexities of supply chains and operating models that comprise of multiple data controllers would be welcome. The case studies included in the draft Guidelines are geared towards more simplistic models of data breaches. Additional case studies should explore the responsibilities and risk allocation in scenarios where multiple stakeholders (including separate data controllers, joint data controllers and data processors) are involved.

Notification thresholds

Within the draft Guidelines, several case studies appear to set a very low threshold for breach notification. This is concerning given the potentially significant financial and administrative burden placed on organisations when investigating incidents, taking into consideration that the number of basic threats and potential breaches is significantly increasing.[6]

The draft Guidelines describe a notifiable scenario in which the personal data of one data subject was incorrectly included in a letter sent to another data subject.[7] If this mailing error was repeated and therefore possibly symptomatic of a wider problem, notifying the supervisory authority would be a reasonable expectation. However, given the non-sensitive nature of the personal data in question, as well as the non-malicious identity of the unintended recipient, it seems more appropriate to create an internal record and notify the supervisory authority only if it becomes apparent that the breach is evidence of something more systematic.

If the threshold for notification is set too low, resources which could otherwise be spent on augmenting internal compliance processes and better protecting data subjects might be misdirected. In addition, an overly inclusive approach to notification could have negative consequences for data subjects, who may struggle to distinguish between real risks and minor/theoretical risks amongst a plethora of notifications.

It must also be considered that if the threshold for notification is set too low, supervisory authorities would be overburdened with a plethora of reports. In addition, obliging organisations to notify users of low-risk incidents could

[5] See pp. 10-11 of the Article 29 Working Party Guidelines on personal data breach notification under Regulation 2016/679, adopted 6 February 2018.

[6] See ENISA'S 2020 Threat Landscape report, available at https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/etl-review-folder/etl-2020-main-incidents.

[7] See case study 16 in the draft Guidelines.

ultimately lead to notification fatigue, resulting in users ignoring notifications altogether.

DIGITALEUROPE recommends that the final Guidelines include additional examples that describe incidents where data breaches have resulted in the inadvertent disclosure of personal data to a third party, but are nevertheless not notifiable to the supervisory authority.

Action by supervisory authorities

Various organisations are finding that supervisory authorities are routinely contacting them in relation to data subject complaints which fall beneath the notification thresholds set out in the GDPR. Many supervisory authorities appear to follow up with data controllers on every single incident reported to them by individuals. It might be helpful for interested parties and EU data protection authorities to agree on some common and standard understanding of how to keep triaging and assessing incident seriousness before determining whether it is appropriate to contact the organisation in question.

DIGITALEUROPE recommends that the final Guidelines should separately frame those incidents which supervisory authorities will pursue on behalf of individuals and those incidents it will conclude directly with complainants. This will enable data controllers to focus more attention on high-risk events.

Finally, although the draft Guidelines are designed to be more targeted towards data controllers and processors, it would be equally important to ensure that all supervisory authorities are aligned on thresholds and enforcement. In particular with the varied reporting platforms and methods, as each Member State has a different approach and venue upon which controllers and processors must utilise in order to report breaches.

FOR MORE INFORMATION, PLEASE CONTACT:

Alberto Di Felice
Director for Infrastructure, Privacy and Security
alberto.difelice@digitaleurope.org / +32 471 99 34 25

Martin Bell
Privacy and Security Policy Officer
martin.bell@digitaleurope.org / +32 492 58 12 80

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 Membership

Corporate Members

Accenture, Airbus, Amazon, AMD, Apple, Arçelik, Autodesk, Bayer, Bidao, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, DATEV, Dell, Dropbox, Eli Lilly and Company, Epson, Ericsson, Facebook, Fujitsu, GlaxoSmithKline, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, NetApp, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Pioneer, Qualcomm, Red Hat, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sony, Swatch Group, Technicolor, Texas Instruments, Toshiba, TP Vision, UnitedHealth Group, Visa, VMware, Workday, Xerox.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv
Estonia: ITL
Finland: TIF
France: AFNUM, SECIMAVI, Syntec Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: INFOBALT
Luxembourg: APSI
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS
Slovakia: ITAS
Slovenia: ICT Association of Slovenia at CCIS
Spain: AMETIC
Sweden: Teknikföretagen, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
United Kingdom: techUK