1 December 2017

Comments by the Centre for Information Policy Leadership
On the Article 29 Working Party's
"Guidelines on personal data breach notification under Regulation 2016/679"
Adopted on 3 October 2017

Introduction

The Article 29 Working Party (hereinafter WP) released its proposed "Guidelines on Personal data breach notification under Regulation 2016/679" (Guidelines) on 3 October 2017. The WP invited public comment on the Guidelines until 28 November 2017.[1] The Center for Information Policy Leadership (CIPL) welcomes the opportunity to submit our comments to the WP.[2]

CIPL appreciates the clarification of many critical issues offered in the Guidelines. The WP seems to have drawn lessons from the experiences of other jurisdictions where breach notification has been a longstanding requirement. On the critical issue of the timing of notification, the discussion of when a controller can be considered to be "aware" of a personal data breach contains much helpful material. The recognition of the need in some factual situations for allowing a "phased notification" of the supervisory authority is appreciated. The inclusion of the flow chart and of example breaches to elucidate the risk assessment process is also helpful.

On the following pages, CIPL offers comments and recommendations for improving the WP's Breach Notification Guidelines, on the following issues.

1. Availability Breaches
2. Risk Assessment (Terminology, Level of Risk, Reassessing Risk)

---

[1] An extension was granted for this submission until 5 December 2017.

[2] CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton & Williams LLP and is financially supported by the law firm and 56 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton & Williams.

3. Criteria to Consider in Assessing Breach Risk (Number Affected, Special Categories)
4. Timing of Notification (Awareness, Law Enforcement Delay)
5. Controller-Processor Responsibilities
6. Supervisory Authority to Notify
7. Methods of Communication to Individuals

Comments and Recommendations

1. Availability Breaches

In Section I.B on page 6, the WP quotes the GDPR's definition of a personal data breach:

> 'personal data breach' means 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))

The WP goes on to cite its pre-GDPR Opinion 03/2014 on Personal Data Breach Notification, in which data breaches are categorised according to the well-known information security triad of confidentiality, integrity and availability. According to that Opinion, a "confidentiality breach" is one that results in accidental or unauthorised disclosure of or access to personal data and an "integrity breach" is one that involves accidental or unauthorised alteration of the data; both would meet the definition in Article 4(12). The Opinion's definition of an "availability breach", which is proposed in the Guidelines, does not clearly fit the definition of a personal data breach in Article 4(12). The WP's definition of an availability breach includes the result of a *loss of access to* personal data, whereas Article 4 refers to *unauthorised access to* personal data as constituting a data breach. (The loss or destruction of data, on the other hand, meets both the WP's definition of an availability breach and Article 4's definition of a personal data breach.)

Some of the examples of "availability breaches" in the Guidelines reveal the inconsistency between the WP's proposed approach and the definition of "personal data breach" in Article 4(12). A security incident such as a ransomware attack, for example, would fit the definition only if the personal data were considered destroyed or lost. The WP seems to acknowledge this, stating at the bottom of page 6: "A breach will always be regarded as an availability breach when there has been a permanent loss of, or destruction of, personal data". If a controller has a backup of data encrypted in a ransomware attack, then the data cannot be considered permanently lost or destroyed.

The temporary unavailability of personal data, while it might indeed be a security incident that is inconvenient and puts individual rights and freedoms at risk, would not *per se* constitute a personal data breach. Of course, a controller suffering a ransomware attack that renders personal data only temporarily unavailable to the data subjects would not be exempt from any liability, under Article 32 for example, and such a controller would have to take actions to mitigate the impact. But the security incident would not qualify as a personal data breach under GDPR and thus would not be subject to Articles 33 and 34 obligations (i.e. it would not require notification or recording as a personal data breach). If, on the other hand, a ransomware incident were found to also compromise the confidentiality or integrity of personal data, then it would qualify as a personal data breach, subject to Articles 33 and 34.

Recommendations on "Availability Breaches"

- Modify the description of an availability breach in Section I.B.2 on page 6 to read "Availability breach – where there is an accidental or unlawful loss or destruction of personal data", which is consistent with the definition in Article 4(12).
- Delete "temporarily" and "power failure or" from the second paragraph in the example box at the top of page 7, to read: "A loss of availability may also occur where there has been significant disruption to the normal service of an organisation, for example, experiencing a denial of service attack, if it renders personal data permanently unavailable".
- In the second paragraph following the first example box on page 7, modify the next-to-last sentence to read: "If the lack of availability of personal data is permanent or long term and is likely to result in a risk to the rights and freedoms of natural persons, then the controller will need to notify the supervisory authority".
- Modify the examples in the second example box on page 7 to reflect that they both involve the temporary unavailability of data, which would constitute a security incident but not an Article 4(12) data breach.
- Either delete Example Breach iii on page 27 or modify the recommendation to read: "While this would constitute a security incident, it is not an Article 4(12) personal data breach subject to Articles 33 and 34. This is, however, without prejudice to the supervisory authority's power to investigate a possible violation of Article 32 security requirements".
- Modify Example Breach 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".

- Modify Example Breach viii on page 29, to respond "no" to both questions about notification and to read in the recommendations section: "While this would constitute a security incident, it is not an Article 4(12) personal data breach and is therefore not subject to Articles 33 and 34. This is, however, without prejudice to the supervisory authority's power to investigate a possible violation of Article 32 security requirements".

2. Risk Assessment

2.1. Terminology

In the first sentence of the Introduction section, on page 4, the WP says it will use the term "breach" to mean "personal data breach". Then in Section I.B.1 on page 6, after quoting the definition in Article 4(12), the Guidelines point out that a breach is a type of security incident and that the GDPR only applies where there is a breach of personal data. It would be helpful if the WP continued and made the distinction between a personal data breach per Article 4(12) and a "notifiable" personal data breach, per Article 33 or Article 34.

Recommendation on Risk Assessment Terminology The Guidelines might introduce a term such as a "notifiable breach" to describe a personal data breach that meets Article 33's standard of likelihood of resulting in risk to the rights and freedoms of natural persons or Article 34's higher standard of high risk. In the flow chart in Annex A, a notifiable breach would be one in which the answer is "yes" to the question in either of the two diamonds in the left column. Using such a term could help clarify the discussion and examples in the Guidelines.

2.2. Level of Risk

The GDPR takes a risk-based approach to data protection, requiring organisations to assess the risks that their data processing activities may pose to individual rights and freedoms and to manage and mitigate such risks with technological and organisational measures. The data breach notification provisions in Articles 33 and 34 rely heavily on risk assessment and in particular on the determination of the level of risk that triggers notification in specific breach situations. The Guidelines offer many examples and elucidations that are helpful to controllers and processors in making such determinations, but some of the discussion is unclear or seems inconsistent with the GDPR.

The GDPR draws on generally accepted principles of risk management, including the description of risk level as the combination of consequences and their likelihood.[3] In Article 32, Security of processing, controllers and processors are required to take into account, among other things, "the risk of varying likelihood and severity" to the rights and freedoms of individuals and to secure personal data using measures appropriate to the risk to mitigate it. Article 32 references Recital 76 on risk assessment, which also describes the process as determining the likelihood and severity of risks to establish the level of risk posed in particular fact situations.

The WP devotes considerable space to risk and risk assessment in these Guidelines. In the discussion related to Article 33, Notification to the supervisory authority, the Guidelines provide examples of particular breaches where notification to the supervisory authority would not be required because the breaches are "unlikely" to result in a risk to individual rights and freedoms (Section II.D, pp.15-16). One example is a confidentiality breach of personal data that are already publicly available. Another example is a confidentiality breach of personal data that are properly encrypted. In both examples, the incidents described would seem to meet the definition of a personal data breach in Article 4(12), in that they led to an unauthorised disclosure of personal data. Yet neither would be likely to put the data subjects' rights at risk, in the first case because the data were already publicly disclosed and in the second because encryption rendered the data inaccessible. Thus, according to Article 33, notification to the supervisory authority would not be required. Nor, necessarily, would notification of data subjects be required.

In its discussion of assessing risk and high risk in Section IV, the WP stresses the need to consider both risk factors, the *severity* of the potential impact of the abuse of breached data and the *likelihood* of such impact occurring:

> Therefore, when assessing the risk that is likely to result from a breach, the controller should consider a combination of the *severity* of the potential impact on the rights and freedoms of individuals and the *likelihood* of these occurring. Clearly, where the consequences of a breach are more severe, the risk is higher and similarly where the likelihood of these occurring is greater, the risk is also heightened. If in doubt, the controller should err on the side of caution and notify. Annex B provides some useful examples of different types of breaches involving risk or high risk to individuals. (Section IV, B, p. 22; *emphasis added*.)

[3] ISO 31000:2009, sec. 2.24, available at https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en.

Some of the breach examples in Annex B, however, do not seem to follow this approach.

Example Breach ii (Likelihood)

In Example ii on page 27, a breach in which a cyberattack on a website resulted in personal data being exfiltrated, the WP recommends notifying the supervisory authority "if there are *potential* consequences to individuals". The criterion here should be if (adverse) consequences to individuals are *likely,* not merely *potential.* Similarly the answer provided to the question on whether to notify individuals is "yes", "depending on the nature of the personal data affected and if the severity of the potential consequences to individuals is high". This analysis ignores likelihood entirely and considers only the severity of consequences. The notes section does not clarify matters, advising notifying the data subject even "if the risk is not high", and offering as a rationale for making such a decision the sensitivity of the data alone. This is not what GDPR requires and could result in causing unnecessary anxiety for individuals by notifying them of breaches posing a low or no risk of adverse consequences.[4]

Recommendation on Example Breach ii

Modify breach Example ii, to eliminate the term "potential" and add a consideration of the factor of likelihood. 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.

Example Breach vi (Likelihood and Severity)

Breach Example vi on page 29 is a confidentiality breach resulting from a cyberattack on a multinational retail website in which usernames, passwords and purchase history are published online. The advice provided is to notify the lead supervisory authority if the breach involves cross-border processing, and to notify data subjects because the breach could lead to high risk. Neither recommendation includes any reference to either the likelihood or the severity of consequences for data subjects that might result. As rightly urged in the notes section, this is the type of breach in which the likelihood of adverse impact could be mitigated at least in part. The controller could force password resets, protecting the accounts of data subjects from subsequent unauthorised access to the affected account, although this would not address the

[4] The WP expresses a concern about protecting individuals from "notification fatigue" on page 17 of the Guidelines.

possible harms from the disclosure of the data before such action was taken, from unauthorised access to other accounts where the individual used the same credentials or from abuse of the purchase transaction data.

Recommendation on Example Breach vi
Modify breach Example vi, to reference both the likelihood and severity of consequences. The advice on notifying the supervisory authority could read: "Report to lead supervisory authority, because cyberattack 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".

Bug Bounty Programs and Security Research
Many companies sponsor security programs in which they pay cash awards to security researchers for reporting vulnerabilities ("bugs"). Responsibly run bug bounty programs, where companies put constraints on and explicitly prohibit researchers from attempting to access someone else's data or compromise third-party data, would be unlikely to result in a risk to data subjects.

2.3. Reassessing Risk
In the discussion on page 16 of situations in which notification is not required, the WP gives an example of a confidentiality breach involving properly encrypted personal data, thus unlikely to pose a risk to the rights and freedoms of individuals. The Guidelines go on, however, to say that the risk and the possibility of notification would have to be re-assessed if future technological developments render the encryption vulnerable. It is impractical to expect controllers to reassess past breaches continuously as tens of thousands of technology vendors disclose vulnerabilities. Unless there is a drastic change or a breakthrough in encryption technology immediately following the breach, or within a short time period (say three to four months), organisations should assume that a breach involving encrypted data, hardware, files or communications will remain encrypted.

The problem is reflected in the recommendation in Example Breach i on page 27, which concerns a stolen CD containing encrypted personal data, and advises that the breach may not be reportable if the encryption is state of the art, the key is not compromised and backups

exist. It then continues to say that notification is required "if it [the breached data] is later compromised".

Recommendations on Reassessing Risk

- Revise the discussion on page 16 to eliminate the notion that controllers should continuously reassess the risk posed by a past data breach in light of future technological developments long after the breach occurred. Such a reassessment need only be undertaken if a major breakthrough that could render the data accessible occurs immediately following or within a short time period after the breach.
- Modify Example Breach i on page 27, to delete the last sentence in the recommendations column regarding a future compromise, or change the sentence to read: "If a major development in encryption that could render the data accessible occurs immediately following or within a short time after the breach, reassess the need to notify".

3. Criteria to Consider in Assessing Breach Risk

3.1. Number of Individuals Affected

The Guidelines include the number of individuals affected among the factors to be considered in assessing risk (Section IV.B, p. 22): "Generally, the higher the number of individuals affected, the greater the impact of [sic] a breach can have". Guidelines go on to acknowledge that "a breach can have a severe impact on even one individual, depending on the nature and context of the personal data that have been compromised". A large number of data subjects affected may indeed pose a greater risk to the controller, of reputational or financial harm, for example. But a breach affecting a large number of individuals should not, by that fact alone, be assumed to pose a likely risk to those individuals' rights and freedoms.

Breach Example ix (Number Affected)

In two of the example breaches, the advice is based to some extent on the number of individuals affected. In Breach Example ix, personal data of 5,000 students are mistakenly sent to the wrong mailing list with over 1,000 recipients (p. 30). The advice on notifying the supervisory authority is simply to notify, without mentioning assessing whether the nature of the data or other contextual factors suggest a likely risk to the data subjects. The advice on notifying the data subject does mention considering the type of personal data involved and the severity of consequences; it also mentions the "scope" of the breach as a factor.

Breach Example x (Number Affected)

In Breach Example x, in which a marketing email exposed the email addresses of all recipients to each other, the advice also cites "a large number of individuals" affected as one of the criteria for notifying the supervisory authority, without, however, mentioning assessing the likelihood of the risk to individuals (p. 30).

Administrative Notification Threshold

In order to manage the number of notifications that supervisory authorities receive and to enable them to deal effectively with those reported, the WP may wish to consider using a threshold of breach size for internal administrative purposes or even for requiring prompt notification to the authority by organisations. Thus, we encourage the WP to (a) consider advising supervisory authorities to use a threshold of number of individuals affected, say between 250 and 500, to help prioritise their efforts, and (b) consider setting a number-affected threshold for notifying supervisory authorities; in such a case the threshold would not apply if a breach would result in a high risk to individuals. Organisations will still have a duty to document *any* personal data breach as envisaged in GDPR Article 33(5), which may be reviewed by the supervisory authorities. The threshold should be consistently applied by all supervisory authorities.

Breach laws in other jurisdictions often set a size threshold for notification of a regulator.[5] The threshold in the various laws ranges from 250 to 1,000 individuals affected. The US state of Massachusetts, for example, which requires notification of the attorney general for breaches of any size, received reports of 3,278 data breaches in 2015. California, with a population nearly six times that of Massachusetts but where notification of the attorney general is required only for breaches affecting more than 500 residents, received reports of 178 data breaches in the same period.[6] (The laws in all US states require notifying every individual of a qualifying data breach, regardless of the total number affected.) Another approach in the United States is seen in the breach notification requirements in the federal health information privacy law, where the

[5] In the United States, 29 of the 47 state breach notification laws require notification of a regulator, in addition to notification of affected individuals. A breach size threshold for notification of a regulator appears in half of those 29 laws. *See* Baker Hostetler, Data Breach Charts, October 2017, available at https://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf.

[6] For Massachusetts breaches, see www.mass.gov/ago/doing-business-in-massachusetts/privacy-and-data-security/security-breaches.html. For California, see California Attorney General, *California Data Breach Report 2012-2015*, p. 9 at www.oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf.

regulator must be notified promptly in the case of breaches affecting more than 500 individuals, but annually for breaches affecting fewer individuals.[7]

Also the experience of the data protection authority in the Netherlands may be instructive on this issue. The Dutch data breach notification requirement sets a higher bar than GDPR for notifying the supervisory authority (likelihood of serious adverse effects versus "unless … unlikely to result in a risk to rights and freedoms …"). Just four months after the new requirement took effect in January 2016, the authority is reported to have received 1,500 breach notifications[8]; a similar or larger volume would pose challenges to under-resourced supervisory authorities.

Recommendations on Administrative Notification Threshold

- Consider advising supervisory authorities to use a threshold of number of individuals affected by a breach to help prioritise their administrative review. The size threshold, say between 250 and 500 individuals affected, should be consistent across all jurisdictions.

- Consider setting a threshold of the number of individuals affected for organizations to notify supervisory authorities, except in the case of a breach that poses a high risk to individual rights and freedoms. The size threshold, say between 250 and 500 individuals, should be consistent across all jurisdictions.

3.2 Special Categories of Personal Data

In the paragraph beginning at the bottom of page 19 and continuing onto page 20, the WP appears to depart from the GDPR in asserting that breaches involving special categories of personal data or potentially implicating certain categories of harm should *per se* be considered likely to occur. On this point, the Guidelines cite Recitals 75 and 85, on Notification obligation of breaches to the supervisory authority. Both Recitals, however, condition their positions on the *likelihood* of harm to individuals. Recital 75, on Risks to the rights and freedoms of natural

[7] Health Insurance Portability and Accountability Act (HIPAA), Data Breach Notification Rule, 45 CFR §§ 164.400-414, https://www.hhs.gov/hipaa/for-professionals/breach-notification.

[8] International Association of Privacy Professionals, "130 days, 1,500 notifications: Does Dutch breach rule foreshadow GDPR?" 16 May 2016, at https://iapp.org/news/a/130-days-1500-notifications-does-dutch-breach-rule-foreshadow-gdpr/#.

persons, clearly states that data processing risks are of "varying likelihood and severity", before going on to enumerate types of harm and types of personal data. Similarly, Recital 85, on Notification obligation of breaches to the supervisory authority, describes types of harm natural persons could experience if a breach is not addressed in an appropriate and timely manner, acknowledging that a control may be able to "demonstrate, in accordance with the accountability principle, that the personal data breach is *unlikely* to result in a risk to … rights and freedoms" (emphasis added).

Recommendations on Criteria for Assessing Risk

- Modify Example Breach ix, on page 30, adding the need to assess the likelihood and risk posed by the particular types of personal data involved and other relevant factors to the consideration of whether to notify the supervisory authority and the data subjects.
- In Example Breach x, on page 30, revise the advice under the question of notifying the supervisory authority to add the need to assess the likelihood of the breach's resulting in posing a risk to individuals' rights and freedoms.
- Revise the language in the opening paragraph on page 20 to eliminate the imputation that any data breach involving special categories of personal data should automatically be deemed to have a likelihood of risk to individuals' rights and freedoms.

4. Timing of Notification

4.1 Awareness of a Breach

The discussion in Section II, Notification to the supervisory authority, of when a controller becomes "aware" of a data breach is very helpful. We certainly agree with the WP that a controller should strive to act promptly to determine whether or not a security incident constitutes a notifiable breach. The Guidelines could be clearer, however, in stating that the 72-hour deadline for notifying does not begin until *after* the controller has completed an investigation that results in awareness that the incident a) involved personal data and b) is likely to result in a risk to individuals' rights and freedoms, per Article 33(1). Such a determination depends on an investigation, which may in some cases be "short", as the Guidelines suggest at the bottom of page 9, but not always.

Article 33(1) qualifies the 72-hour time limit for notifying the supervisory authority as "where feasible." Based on over a decade of experience with breach notification in other jurisdictions, such a time frame is not feasible in many, perhaps in most, breaches. Even in cases in which the

facts seem to be straightforward, such as an email containing sensitive personal information mistakenly sent to an unintended recipient, an assessment of the severity and likelihood of the risk associated with the particular circumstances is typically not apparent at the outset. Logs may need to be reviewed, people interviewed and an affidavit obtained from the unintended recipient confirming that the data were not accessed, further disclosed or used in an unauthorised manner, and have been permanently deleted. In incidents where an attacker uses sophisticated techniques to cover tracks or leave false trails, an organisation may need to conduct a forensic investigation, often including hiring outside expertise, to determine what occurred. It would be helpful if the WP made clear that an organisation's decision to hire a forensics firm or engage in a technical investigation does not automatically mean the organisation is aware of a notifiable breach. Instead it would only become aware of a notifiable breach if the investigation revealed sufficient facts to enable the organisation to assess the likelihood and severity of the risk.

Further on the issue of timing of notification, US state breach notification laws typically allow data owners (controllers) time to "restore the reasonable integrity of the affected system" before notifying affected individuals or regulators. The Guidelines acknowledge this issue in the description of the practical steps that controllers and processors should take in response to all breaches, where the final step listed is "[a]t the same time, the controller should act to contain and recover the breach" (p. 10). In fact, this last is an immediate necessity, in order to ensure the ongoing security, confidentiality and integrity required in Article 32(1)(b). While having a comprehensive breach response plan will enable an organisation that has suffered a breach to proceed on several levels simultaneously, the essential actions to "stop the bleeding" invariably add time to the assessment process.

The statement on page 11 that in a breach originating with a processor the controller should be considered as "aware" once the processor has become aware seems to contradict the intent of the GDPR. In breaches originating with a processor, notification of the supervisory authority is a two-step process. This intention is reflected in the distinct breach notification time frames applicable to controllers and processors in Article 33, paragraphs (1) and (2), respectively. Controllers' obligations are only explicitly linked to processors' obligations in Article 28(3)(f), which merely requires the processor to assist 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". The processor will often not be aware of facts that are relevant to determine whether a personal data breach has occurred, such as the likelihood and

severity of the risks to individuals, the conditions under which the data were collected by the controller, the sensitivity of data based on context or whether the data concern real people or are only dummy data used in testing. This is also true for the "accidental", "unlawful" and "unauthorised" elements of a breach, which raise highly contextual issues often requiring the controller's knowledge.

Example Breach vii (Awareness)
In Example Breach vii on page 29, where a processor that hosts websites identifies a coding error that allows any user to access other users' accounts, the WP advises that the processor must notify its controller-clients without undue delay. Then the Guidelines say that controllers should be considered as "having become aware" when notified by the processor, "assuming that the website hosting company has conducted its own investigation". The point could be expressed more appropriately by clarifying that the controller, once notified by the processor, is responsible for determining the likelihood of risk to individuals' rights and freedoms, whether through joint or separate investigations.

The breach examples offered in Section II.A on page 9 to illustrate when awareness would be reached do not all adequately reflect where investigation would be needed before a likelihood of risk to individuals could be determined with even a reasonable degree of certainty. In the first example, a lost CD with unencrypted data, the conclusion is that while it may not be possible to know whether the data on the disk were accessed, the controller can know with "a reasonable degree of certainty" that a [notifiable] breach has occurred and thus "the controller would become aware when it realized that the CD had been lost". This does not take into account the need to investigate whether or not the disk contained *personal* data and the nature of the data, to enable the controller to determine a likelihood of risk to the data subjects.

In the last example in the box on page 9, the assertion is that "there is no doubt that a [controller] has become aware" that a [notifiable] breach has occurred once it has been contacted by a cybercriminal claiming to have hacked the controller's system and asking for ransom. A controller in that situation would first have to conduct an investigation to verify the claim of the cybercriminal, the involvement of personal data and the likely risk to individuals posed by the incident, including whether the controller has a backup of the data. Only after that, could the controller be "aware" of a need to notify.

We note that in the example in the box on page 10, of a user's report of receiving a fraudulent email containing personal data related to the controller's service, the Guidelines do

appropriately acknowledge the need to include in the "short period of investigation" whether the incident presents a likely risk to individuals.

Finally, the Guidelines also envision a situation in which the controller may notify the supervisory authority in phases (p. 13). In many cases, a controller will not be able to predict, as the WP recommends, whether it will be in a position to provide more information at a later stage, which the supervisory authority should not hold against the controller. In addition, given the risk that could arise if incomplete information about an incident were revealed, we recommend that there be a mechanism through which controllers could request that a supervisory authority keep information confidential until the controller's investigations are complete.

Recommendations on Timing of Notification

- Delete "short" from the phrase "short period of investigation" in the paragraph at the bottom of page 9 and in the box on page 10, and "brief" from "brief period of investigation" at the top of page 11. The importance of notifying without undue delay might be emphasised in other ways without unrealistically asserting that all initial investigations of security incidents will be "short".

- 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". As our discussion of the problems with the examples above indicates, 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".

- Consider updating 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.

- Modify Example Breach vii on page 29: Revise second sentence under notification of supervisory authority. The advice could read: "Having been notified by the processor, a

controller is responsible for assessing the likelihood of risk to individuals' rights and freedoms, either in concert with the processor or separately, as provided for by contract. The controller should notify the supervisory authority, unless it determines that such risk is unlikely".

- Advise that in a phased notification of a supervisory authority, a controller may avail itself of a mechanism for keeping reported information confidential until its investigation is complete.

4.2 Law Enforcement Delay

Most data breach notification laws in other jurisdictions allow for a limited "law enforcement delay" in making the required notification. The use of such a delay is generally discretionary and restricted to circumstances in which law enforcement says that notifying would impede an investigation.[9] While the use of a law enforcement delay appears to be rare,[10] the WP should consider addressing cases in which incidents are under criminal investigation and some delay in notification would be appropriate. Recital 88 of GDPR recognises this possibility, noting that rules and procedures should take into account "the legitimate interests of law-enforcement authorities where early disclosure could unnecessarily hamper the investigation of the circumstances of a personal data breach".

5. Controller-Processor Responsibilities

We appreciate the attention the WP brings to the issue of controller-processor responsibilities regarding data breaches. As noted in the first paragraph in Section II.A.3 on page 11, the controller has overall responsibility for protecting personal data and therefore for meeting the obligations of personal data breach notification. The WP goes on to cite the requirement for a controller to contractually obligate processors of the controller's personal data to assist the controller in ensuring compliance with Articles 32 through 36.

Because the specific notification practices between the processor and controller are subject to contract, the controller, who bears the ultimate responsibility for breach notification, should

[9] See Baker-Hostetler, U.S. State Breach Law Summary, October 2017, at www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/State_Data_Breach_Statute_Form.pdf.

[10] In California, a law enforcement delay in notification occurred in 7 percent of the breaches reported to the attorney general from 2012 through 2015. California Attorney General, *California Data Breach Report 2012-2015*, p. 26 at www.oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf.

have the discretion to determine the procedures its processors are to follow in the event of a data breach. Article 33's only requirement on controller-processor obligations regarding notification is that a processor, after becoming aware of a personal data breach originating with the processor, shall notify the controller "without undue delay" (Article 33(2)).

In the third paragraph under Processor obligations on page 11, the WP recommends that a processor's notification of a controller should be "immediate". This is an unclear and unrealistic expectation that could imply that processors should notify controllers of any and every security incident, without any prior investigation. This could run counter to the parties' agreements or involve other, non-breached parties and could lead to an increase in incorrect breach notifications to both regulators and data subjects. Some supply chains could have four or five layers, requiring time for investigation in order to determine what entities are involved and need to be notified. "Prompt notification" would be a better standard here, emphasising the necessity of avoiding undue delay. This may be a reasonable practice that could in some cases lead to a speedier decision on the need to notify both the supervisory authority and affected individuals, and could be provided for by contract.

In paragraph 5 of Section II.A.3 on page 11, the WP advises that if provided for by contract, a processor could make the notification on behalf of a controller to both the supervisory authority and affected individuals. The WP no doubt refers here only to a breach that originates with the processor. While contracts could permit use of such a procedure in breaches originating with a processor, the controller remains ultimately responsible for compliance with Articles 33 and 34 and should oversee and approve the processor's actions. This includes the content and method of the communication to individuals. One factor to consider is the need to make the breach communication recognisable to the recipients. A communication coming from a data processor who is likely unknown to the recipient may be ignored or not trusted. The controller should ensure that the entity with which the individual has a relationship is prominently identified, regardless of who sends the communication.

Furthermore, there will be cases in which a single processor providing services to multiple controllers suffers a data breach. In such cases, the WP should recognise the flexibility in the way the processor notifies the numerous affected controllers. For example, in terms of a method for communicating to all controllers, the processor should be allowed to discharge its legal obligation under GDPR (subject also to contractual terms) by sending an automated email requiring controllers to access their accounts or log on to a specific website, in order to ensure swift communication and breach response.

Finally, there may be cases in which there are joint controllers, each with the obligation to notify of the same personal data breach affecting a jointly managed system. It would not benefit supervisory authorities or data subjects to receive multiple notifications of the same breach. The WP should advise that in light of such situations, controllers can designate responsibility for notification or jointly notify the supervisory authority and jointly communicate with affected individuals.

Recommendations on Controller-Processor Responsibilities

- Change the word "immediate" to "prompt" in the second sentence of the third paragraph in Section II.A.3 on page 11, and revise the last sentence in that paragraph to read: "A processor's prompt notification of the controller of a breach originating with the processor is important, as it enables the controller to make a determination of the likelihood and severity of risk to individuals and of the need to notify the supervisory authority, through investigations conducted either in concert with the processor or separately, according to contract terms".

- Delete 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". Replace the deleted sentence 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 at least has found that the breach affects the controller) and has taken steps to secure the system, as required by Article 32(1)(2).

- In paragraph 5 of Section II.A on page 11: Add to the beginning of the first sentence the phrase: "In the case of a breach originating with the processor …".

- Add a statement that joint controllers can designate responsibility for notification or jointly notify the supervisory authority and jointly communicate with affected individuals.

6. Supervisory Authority to Notify

Article 33(1) requires a controller to notify the competent supervisory authority. In Section II.C on pages 14-15, the WP notes that when a personal data breach affects individuals in more than one member state, the lead supervisory authority is the one that a controller must notify.

The Guidelines go on to state that while a controller may choose to notify supervisory authorities in all member states with affected data subjects, the WP recommends that if the choice is to notify just the lead authority, then the controller's notification should identify all the affected member states.

The WP should also address specifically the situation of a controller that does not have an establishment in the EU and one in which the breach only affects individuals who are not located in the jurisdiction of the lead authority. A controller in the former situation might notify the competent authority in the jurisdiction where the controller's representative is located, in addition to the supervisory authority where the breach took place, as generally advised by the WP.

In addition, the data breach notification obligation in the GDPR overlaps with incident reporting obligations existing under the NIS Directive (Cybersecurity) and other sectorial regulations, such as the Payment Services Directive 2. In practice, this means that a single security incident could trigger the obligation for controllers to notify multiple authorities, in different countries, within different timelines, and require different types of information in different formats. Controllers may therefore have to dedicate significant resources to handle those notifications rather than to manage and contain the incident and protect the rights and freedoms of individuals. We would recommend that data protection authorities work closely with financial and other competent authorities to streamline the processes and procedures for such reports.

Recommendations on Supervisory Authority to Notify

- Modify the Flow Chart in Annex A on page 26: In the box in the right 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)".
- Clarify which supervisory authority should be notified by a controller that does not have an establishment in the EU and which authority should be notified by a controller when a breach affects only individuals not located in the jurisdiction of the controller's lead authority.

7. Methods of Communication to Individuals

In Section III.C., Contacting Individuals, on page 18, the WP discusses how a controller should communicate about a personal data breach to affected individuals. The Guidelines recommend

notifying individuals "directly", in "dedicated messages" that are solely devoted to the data breach communication. As stated by the WP in the Introduction to the Guidelines, the primary objective of such a communication should be to limit damage to individuals by providing them with information about the breach that will enable them to take appropriate action to protect themselves against its consequences. To be effective, the communication must capture the attention and win the trust of recipients, but not all of the methods recommended in the Guidelines are likely to do this.

For example, because of their frequent use in phishing and other forms of consumer fraud, such email and SMS may be regarded by recipients as suspicious. If recipients do not trust the communication, believing it to be fraudulent, they will not take appropriate defensive measures. While the Guidelines do point out that multiple methods of communication should be considered, the potential drawbacks of relying exclusively on fraud-prone communication channels should also be mentioned.

Recommendation on Methods of Communication to Individuals
In Section III.C, on page 18, third paragraph, add a warning about the potential drawbacks of email and SMS as a sole communication method for notifying individuals about a personal data breach.

Conclusion

Thank you for the opportunity to provide comments on key issues related to personal data breach notification. We hope that our recommendations, which are drawn also from the Hunton & Williams law firm partners' long experience in dealing with data breach notification in multiple jurisdictions, will assist the WP as it finalises its Guidelines. Please do not hesitate to contact us for further information or clarification at bbellamy@hunton.com or mheyder@hunton.com.