2 March 2021

Comments by the Centre for Information Policy Leadership on the European Data Protection Board's Guidelines 01/2021 on Examples Regarding Data Breach Notification

On 14 January 2021, the European Data Protection Board (EDPB) issued its Draft Guidelines 01/2021 on examples regarding data breach notification (Guidelines).[1] The EDPB invited public comments on this document by 2 March 2021. The Centre for Information Policy Leadership (CIPL)[2] welcomes the opportunity to submit the comments and recommendations below as input for the final Guidelines.

CIPL welcomes the EDPB's initiative to provide concrete personal data breach (Data Breach/es) use cases and to provide recommendations to help organisations put in place relevant technical and organisational measures, understand the risk factors to consider when assessing Data Breaches, and decide whether a notification to the data protection authority (DPA) and individuals is necessary (Notifiable Data Breach/es).

CIPL notes that there has been a trend of organisations over-notification of Data Breaches,[3] which has resulted in DPAs being overwhelmed with notifications. CIPL hopes these Guidelines will assist organisations in identifying Notifiable Data Breaches and help them make timely notifications in order to help prevent harm to individuals. The Guidelines offer pragmatic recommendations that consider the complexity of these situations for organisations that are the victims of attacks perpetrated by bad actors, as is typically the case.

CIPL believes these Guidelines to be timely, as cyberattacks have surged in the context of the COVID 19 crisis, which has triggered an acceleration of digital interactions and activities. In this context, consistency of approaches among DPAs in assessing whether a Data Breach is notifiable is paramount to an effective response by organisations. CIPL recommends the EDPB make clear that as per the WP 29 Guidelines on Personal data breach notification under Regulation 2016/679,[4] a Notifiable Data Breach in the context of

[1] **Guidelines 01/2021 on Examples regarding Data Breach Notification - version for public consultation.**

[2] CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and over 80 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 Andrews Kurth.

[3] See Contribution from the **Multistakeholder Expert Group to the Commission 2020 Evaluation of the General Data Protection Regulation,** page 36: "Organisations struggle in identifying the moment when controllers can be considered to have become "aware" of a breach. […] This may lead to two alternative scenarios: (i) organisations notify all security incidents as soon as they reach a minimum level of awareness that such incidents may constitute a potential data breach under the GDPR, overloading the supervisory authorities […]"; "organisations tend to notify DPAs in cases that are likely below the threshold in order to avoid potential fines in case of wrong judgement."

[4] **https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052.** See also **CIPL Comments on WP29's Breach Notification Guidelines**.

a cross-border processing has to be brought to the attention of the lead DPA only, which is not necessarily the DPA of the country where the potentially affected individuals are located or where the Data Breach has materially occurred. There have been instances where DPAs have reached out to organisations directly without regard for the one-stop-shop mechanism, potentially affecting the efficiency of organisations' management of the Data Breaches.

More generally, CIPL underlines that having a robust accountability framework within an organisation[5] is essential for assessing relevant risks, implementing a level of security appropriate to the risks, devising appropriate policies and crisis management procedures, training employees, performing processor due diligence, auditing practices and responding to a Data Breach. In this context, CIPL welcomes the recommendations in paragraphs 11 to 13 of the Guidelines that help foster greater accountability practices within organisations by stressing, for example:

- The importance of setting up dedicated roles, responsibilities and reporting lines for the employees of the organisation involved in addressing the Data Breach;
- The necessity of training and raising the awareness of employees processing personal data;
- The need for a clear reporting process and adequate policies and procedures, including, for example, the suggestion for a Handbook on Handling Personal Data Breaches or any other accountability tool deemed relevant by the organisation.

CIPL believes that the Guidelines are generally not well aligned with current market practices and should further consider recognised principles of forensic evidence. To better align the IT security measures in place in many organisations and to avoid unnecessary problems in implementation by organisations, CIPL recommends that the EDPB consults with the ENISA prior to issuing the final Guidelines. The Guidelines should also highlight the innovative and unforeseeable nature of attacks, including state-sponsored attacks and cybercrime networks.

In addition, the proposed Guidelines are at once too narrow in some instances, while also sometimes extending beyond the language of the GDPR and not sufficiently considering the following points.

1. Preliminary Comments

1.1 Security obligation and Data Breaches

CIPL fully agrees with the Guidelines that prevention and anticipation of Data Breaches may be more effective than correction. However, Article 32 of the GDPR expressly confirms that security is a risk-based activity that requires the implementation of technical and organisational measures to ensure a level of security appropriate to the risk of any anticipated potential harms in order to mitigate that risk. This implies contextual discernment of existing risks and potential future harms. It cannot be an obligation for

[5] See CIPL Accountability Wheel in Appendix 1 and **The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society.**

organisations to guarantee absolute security of data processing activities.[6] Security management is a complex task relying on a wide variety of factors depending on context and requiring ongoing monitoring of internal and external threats. External threats, in particular, become more sophisticated every day and may be unpredictable even for the most mature organisations.[7] In addition, human errors can never be fully excluded, only lessened through training and awareness sessions. Mitigation measures must always take into account the specific circumstances of the processing.[8] In several instances, identifying a breach can take a substantial amount of time.[9] Therefore CIPL recommends that the Guidelines avoid suggesting that the majority of security threats and Data Breaches can be prevented easily through organisational and technical measures without taking into account the specific context at stake.

The Guidelines seem to suggest that organisations may not have provided an appropriate level of security because they have suffered a specific type of Data Breach or because it affects sensitive data.[10] In other words, because an organisation lost sensitive data, that organisation did not have appropriate security. That is not accurate. As explained above, this conclusion is not consistent with the GDPR risk-based approach to security and presupposes a failure on the part of the organisation. By providing for a Data Breach notification obligation to DPAs and individuals as the case may be, Articles 33 and 34 GDPR expressly acknowledge that not all risks can be fully mitigated with state-of-the-art security, and that Data Breaches are to be expected and are not always due to a lack of implementation of appropriate measures. This would be the case only when technical and organizational measures do not ensure a level of security appropriate to the risk, taking into consideration cost of implementation, nature, scope, context and purpose of processing, as well as varying likelihood and severity for the rights and freedoms of individuals. In other words, appropriate technical and organisational security does not completely extinguish all possible vulnerabilities in a system, and breaches will not always be indicative of a lack of compliance with Article 32 GDPR. Nor should breaches alone lead to systematic enforcement, especially if the organisation

[6] In other words, Article 32 GDPR provides for an obligation of means and not an obligation of result.

[7] See for instance zero day exploit which is an exploit for a vulnerability in a piece of software that is not publicly known yet and gives attackers a sure way of accessing a system. **https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/zero-day**. See also the ENISA Threat Landscape 2020 explaining that cyber-attacks become more sophisticated, targeted, widespread and undetected **https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020.** In addition, the existence of criminal rings and networks selling cybercrime tools SaaS, make it fairly easy for a motivated attacker to deploy sophisticated attacks at a very low cost.

[8] For instance, measures to check unusual data flows between file server and employees' workstations to mitigate the risk of exfiltration of data could lead to unlawful behavioural surveillance under many national employment laws.

[9] See the 2019 **IBM survey** on 506 organisations of various sizes in 16 countries, across 17 industries which determined that the average time to identify a data breach in 2019 was 206 days.

[10] See for instance Paragraph 8 of the Guidelines: "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". Paragraph 18: "The majority of these breaches can be prevented by ensuring that appropriate organizational, physical and technological security measures have been taken"; Paragraph 41: "Though backup was in place, it was also affected by the attack. This arrangement alone raises questions about the quality of the controller's prior IT security measures"; Paragraph 65: "The fact that a breach could happen in such a sensitive environment points to significant data security holes in the controller's system"; Paragraph 131: "The fact that a breach could happen and go undetected for so long [...] highlighted significant problems in the controller's IT security systems."

is acting with full accountability as illustrated in Appendix 1.[11] CIPL recommends that the Guidelines avoid inferring that a Data Breach is indicative of defective organisational measures. The focus should lie more on how Personal Data Breaches are handled in an efficient way.

1.2 Risk assessment of the Data Breach

Each Use Case in the Guidelines includes an analysis of the risk involved with the Data Breach, relying on factors such as "significant effect" on individuals, the risks to a "data subject's private life" and potential "material damage." This risk analysis enables organisations to determine whether a Data Breach becomes a Notifiable Data Breach. In order to provide more clarity and coherence with the risk assessment terminology of Articles 24 and 32 GDPR, CIPL recommends that the Use Cases clearly mention that risk assessments cover an analysis of the likelihood and severity of the risks to the rights and freedoms of individuals.[12]

The Guidelines appear to link the number of potentially affected individuals to the notification threshold.[13] CIPL highlights that this is not a requirement under GDPR for Data Breach notification purposes.[14] CIPL believes that linking the number of potentially affected individuals to determine whether the Data Breach should trigger notification could have unintended consequences. For instance, an incident which is unlikely to cause harm to individuals could be seen as having a higher risk classification due to the number of individuals potentially impacted, and could result in inappropriate regulatory notification. This could result in overly burdening organisations, DPAs and individuals in situations that present very low to no risk only because the volume of individuals impacted is high (see section 1.4).

Use Case 1 implies that in the event that the exfiltrated data was encrypted, the organisation should still ensure that cryptanalytics progress could not render the encrypted data intelligible in the future. CIPL believes this places an unreasonable and unattainable burden on organisations. It may also create a high burden for DPAs as they would also have to investigate whether this possibility materialised. The Guidelines should clarify that the risk analysis after the Data Breach should be conducted with a level of reasonableness given the state of technology at the time of the Data Breach and not with the possibility of what it could happen in the future. This approach would also be fully aligned with Article 32 GDPR referring to the "state of the art" in defining the measures appropriate to the risk. Further, a lack of

[11] The situation would be different in case of a systemic problem causing several similar Data Breaches where the organisation does not take steps to address the situation.

[12] This analysis may also take into account the fact that some of the data covered by the Data Breach may already be publicly available (e.g. on social media). See for example Use Case 5 where job application data may be available on professional social media platforms and Use Case 8, where business data may already be publicly available.

[13] See for instance Paragraph 43: "The nature, sensitivity, and volume of personal data increases the risks further, because the number of individuals affected is high, as is the overall quantity of affected personal data." Paragraph 64: "The breach concerns financial data beyond the identity and user ID information, making it particularly severe. The number of individuals affected is high." Paragraph 80: "The combination of the low number of individuals affected, the immediate detection of the breach and the measures taken to have its effects minimized make this particular case no risk."

[14] Article 35 GDPR provides that a data protection impact assessment (DPIA) may be required in case of processing on a large scale of special categories of data, but there is no automaticity with the obligation to notify the DPA or the individuals in case of a Data Breach.

evidence, e.g. log files for exfiltration, should not automatically lead to the assessment that data was exfiltrated. The Guidelines should confirm that organisations undertake a holistic risk assessment prior to any Data Breach Notification, which takes into account all of the circumstances, including the facts and conclusions that can be established with a degree of certainty, as opposed to speculation or remote possibility.

Additionally, the Guidelines should clarify the point at which organisations can reasonably end Data Breach investigations and begin to draw conclusions, taking into account the strain these investigations place on resources. For example, Use Case 2 provides that "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." Use Case 1, states that "an internal investigation…determined with certainty that the perpetrator only accessed 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." This goes beyond the GDPR, which does not require organisations to fully mitigate every potential and theoretical risk. That would be impossible in any case, even for the most sophisticated organisations. In addition, organisations cannot practically continue their investigations for an indefinite period of time. Organisations need to be able to rely upon their information security experts to make assessments as to the reasonable chances of identifying the cause of a data breach.[15] It should be borne in mind that an organisation will be very determined to identify any such causes. Therefore, CIPL recommends that the Guidelines expressly mention that organisations should perform risk assessments, draw conclusions and make decisions with a "reasonable degree of certainty" as provided in the previous WP 29 Guidelines on Personal data breach notification under Regulation 2016/679.[16]

More generally, CIPL recommends that the Guidelines recognise that Data Breaches may at times present unprecedented questions and challenges against the backdrop of external attackers who constantly change their methods of attack. The Guidelines should make clear that there might not always be a "right" answer – and that the expectation is for organisations to act in a reasonable and proportionate manner. This would be aligned with the GDPR's risk-based approach. Article 33(4) of the GDPR acknowledges this by providing that the organisation may not be in the position to provide complete information on the Notifiable Data Breach and that notification in phases is acceptable. This approach would also make the Guidelines more flexible and future-proof to be able to take into account future technological developments, business models, actors and data uses in new contexts. This approach will better accommodate the variety and complexity of current and future data uses and business relationships.

1.3 Notification timeline

Paragraph 9 of the Guidelines explores the complexities of an investigation chronology, but does not properly acknowledge that a credible risk assessment requires a reasonable level of examination and factual analysis. A credible risk assessment includes a detailed forensic analysis to determine the risk of likelihood and severity of harm to individuals and assess whether a Data Breach is reportable. In the more complex scenarios, and in particular those that involve sophisticated external attacks, investigations may

[15] For instance a Data Breach that is based on internal human error without malicious intent would probably be considered as lower risk than an attack performed by a malicious actor.
[16] See note 4 at page 11.

take place over several weeks before facts (even basic facts such as whether there was any possibility of unauthorised access to data) can be established. In order to acknowledge this, CIPL recommends that the language stating "controllers should make this assessment at the time they become aware of the breach … [and] not wait for a detailed forensic examination" should be revised. In addition, it is important to highlight that the standard may be contradictory, as organisations are being asked to make an objective and legal assessment at a time when they may not have sufficient information about the events. By requiring organizations to prepare preliminary notifications when they are still gathering information, the Guidelines are placing controllers in a risky position, as the supplementary notification could contradict the content of the preliminary notification and therefore increase exposure for controllers. Finally, the outcome of the investigation could affect the controller's decision to notify the DPA, making early notifications without proper assessments unnecessary and burdensome. CIPL would welcome case studies taking into account these realities, including examples of smaller organisations, such as start-ups, that do not necessarily have the expertise to conduct these investigations internally.

The Guidelines must also clarify how they relate to the previous WP 29 Guidelines on Personal data breach notification under Regulation 2016/679[17], especially with regards to the situation of when a controller can be considered to be "made aware" of a breach. The Guidelines provide that "The breach should be notified when the controller is of the opinion that it is likely to result in a risk to the rights and freedoms of the data subject. Controllers should make this assessment at the time they become aware of the breach." The WP 29 Guidelines contain helpful construction that the organisation's "awareness" of a breach should not always necessarily be when it is first notified of a potential incident, but when it has a reasonable degree of certainty that an incident has occurred that has led to personal data being compromised. With the EDPB recommendation above, it would be helpful to acknowledge that there can be significant work to do in practice between these two points (from "awareness" to "notice"), which is why the GDPR provides a 72 hour period for this, extended from initial draft legislative proposals of 24 hours, and that organisations will not be penalised or criticised by DPAs for taking the statutory allotted time to make these assessments.

Additional Use Cases would be welcomed to better-illustrate when an organisation becomes "aware" of a Data Breach. There is often a practical delay between when an employee first becomes aware of a breach and when the employee with responsibility for data protection matters is properly informed. The Guidelines should also take into account that new and sophisticated incidents may be difficult to identify and may result in longer timelines for communication to the DPO or other appropriate internal channels. For instance, in the context of a global incident, it may take time to identify the scope of the breach, the affected jurisdictions and when "the GDPR part" begins. It should be clarified that the organisation "becomes aware" of a breach under the GDPR when it establishes that the global breach affects personal data subject to the GDPR. In particular, statements such as "we think that some EU data may be involved, but we don't know what data or what countries" should not be sufficient to consider that the organisaton is "aware" of a GDPR Data Breach before there has been explicit confirmation of the scope of the Data Breach.

In addition, the Guidelines should clarify that organisations that are diligent and detect prospective issues that may not have fully materialised yet should not be punished for their early detection, evaluation and

[17] See note 4.

intervention in the event of subsequent reporting. Further, CIPL would welcome clarification on how organisations can properly balance the obligation to notify individuals and DPAs about Data Breaches within a short timeline with the obligation to carry out proper due diligence and implement reasonable and proportionate remedial actions in more complex scenarios. In addition, the truncated timeframe for data breach notification proposed in some instances in the Guidelines[18] appears to go beyond the requirements of the GDPR and should be revised or removed.

1.4 Data Breach notification

The Guidelines should set out clear notification thresholds especially for small-scale Data Breaches and avoid setting a low threshold for notification. The Guidelines as currently drafted may result in swamping DPAs with notifications as already mentioned. Breach notification may also be a resource-intensive activity depending on the size and complexity of the organisation. This may result in a significant financial and administrative burden for organisations, exacerbated by the rise in external threats and attacks. If the threshold for notification is set too low, resources that could otherwise be spent on augmenting internal compliance processes and protecting individuals might be misdirected.

Article 34(1) GDPR requires an organisation to notify individuals when a data breach is likely to result in a high risk to their rights and freedoms. The Guidelines provide that where an organisation chooses to notify individuals using public communication (e.g., website post), it must be precise and clear with "exact references to the relevant GDPR provisions."[19] CIPL believes this goes beyond the requirements of the GDPR and should be removed. Rather, CIPL suggests the Guidelines change this requirement to a recommendation and best practice demonstrating transparency and accountability of the organisation that can be used as a mitigating factor as suggested by the Guidelines in paragraph 59.

CIPL also underlines the importance of not setting a standard for Data breach notification to individuals that is too low. The objective should be to limit notification to individuals to the highest-risk cases to avoid "notification fatigue" by making these notifications a regular practice. Frequent notification would, in fact, be less protective of individuals as it would not enable them to differentiate situations where a positive action is required to protect themselves from notifications where the risk to their rights and freedoms is trivial. Finally, over-notification of individuals could lead to a severe loss of trust which could be harmful to the digital economy.

[18] See Paragraph 24 "Therefore, it could be determined that exceeding the 72-hour time limit is unadvisable in any case, but when dealing with high risk level cases, even complying with this deadline can be viewed as unsatisfactory."
[19] See Case 4, Paragraph 47.

1.5 DPA oversight and enforcement

As security and breach reporting are based on a risk assessment, there is always a chance that the residual risk materialises even in cases where the organisations assessed the risk as being unlikely. To avoid this uncertainty, some organisations choose to report every Data Breach to the DPA, regardless of whether the threshold for notification has been met. As previously mentioned, this situation results in over-reporting of Data Breaches to DPAs that do not have the resources to analyse and handle this volume of cases.[20] It also creates the risk that notifications of Data Breaches conveying high risks get lost in the huge quantity of trivial notifications. Lastly, it does not promote accountability of organisations that mechanically notify the DPA to protect themselves instead of conducting assessments in good faith taking into account the likelihood and severity of risk for individuals.

In order to not exacerbate over-reporting, CIPL recommends that the Guidelines avoid providing that "if a controller self-assesses the risk to be unlikely, but it turns out that the risk materialises, the relevant SA can use its corrective powers and may resort to sanctions."[21] At a minimum, this statement should be nuanced and limited to circumstances of gross negligence when assessing the potential risk of the Data Breach for individuals. In other exceptional cases where an organisation, in good faith, assessed the risk appropriately with the involvement of qualified security professionals and determined it did not meet the notification threshold, but harm materialised anyway, it should still be considered to have fulfilled its obligation under Article 33 GDPR. The DPA should not automatically resort to its corrective powers, but should seek to address the issue with the organisation and, as the case may be, with the individual(s).

CIPL observes that there is currently a tendency of some DPAs to contact organisations on behalf of individuals for incidents which are not Notifiable Data Breaches. Several DPAs appear to follow up with organisations on every single incident reported to them by individuals. The Guidelines should clarify that DPAs should first verify whether the incident is a Notifiable Data Breach before reaching out automatically to organisations. The Guidelines should also provide for a common approach for DPAs to assess when organisations should be contacted directly by the DPA in the absence of a breach notification. CIPL recommends the Guidelines separate incidents that DPAs will pursue on behalf of individuals from incidents that they will conclude directly with complainants.

[20] See the Irish Data Protection Commission warning that companies who 'over-report' and adopt an overly conservative approach to the GDPR's breach notification requirements may risk enforcement action from the Data Protection Commission: https://www.irelandip.com/2018/02/articles/uncategorized/reporting-data-breaches-data-protection-commission-may-result-enforcement-action-warns-deputy-data-protection-commissioner/. See also the ICO warning against over-reporting https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/09/cbi-cyber-security-business-insight-conference/

[21] See paragraph 1.10 of the Guidelines.

Summary of CIPL Recommendations:

- **Avoid suggesting that Data Breaches can be prevented easily through organisational and technical measures without taking into account the specific context at stake;**
- **Do not conclude that a Data Breach is indicative of defective organisational measures;**
- **Clarify the relation of the Guidelines with the earlier WP 29 Guidelines on Personal data breach notification under Regulation 2016/679;**
- **Clarify that a risk assessment covers an analysis of the likelihood and severity of the risks for the rights and freedoms of individuals;**
- **Avoid relying on the number of potentially affected individuals to determine whether notification of the Data Breach should be required;**
- **Provide that the risk analysis should be conducted with a level of reasonableness given the state of technology at the time of the Data Breach and exclude mere speculative considerations on remote possibilities;**
- **Clarify the point at which organisations can reasonably end Data Breach investigations;**
- **Revise the statement that controllers should make risk assessments at the time they become aware of breaches and not wait for a detailed forensic examination;**
- **Take into account that global and sophisticated incidents may be more difficult to identify and may result in longer timelines for communication to appropriate internal channels;**
- **Clarify how organisations can balance a short notification timeline with the need to perform due diligence and implement remedial actions in more complex scenarios;**
- **Avoid setting low thresholds for notifying DPAs and individuals;**
- **Avoid providing that if an unlikely risk materializes, the DPA can use its corrective powers and resort to sanctions; and**
- **Provide that DPAs should verify whether the incident is a Notifiable Data Breach before reaching out automatically to organisations in situations where an incident is reported by individuals.**

2. Specific comments on Use Cases

As a general comment, CIPL believes that the Guidelines should make clear that the Use Cases are limited to specific fact patterns. Organisations cannot be expected to extrapolate rigid step-by-step instructions for dealing with similar, but not completely analogous, real-world scenarios. The Guidelines should instead emphasise that Data Breaches should be assessed on a case-by-case basis and should note that changing one factor in the Use Case could lead to a different outcome. The Guidelines should also should include a few paragraphs on the main take-aways from the Use Cases and stipulate that the Use Cases will be re-evaluated in the future as needed to reflect evolving market practices.

In addition, it would be useful if the Use Cases:

- Include examples of factors/facts that would have changed the outcome of the analysis (i.e. an initially Notifiable Data Breach would become non-notifiable and vice-versa);

- Include examples concluding that the issue identified is not a Data Breach but a security vulnerability (for instance, in the case of an inadvertent disclosure of data to a third party);

- Include an example involving B2B contact information to confirm that a Data Breach is unlikely to result in risk to individuals and therefore should not generally be a Reportable Data Breach.[22]

Further, it is worth reiterating that the key criteria to qualify the Notifiable Data Breach is not the cause of the Data Breach or the nature of the security incident as the Use Case classification of the Guidelines appear to suggest, but rather the likelihood and severity of the risks to the rights and freedoms of individuals. Finally, CIPL suggests that the EDPB works on separate guidelines to address more complex scenarios including multiple controllers, joint controllers and processors, and decentralised supply chains and operating models. The current Use Cases appear to reflect overly simplistic situations that are not aligned with the growing complexity of dynamic relationships between organisations and innovative data uses.

2.1 Ransomware - Cases 1-4

CIPL believes that access to encrypted or unencrypted data during a ransomware attack with no risk of harm to individuals (where, for example, the data is restored without causing any service disruptions and there was no exfiltration of data) should not be considered a Notifiable Data Breach.

In addition, notification should not be required before data exfiltration has been confirmed in cases where data has been encrypted by the attacker. In other words, organisations should be allowed to ascertain whether data exfiltration has occurred in cases where it is the deciding factor of the attack before requiring notification to the DPA.

[22] These processing activities generally involve only contact information including names and email address of contact persons at corporate customers that may already be publicly available.

Use Case 2 provides an example of a ransomware attack, with an online back-up failure, which the controller is able to mitigate with existing paper back-ups. The assessment identifies no personal data gaps or losses. Within a week the controller has been able to take steps to mitigate the attack and this leads to the consequence of "minor delays in order delivery" and loss of metadata (e.g. logs, time-stamps). It is not clear how the Guidelines make a link between a "minor order delay" and a data protection risk. If the example is understood correctly, the "damage to reputation" would be to the controller's reputation (in not fulfilling expectations on delivery timescales), not to the individual's reputation as a result of compromised data (as in this example the data is encrypted, it has not been exfiltrated and the confidentiality of the personal data "is not compromised"). The Guidelines should not recommend using the worst case scenario as the baseline for the risk assessment in case of doubt of potential access (see CIPL's comments above on the need to apply a reasonableness test in the risk assessment of the Data Breach).

2.2 Data exfiltration attacks – Cases 5-7

It is not clear how Use Case 5 results in a Data Breach requiring internal documentation in line with Article 33(5) GDPR. The incident involves devices being stolen, and the Guidelines conclude that the confidentiality and availability of data was not impacted due to several mitigating factors such as strong passwords and remote wiping of data, while back-up data was available to the controller. Therefore, in line with the definition of Article 4(12) GDPR, this security incident does not appear to lead "to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed." CIPL suggests that this Use Case be amended accordingly or further clarified.

In Use Case 7, the Guidelines consider that notification to 100 000 individuals would be required after a credential stuffing attack on a banking website[23] due to a website vulnerability that allowed the attacker to view the individuals' name, surname, gender, date and place of birth, fiscal code and user identification codes. The Guidelines should clarify that notification would not be always required in cases of credential stuffing attacks (in particular when there is no website vulnerability causing the issue). Often, organisations have no means to prevent credential stuffing attacks[24] as they relate to third parties obtaining valid credentials in the context of another breach. In addition, credential stuffing attacks are not always likely to result in a risk to the rights and freedoms of individuals. CIPL recommends that credential stuffing issues be rather regarded primarily as security issues. They should only trigger breach notification obligations in severe cases of malicious action taken on the data upon access, such as taking back up copies or exfiltrating data on a large scale.

In addition, successful account logins are common during credential stuffing attacks but do not always pose a risk to individuals if, for instance, the attacker was only logged in for a few seconds or did not access any personal data.[25] Customer accounts can also be set up so that little-to-no personal data is

[23] CIPL highlights that this Use Case needs to be adapted to take into consideration that banks are required to have a two-factor authentication under the PSD2 Directive.

[24] The issue generally comes from the use of similar passwords across different websites. In such cases, the victim organisation can do little to prevent access with valid credentials.

[25] The investigation could reveal that the attacker did not view any personal data (i.e., application logs allow companies to see what pages or data is accessed once a user logs in), or the landing page of an account upon log in

available on the account, or the data is pseudonymised, or the data available would cause minimal-to-no risk to the individual.[26] In these cases, if password resets are forced, there would be no risk to the rights and freedoms of individuals and notification would not be required.

2.3 Internal human risk source – Cases 8 - 9

Use Case 8 deals with the exfiltration of business contact data by a former employee during his/her period of notice with the intention to reuse this data to launch his/her new business. In this case, the threshold for a Notifiable Data Breach appears overly low. CIPL believes that notification should only be required where data is stolen and used for malicious purposes that could result in a risk to the rights and freedoms of individuals. The unauthorised use of personal data could also be prevented by requiring the ex-employee to sign a written attestation that the stolen data will be deleted and will not be further used. A written commitment would effectively deter the ex-employee from creating potential harms.

2.4 Mispostal – Cases 13-16

Use Case 14 implies that a social security number is being treated as sensitive personal data where this is not the case as per Article 9 GDPR. CIPL recommends this case to be revised or further clarified. Additionally, similar to Use Case 8 above, the Guidelines note that a controller can ask for deletion of a message inadvertently sent to a list of incorrect recipients, but that the controller cannot be certain that they will comply with the request. The Guidelines should provide clarity here on the steps that may be taken to mitigate this risk – for example, by receiving a confirmation from the recipients that the message has been deleted.

Use Case 16 describes a situation in which information relating to car insurance was sent via post to the wrong policyholder. The incorrectly delivered letter contained the name, address, date of birth, license plate number, approximate annual mileage and the classification of the insurance rate for the current and following year. Although a one-time incident, involving two individuals, the Guidelines make this a Notifiable Data Breach, assuming that it cannot be completely ruled out that the letter will be posted on social networks or that the policyholder will be contacted. CIPL believes this case adopts too low of a threshold that treats a highly unlikely worst case scenario as a realistic outcome ("it cannot be completely ruled out" – see Section 1.2 on the risk assessment of the Data Breach). Absent a clear and evidence-based assessment of the risk of malicious use by the unintended recipient, this Data Breach should not be notifiable. If the mailing error was frequent, affecting several individuals, it may be symptomatic of a wider problem. In this case, CIPL believes a notification to the DPA and individuals may be necessary after a proper risk assessment has been conducted. Alternatively, the Guidelines could clarify whether receiving a confirmation from the recipients that the message has been deleted would reduce the risk in such cases.

Use Case 17 describes a fraudulent call to change a victim's email address to receive the victim's billing statements. The Guidelines consider that the unauthorised access to the billing data poses a risk to the

---

does not display any personal data and the controller is able to confirm that the attacker did not navigate beyond the landing page.

[26] i.e., accounts where only names and masked account numbers are available and additional authentication is required to access personal data, such as addresses or billing statements.

victim and qualifies as a Reportable Data Breach. However, the Guidelines should clarify that notification is only required where the controller causes the identity theft and the Data Breach results from the identity theft. Controllers should not be required to report attempts of identity theft (successful or not) to DPAs if there is no risk to the rights and freedoms of individuals.

In addition, the controller can take appropriate actions to prevent a Data Breach from occurring. The controller could have discovered the fraudulent request after the operator had changed the victim's email address and prevented the billing data from being delivered to the wrong email address. Controllers may be expected to notify the victim of such attempts or take precautions to protect their customers from potential fraud, but notification to the DPAs should not be automatically required.

More generally, controllers should not be required to report cases of identity theft if fraudulent transactions are made by a malicious party using personal data obtained via a source other than the controller. For example, it is common for fraudsters to obtain credit card and billing information on the dark web and use the data to make fraudulent purchases. However, the controller should not have to report such cases to the DPAs since the controller did not cause the Data Breach that led to the fraud.

Summary of CIPL Recommendations:

- **Emphasise that the Use Cases are limited to specific-fact patterns and that case-by-case and contextual analysis of a Data Breach is necessary;**
- **Draft separate guidelines to address more complex scenarios including multiple parties and decentralised supply chains;**
- **Recognise that organisations should ascertain whether data exfiltration has occurred before deciding to notify the DPA;**
- **Acknowledge that a credential stuffing attack may not always be a Data Breach;**
- **Acknowledge that some risks cannot be completely ruled out, but that this does not automatically make the Data Breach notifiable; and**
- **Do not require automatic notification in case of identity theft.**

CIPL is grateful for the opportunity to provide recommendations on the EDPB's Guidelines on examples regarding data beach notification. If you would like to discuss these recommendations or require additional information, contact Bojana Bellamy, bbellamy@huntonAK.com, Markus Heyder, mheyder@huntonAK.com, or Nathalie Laneret, nlaneret@huntonAK.com.

Appendix 1: CIPL Accountability Wheel: Elements of Organisational Accountability

For security, Data Breach prevention and management, the essential elements of accountability include:

- ***Leadership and Oversight*:** Recognition and buy-in from the leadership level of an organisation. This includes executive-level oversight and accountability for data processing and data security. It also includes creating a culture that promotes accountable and secure data processing activities.
- ***Risk Assessment***: Implementing a risk-based approach to security and Data Breach prevention is required under Article 32 GDPR. Risk assessment should include consideration of the state of the art, the cost of implementation, the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals.
- ***Policies and Procedures***: Having policies and procedures in place is a necessary to process data in a secure way. This should include employees' obligations and due diligence on partners and vendors.
- ***Transparency*:** Meaningful transparency is a critical component of building trust, and it requires that individuals be given information on data processing activities.
- ***Training and awareness***: Employees, contractors and third parties should have clearly defined roles and responsibilities and be properly trained to address a Data Breach.
- ***Monitoring and Verification***: Organisations should conduct audits (internal and external) to verify that employees adhere to their policies and contractors comply with their contractual commitments. This may also include mock exercises to verify the respect of procedures in case of Data Breach. This enables to identify potential compliance gaps and to rectify them.
- ***Response and Enforcement***: Organisations should have processes in place for enforcing internally their policies regarding security and Data Breach management, including processes to escalate a Data Breach, assess risks and notify DPAs and individuals if necessary. They should also have processes to address requests and inquiries from DPAs and individuals and as the case may be provide for redress.