ANPD Autoridade Nacional de Proteção de Dados

CIPL AT 20 — SHAPING DATA POLICY FOR TOMORROW
HUNTON ANDREWS KURTH

MODEL FOR CONTRIBUTIONS CONCERNING THE PRELIMINARY INPUTS Nº 2/2021

NAME OF THE INSTITUTION/INDIVIDUAL: Centre for Information Policy Leadership (CIPL)

CPF/CNPJ: N/A

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUCTION

The questions below aim at gathering inputs for the new regulation of comunications to the ANPD and data subjects about security incidents that can pose risks or relevant harms to data subjects. Although the law establishes minimum criteria, ANPD must regulate some items such as the deadline for notification, and must define the form and best way for organizations to submit information as per Article 48 and following articles of Law 13.079 of August 14th, 2018 and item 3 of the 2021-2022 ANPD Regulatory Agenda.

Questions include the criteria for the ANPD to assess risks and relevant harms; the difference between risks and harms; considerations to be made in the risks and harms assessments; information that controllers must give to the ANPD and data subjects; the reasonable deadline to notify the ANPD and data subjects; and possible exemptions to the obligation to notify the ANPD and data subjects, among other topics.

Respondents can add other topics that are relevant to this analysis and regulatory impact to their response below.

ABOUT CIPL

The Centre for Information Policy Leadership (CIPL) welcomes the opportunity to respond to the second public consultation organised by the Autoridade Nacional de Proteção de Dados (ANPD) and would like to compliment ANPD for its engagement with, and request for input from, diverse stakeholders.

CIPL is a global data privacy and cybersecurity think tank based in Washington D.C., London and Brussels, founded in 2001 in the law firm of Hunton Andrews Kurth LLP. 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 as well as law- and policymakers around the world. We work with senior leaders and privacy experts of 80+ leading global organisations who provide us with insights into their data privacy practices and decision-making processes as well as inform and help shape our work as a think tank. See more about CIPL at https://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.

CONTRIBUTIONS **IMPORTANT:** The comments and suggestions concerning this call for inputs must be justified. Contributors must add the appropriate references (links) to any international norms mentioned.	
TOPIC/QUESTION	**CONTRIBUTION/INSTITUTION**
When can an incident result in risks or relevant harms to data subjects? What criteria should the ANPD take into account to consider the risks or harms as relevant?	Data processing activities will always present some degree of risk to individuals resulting from security incidents. Risk assessments include an analysis of the likelihood and severity of the risks to the rights and freedoms of individuals, which include any potential harms to individuals. The risks and harms associated with a particular security incident are not always correlated with the size or scope of the incident itself (e.g., breach of financial information for a small number of people might be more significant than a larger breach of less sensitive data). Harms can be classified as follows: • Material and non-material harms—also known as tangible and intangible harms. Materiality should be expressed in measurable and objective terms, such as a monetary value of the harm caused. Material harms may require prioritisation over non-material harms, depending on context; and • Societal harms—the consideration of societal harms (e.g., the public refraining from using a COVID-19 tracing app in case there was a security incident that was widely shared on the media) is not an LGPD requirement and the ANPD should not expect organisations to consider societal harms in all of their risk assessments. However, organisations may decide to consider them in appropriate circumstances (in the example mentioned previously, when processing personal data to fight the COVID-19 pandemic). The assessment of risks and the likelihood of harm in the context of security incidents, notification of incidents and remediation should not be considered in isolation from other aspects of LGPD-related risk assessments. Brazilian organisations are specifically required under Article 6, VII and VIII to adopt technical and administrative measures to ensure the security of personal data and prevent harms from happening—these would be mitigation measures considered as part of a risk assessment. Article 46 of the LGPD goes further in obliging controllers and operators to

	adopt specific measures to prevent and manage incidents. These measures include risk assessments as well as mitigation and controls that are implemented on the basis of risk assessments. Organisations cannot be obliged to guarantee absolute security of data processing activities; rather, they must implement security measures that are appropriate to the risk of any anticipated potential harms, as determined by risk assessments. Security management is a complex task relying on a wide range 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. In addition, the risk of human error can never be fully excluded; it can only be reduced through training. **Therefore, the ANPD regulation on security incidents must be flexible to account for the specific contexts and varieties of any security incidents, and must <u>not</u> be prescriptive or expect organisations to implement any specific methodology, especially since risks may vary over time and methodologies may have to evolve with the changing risk landscape. The ANPD could, rather, provide examples to organisations** of (i) what could be potential risks and harms resulting from various types of security incidents, (ii) non-ehaustive criteria that controllers can use when assessing the level of risk involved in the security incident, and (iii) methodologies that are commonly used in the market for managing security incidents (see response to the question below on "Are there any recommended methodologies for assessing the severity of security incidents? Which ones?". This would allow the ANPD to create and facilitate as much consistency as possible, keeping in mind the context and sensitivity of individual risk assessments and the resulting need for flexibility. Regarding point (ii) in the paragraph above and the second part of this ANPD question, below is a non-exhaustive list of criteria that organisations commonly take into account when assessing the level of risk of a security incident: • Likelihood that harms to individuals will occur/materialise as a result of the incident – this is important to differentiate between incidents where the risks for the data subjects may be present but the likelihood of such risks or harms actually materialising is low, versus incidents where the risks are present and the likelihood of such risks or harms materialising is significant; • Severity of the possible harms to individuals (e.g., possible harms resulting from incidents where data is disclosed by accident to a trusted party are likely to be less severe than possible harms resulting from incidents where data is disclosed to the wider public); • The type of security incident (e.g., breach of confidentiality by a person with access to data, breaking into a system and therefore violating its integrity, making data unavailable to their legitimate users); • The nature and sensitivity of personal data (i.e., the more sensitive the data, the higher the risk of harm will be to the people affected, but consideration should also be given to personal data that may already have been made public by the data subject);

	• How easily individuals can be identified (e.g., if personal data was encrypted and the encryption key has not been disclosed, the risks are likely to be much lower); • Any special characteristics of the affected individual (e.g., data relating to children/other vulnerable individuals may result in a higher risk than data of adults); • Whether the same type of incident has happened in the past; and • The measures taken by the controller to mitigate the impact of the event. CIPL believes that linking the determination of whether the security incident should trigger notification to the number of potentially affected individuals could have unintended consequences. For instance, an incident that 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. The number of impacted individuals is not a good indicator of the actual harm or likelihood of harm that an individual may suffer as a result of a security incident. **The ANPD should therefore require organisations to undertake a risk assessment of the security incident taking into account the criteria listed above and any other relevant criteria to define whether they should notify the incident to the ANPD and to data subjects. Article 48 of the LGPD establishes that organisations should notify incidents that may result in risk or harms that are "relevant". When interpreting this requirement, the ANPD should consider as "relevant" only those risks and harms that are (i) material, and/or (ii) classified as high-risk under the controllers' risk assessment** (see response to the question below). It is necessary that the ANPD interpret the LGPD in a manner that ensures that the threshold of "relevant" risks and harms is set at the right level, so that organisations have to notify only those incidents where there is a likelihood of material harm to individuals and where they classify as high-risk. CIPL has added below some practical examples of incidents that are non-material and not high-risk and therefore should not be considered as notifiable: • An employee has incidental access to a document related to a recruitment process. Although the document may contain personal data that, if exposed more broadly, could create the risk of adverse consequences to the data subject (for instance, in terms of relationship with the current employer), the likelihood of such risk materialising is low because the member of staff is bound by confidentiality requirements and has notified internally his or her incidental access with a committment to deleting the document. • Some personal data (like photographs, information about professional promotions, etc.) have unintentionally been made available through access to a temporary but shareable URL link to content in an internal communication tool. Although it cannot be completely excluded that such link could be used by an unauthorised person to access such content, the likelihood of this risk occuring is minimised by the temporary

validity of the link as well as moderation measures limiting the nature of the content shared in the tool. In addition, potential harms to individuals did not materialise.

- Invoices including details of individualised transactions (e.g., date, time and location of purchase) are erroneously shared in a business-to-business context. Although the information contained in the invoice could potentially lead to the identification of customers, such process would require a matching effort and access to external data sets. In addition, the merchant is bound by confidentiality obligations and commits not to make any further use of such information.

Should the risks or relevant harms be divided into categories (e.g., low, medium, high, etc.)? How can these levels be distinguished? Should low risks or harms be considered relevant or not relevant?

Organisations use a variety of methodologies to undertake risk assessments. Larger organisations normally categorise the levels of risk when undertaking risk assessments, including assessments that relate to security incidents. These categories can range from, most commonly, low-risk/medium-risk/high-risk, and some organisations also use extra categories such as no-risk/very-high-risk/very-low-risk. There are a number of methodologies that organisations follow to measure the level of risk associated with these categories. Larger organisations may also make use of tools that enable them to apply a scoring to each of these categories and objectively calculate the final score of an event being measured using specified criteria (such as the criteria outlined in our response to the question above). Some organsations also utilise a risk matrix such as the one shown below. As mentioned in our response to the question above, CIPL recommends that only those risks that are classified as high-risk should be considered notifiable.

Below is an example of a likelihood and severity matrix that organisations use to assess the risks involved in security incidents:

LIKELIHOOD OF HARM OCURRING SEVERITY OF HARM	HIGH LIKELIHOOD	MEDIUM LIKELIHOOD	LOW LIKELIHOOD
HIGH SEVERITY	High likelihood High severity	Medium likelihood High severity	Low likelihood High severity
MEDIUM SEVERITY	High likelihood Medim severity	Medium likelihood Medium severity	Low likelihood Medium severity
LOW SEVERITY	High likelihood Low severity	Medium likelihood Low severity	Low likelihood Low severity

The ANPD should <u>not</u> mandate that organisations use specific methodologies or tools to assess risks relating to security incidents. The ANPD should leave it to the organisations to decide which risk assessment methodologies and

	tools are most appropriate to the context of the organisation, as long as organisations can demonstrate that they have appropriately assessed the risks (e.g., smaller organisations may choose to assess risks informally based on questions and internal expertise while larger organisations may implement more complex tools and even tie these assessments to their overall enterprise risk management function). Controllers should have the ability (but not the obligation) to build risk matrixes that work for their organisation. It could be helpful, especially for smaller organisations, for the ANPD to provide a checklist or a list of questions that would indicate whether an incident is notifiable (e.g., Has the incident resulted in concrete and material harms to individuals? Has it involved sensitive personal data or personal data relating to vulnerable individuals?). The ANPD could also elaborate a tool that organisations can use to assess the risks (e.g., a spreadsheet with a scoring system), making it clear that this tool is optional and that organisations may develop their own, or use outsourced, tools/methodologies. The ANPD could also provide examples of what are risks and harms that organisations can consider, as well as case studies involving notifiable and non-notifiable incidents.
How can risks to data subjects be distinguished from harms to data subjects? How are these concepts related?	Risks are the probability or possibility of a harm happening. Where there is a risk of harm, actual harm may materialise. As explained in the question above, harms can be material or non-material/tangible or intangible. A security incident can reveal the existence of (i) a significant risk, in which case the harmful event remains latent, or (ii) harms to individuals, in which case there is sufficient evidence that the event has already produced its harmful results. Although the concepts of "risk" and "harm" are separate, they are intrinsically related for the purposes of risk assessments.
What should be considered in the risk assessments of incidents?	See response to the first question above on "When can an incident result in risks or relevant harms to data subjects? What criteria should the ANPD take into account to consider the risks or harms as relevant?"
Which information should controllers provide to the ANPD beyond the information listed on Article 48, paragraph 8 of the LGPD?	Article 48, paragraph 1 of the LGPD establishes a sufficiently comprehensive list of information that controllers should provide to the ANPD and data subjects when notifying security incidents. It does not establish that the ANPD should require the provision of information beyond what is on this list. **CIPL recommends that the ANPD do <u>not</u> require providing specific additional information, but that it leave it for controllers to decide whether providing additional information would be helpful on a case-by-case basis**, in particular when notifying the incident to the ANPD and cooperating with a possible ANPD investigation. Such additional information could relate to, for instance, the complexities of an incident of global reach involving multiple jurisdictions and/or additional third parties.
What is a reasonable deadline for controllers to notify the ANPD about security incidents? (Article 48, paragraph 1 of the LGPD)	Article 48, paragraph 1 of the LGPD establishes that controllers should communicate "within a reasonable timeframe" to the ANPD and to data subjects such security incidents that may result in relevant risks or harms to data subjects, and that the ANPD may define this timeframe. The ANPD regulation should set out clear notification thresholds especially for small-scale incidents and avoid setting a low threshold for notification. Incident notification may 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.

	The ANPD may be tempted to follow the 72 hours/three days-standard established by Article 33 of the EU General Data Protection Regulation (GDPR). It is important, however, that the ANPD acknowledge that not all GDPR provisions are realistic. The ANPD does not need to follow the EU examples in every instance, but rather should only follow those examples that are effective and provide the highest level of protection to individuals, considering also the particularities of the Brazilian context—see the Hunton Andrews Kurth's report on Seeking Solutions: Aligning Data Breach Notification Rules Across Borders, which highlights key differences and opportunities for convergence in existing data breach notification regimes around the globe. 72 hours or three days (or even two days as provisionally recommended by the ANPD on its website) is not enough time for an organisation to fully understand the scope and extent of a security incident and therefore define whether it should be notified. Because of this, in the EU organisations will often preemptively notify a data protection authority of a data breach just to stop the clock, which results in over-notification and the associated cost to time and resources (see CIPL's contribution from the Multistakeholder Expert Group to the Commission 2020 Evaluation of the GDPR, page 36). In fact, fixed timelines for notification of security incidents can have a number of unintended consequences: • Rushing notifications for fear of sanctions before a full assessment of the events can be performed resulting in over-notification of incidents to the ANPD, including notification of incidents that are incidental and that end up entailing only a low or medium-risk. Rushed and pre-mature notification also does not promote good accountability practices of those 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; • Creating a false sense of urgency that may inadvertently result in a situation in which the notification has to be supplemented or rectified as the assessment evolves; • Shifting resources from containing and mitigating the incident to notifying it (which is particularly relevant for small and medium-size organisations that have limited resources); and • Creating the risk of liability for the organisation even where it is acting with the greatest standard of diligence and care. Allowing organisations more time to actually understand what has happened, assess the true risk of the incident, and deal with it appropriately will mean that the ANPD will be provided with better quality reports and will likely receive fewer notifications, as controllers will have more certainty on whether or not to notify the incident. 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. Also, a credible risk assessment includes a detailed forensic analysis to determine the likelihood and severity of harm to individuals and assess whether a security incident is reportable. In the more complex scenarios, and in particular those that involve sophisticated external attacks,

	investigations may 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. See for instance the 2020 BakerHostetler Data Security Incident Response Report, which showed the time from incident discovery to notification to take an average of 38 days. The 2020 Verizon Data Breach Investigations Report indicates that data breaches take months or longer to discover on large organisations while this time is smaller in small organisations. CIPL therefore supports the existing standard of the LGPD that does not establish a fixed term for the notification of security incidents and, rather, places the onus on the controller to ensure that the notification is issued in a timely manner appropriate to the nature and level of risk involved in the incident. **CIPL recommends that the ANPD (i) maintain the existing LGPD standard of an open but "reasonable" deadline, while (ii) providing additional guidance and examples (i.e., use cases) to illustrate when an organisation becomes "aware" of an incident, what would be considered timely notifications, and how organisations can demonstrate that they have complied with this timeline while taking measures to effectively contain and remediate the incident**. If the ANPD decides not to incorporate this suggestion, CIPL suggests that at a minimum the timeline for notification should be 3 working days from the moment the organisation becomes aware of the incident, factoring in working/business days. The ANPD should also provide guidance concerning what it means to become "aware" of the incident and therefore where the clock starts ticking for them to notify the ANPD. Rather than requiring notification within a reasonable timeframe counting from the awareness of the incident, **CIPL recommends starting the clock from when an incident has been (or reasonably should have been) confirmed coupled with clear guidance as to what level of reasonable certainty that controllers should have that the incident has actually occurred**. In addition to this, the ANPD should consider that the same people who have to mitigate security incidents are also the ones who have to provide information necessary for reporting. Thus, the ANPD should not prioritise reporting over remediation, as this could ultimately be worse for data subjects. This is even more relevant for smaller entities that have fewer resources.
What is a reasonable deadline for controllers to notify the data subjects about security incidents? (Article 48, paragraph 1 of the LGPD) What information should they provide in this notification? The same information as listed in Article 48, paragraph 1 of the LGPD?	See previous question for considerations on the reasonable deadline for notification. The same considerations apply in relation to communication to individuals. In particular, **CIPL recommends that the ANPD requires controllers to notify data subjects "on a reasonable timeframe" only where there has been a confirmation that data subjects are at risk of material privacy harm that has been classified as high-risk, and the controller is in a position to advise on steps the data subjects can take to protect themselves** (i.e., to reduce the risk of harm). This would avoid "notification fatigue" that could result of constant notifications about incidents that are inconsequential. Constant or fequent notifications would, in fact, undermine the protection of individuals as it would undermine their ability or even willingness to continually differentiate between situations that require action on their part to protect themselves from situations in which the risk of harm is trivial and no action is required. A phased communication could also be reasonable provided that it does not overwhelm or cause unnecessary anxiety to data subjects. In cases where data subjects need to be

	informed so that they can take mitigating actions themselves, it makes sense to notify them sooner rather than later, so long as it is feasible to do so. Regarding the content of the communication, the information listed in Article 48, paragraph 1 of the LGPD is sufficient. This content and style of this notification should not, however, be the same as the content of the notification to the ANPD as they serve different purposes. Any mandatory requirements in terms of the content of the notification should be interpreted flexibly and not understood as a requirement to quote the LGPD. The ANPD should thus provide the following guidance to controllers: • The communication should be written in clear, plain and simple language, avoiding technical and legalistic terms, should be concise and provided in a user-friendly manner (e.g., the ANPD could recommend a layered approach for data subjects to obtain further information if they wish); • The communication should be independent from other communications issued by the controller (e.g., a specific email rather than part of an email with offers of products and services); • The communication should avoid alarming language and should focus on the measures that data subjects can take to further protect themselves; and • They should limit the information provided regarding the mitigation measures that were or will be adopted to a level that is useful to individuals (note that providing a lot of detail may open doors for malicious actors to circumvent remediation plans). Whichever the case, the communication requirement should not be utilised as a means to penalise the controller that suffered a security incident (e.g., by harming its public reputation). The focus of the communication should remain the affected individual and its content limited to the information which is useful to further protect that individual and required in Article 48, paragraph 1.
What is the most appropriate way for notifying security incidents to data subjects? Should this communication always be direct and individual (e.g., via post, email, etc.) or, in determined circumstances, can this communication be public (e.g., notification via media, internet publication, etc.)?	There is no standard/one-size-fits-all approach for notifying security incidents to data subjects. Controllers are best placed to know how to most effectively communicate with their users/data subjects and may have their own ways of effecting such communications. The effectiveness of communication should be the main criterion for notification, rather than a pre-determined format. Preferably, the notification should follow the method with which the controller regularly interacts with the data subject. **CIPL recommends that the ANPD (i) do <u>not</u> require a specific type of notification, but rather provide examples to controllers of how they can notify data subjects, and (ii) acknowledge that the efforts involved in the notification must be appropriate to the level of risk and the specific circumstances of the case**. The ANPD should inform controllers that they should choose the most appropriate type of notification to achieve the goal of informing individuals of the incident and allowing individuals to take any necessary measures (e.g., change their passwords) to further protect their personal data. Some examples include:

	• When data subjects are identified/individualised and the controller has a direct relationship with them:
	  ○ Letter sent by post;
	  ○ Email;
	  ○ SMS;
	  ○ In-app or platform notification (e.g., pop-ups or banners).
	• Exceptionally, the ANPD should allow for public notifications when (i) data subjects are not identified/individualised, (ii) the controller does not have a direct relationship with them, (iii) the regular means of communication have been rendered unaccessible as a result of the incident (e.g., data subject lost access to email), (iv) identifying and notifying individuals would involve a disproportionate effort (e.g., involving prohibitive costs), and (v) notification must be urgent due to the high-risk character of the specific incident. Examples include:
	  ○ Post on website; and
	  ○ Communications through media channels (such as relevant news websites and TV).
	In addition, the ANPD should consider that there may be instances where data subjects are identified, but it is not possible to notify all of them (e.g., where email accounts have been closed or the individual moved addresses and did not update their new address on the controller's system). A public notification may not be adequate in these cases, as it would only serve to cause more anxiety than it would provide information to impacted individuals. In those instances, the ANPD should <u>not</u> require the controller to publicly communicate the incident.

What could be the exemptions to notify the ANPD?	Controllers should not be required to notify to the ANPD security incidents which/where: • Are unlikely to result in a high-risk of actual harm to individuals according to the risk methodology applied by the controller (see response to the first question); • Involve solely non-personal data (including anonymous data), as the LGPD covers only the protection of personal data; • Involve personal data that has been rendered unintelligible or unidentifiable prior to the incident and there is no risk of data being re-identified (e.g., encryption where the key has not been disclosed, anonymous data); • Involve the unintended disclosure of personal data solely to a trusted third party; and • Immediately following the incident the controller has taken mitigation actions/measures that ensure that the level of risk required to trigger notification to affected data subjects is no longer present.

What could be the exemptions to notify data subjects?	In addition to the exemptions listed above, controllers should not be required to notify to data subjects security incidents which/where: • Have been effectively mitigated by the controller after it has become aware of the event and therefore no longer presents risks of harms to data subjects; • Risks and harms to individuals are unlikely to materialise; • Involve solely personal data that is already in the public domain; • Issuing such notifications would impede a criminal investigation; and • One of the joint-controllers in a data processing relationship does not have the data subjects' identifying information (e.g., credit card network operators that are joint-controllers with credit card issuers would only have the credit card numbers without identifying data). In these cases, the ANPD should not require this joint-controller to notify data subjects. Rather, this should be the responsibility of the other joint-controller that has the data subjects' identifying information.
What criteria should the ANPD adopt when assessing the severity of security incidents? (Article 48, paragraph 2 of the LGPD)	See response to the first question above on "When can an incident result in risks or relevant harms to data subjects? What criteria should the ANPD take into account to consider the risks or harms as relevant?"
Are there any recommended methodologies for assessing the severity of security incidents? Which ones?	The three mostly used methodologies for assessing security incidents and managing risks relating to data processing are: • European Union Agency for Cybersecurity (ENISA), Recommendations for a methodology of the assessment of severity of personal data breaches, 20 December 2013; • International Organization for Standardization (ISO), ISO 31000 – risk management; and • National Institute of Standards and Technology (NIST), NIST Privacy Framework: a Tool for Improving Privacy Through Enterprise Risk Management, version 1.0, 16 January 2020. Brazilian organisations should, nevertheless, have the ability to build an incident management process that suits their structure, nature of business and overall risk management frameworks. Methodologies for assessing the severity of security incidents can be used as reference material and know-how but should not be treated as a mandatory component of an incident management process that is regarded as compliant with LGPD.
What measures can the ANPD require, including technical and administrative measures, from controllers to adopt after they notify security incidents?	Article 48, paragraph 2, II of the LGPD provides that the ANPD may require controllers to adopt measures to reverse or mitigate the effects of the security incident. CIPL recommends, however, that rather than requiring controllers to take specific measures, the ANPD make recommendations of such measures or require controllers to define these measures and present them to the ANPD (e.g., in a document). This is because controllers will be better equipped to know which would be the most effective measures and would have a better understanding of the technical aspects involving the

	security incident. Similarly, in case the ANPD recommends (or ultimately requires) specific measures to be taken, controllers must be able to dispute such measures and propose more appropriate ones. **Controllers should therefore play a primarily role in determining the mitigating measures and the ANPD's role should be to provide an overall validation of the sufficiency of such remediation measures, taking into account the reasonable security requirements**. This is particularly relevant for controllers that are larger organisations. Measures that the ANPD may recommend include: • Taking rapid decisions to contain the incident, such as shutting down a system, isolating it from the network, and deactivating certain functions; • Measures intended to resolve certain effects of the security incident, such as eliminating malware or deactivating compromised accounts; • Data minimisation; • Measures aimed at completely restoring services to their normal levels and avoid, as far as possible, any new incidents occurring due to the same cause; • Measures to prevent similar incidents from happening in the future such as improving security systems and creation of internal policies and procedures, additional privacy and information security training, audits, addressing internal vulnerabilities, implementing an accountability/comprehensive data governance programme; • Evidence collection and custody to contain and reverse the impact of the incident; and • Documenting the incident and measures taken.
Further considerations concerning the management and notification of security incidents	• **The ANPD should take accountability into account as a mitigating factor when enforcing the LGPD following a security incident notification**—in particular in the cases where the controller has taken comprehensive and effective steps to contain and mitigate the risks and has been capable of demonstrating those while collaborating with the ANPD. Having a robust accountability framework within an organisation 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 operator due diligence, auditing practices and responding to a security incident. See for instance the CIPL Accountability Framework on the White Paper "The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society". • **A security incident is not an indicator of insufficient protection of personal data**—it is important that the ANPD understand that just because there has been a breach does not necessarily mean that the technical and organisational security measures put in place have been insufficient. Each incident and the security measures deployed need to be considered on their own merits. The ANPD should acknowledge that perfection is not the standard in information security. Industry security standards are meant as guideposts to make sure entities are

	managing risk appropriately. They should not be read prescriptively because doing so can actually diminish core security by sapping resources and losing focus on key risks. • **Operators should not be the ones to determine if a data breach notification should take place**—when the ANPD published the public consultation under discussion, it also published (i) a preliminary guide on data breaches where it established that "[a]lthough the responsibility and obligation for reporting to the ANPD lies with the controller, if information is exceptionally submitted by the operator, it will be duly examined by the ANPD"; and (ii) a template of the notification with a field to be marked by the notifying entity to inform whether it is the controller or the operator. Article 48, paragraph 1 of the LGPD is clear in providing that the controller must notify the ANPD about data breaches. Controllers, with support from their operators to the extent necessary, will be better equipped to fully assess the severity of a data breach and examine the potential impacts that it may cause to data subjects. Controllers should be the ones to determine whether the breach is to be notified to the ANPD and data subjects. In this regard, CIPL strongly recommends that the ANPD not suggest or imply that operators might have to notify the authority or data subjects. The ANPD could, rather, recommend that operators notify controllers of security incidents involving their personal data and cooperate to provide controllers with the relevant information as well as manage the incident. The ANPD could further recommend that this be included in the controller-operator contract. • **The ANPD should only proactively contact organisations after they have reasonable certainty that an incident is notifiable under their risk assessment mechanism**. The ANPD may receive complaints and questions from individuals concerning security incidents that they have become aware of through means other than a formal LGPD notification. Not all of these incidents may fall under the notification threshold that the ANPD will establish. The ANPD should not be tempted to follow-up on all of these cases, but rather only on those with respect to which it has reasonable certainty that it meets the notification threshold.
Recommended regulatory guidance and reference materials	Recommended regulatory guidance: • Irish Data Protection Commissioner, Guidance Note: A Practical Guide to Personal Data Breach Notifications under the GDPR, October 2019; • UK Information Commissioner's Office, guidance on personal data breaches; and • The European Data Protection Board is currently updating the Guidelines 01/2021 on Examples regarding Data Breach Notification and the ANPD should follow these developments. CIPL papers: • CIPL Response to the EDPB's Guidelines on Examples Regarding Data Breach Notification, 2 March 2021 • CIPL Comments on WP29's Breach Notification Guidelines, 1 December 2017

	• White Paper: Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR, 21 December 2016

SUGGESTIONS OF PROVISIONS
CIPL does not have suggestions.