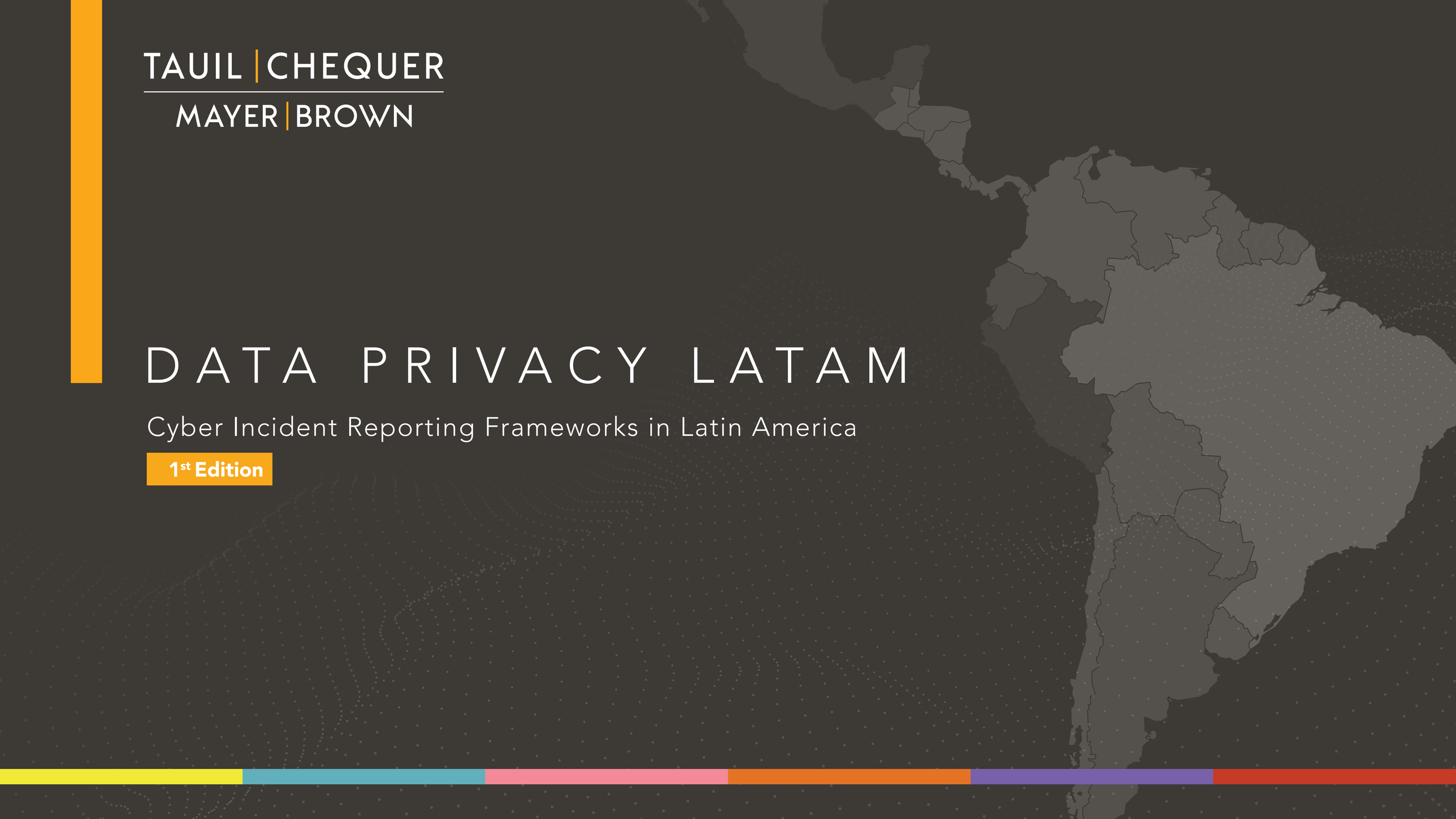
TAUIL | CHEQUER
MAYER | BROWN

DATA PRIVACY LATAM

Cyber Incident Reporting Frameworks in Latin America

1st Edition




MEXICO
COLOMBIA
BRAZIL
PERU
CHILE
ARGENTINA

BRAZIL

WHAT TRIGGERS NOTIFICATIONS?

Notification to the Brazilian Data Protection Authority (ANPD) and the data subjects: Data controllers are required to report any confirmed adverse event that affects any kind of personal data (any personal identifiable information), such as unauthorized access, destruction, loss, modification, leakage or any illegal data processing activity, as long as said events (i) are likely to put the data subjects at risk (mainly regarding their rights and/or freedoms) and/or (ii) cause any relevant damage to the data subjects. Risks are higher if the incident involves sensitive personal data (e.g., racial origin, trade union or political organization membership, data concerning health, sexual orientation or biometrics); involves vulnerable categories of data subjects (children, elderly people, etc.); or is likely to facilitate financial fraud, discriminatory behavior against the data subjects and/or identity theft or impact on data the subject's reputation and honor. The amount of data, how easily data subjects may be identified as per the personal data in question, territorial extension of the incident, and if the incident was intentionally caused by hackers are also criteria to determine whether the event is likely to put data subjects at risk. ANPD has yet to issue the definitive guidance regarding data breaches. Therefore, the triggers above are likely to be reviewed in near future.

Notification to the Brazilian Securities and Exchange Commission (CVM): If the company has stocks publicly traded in the Brazilian stock market or other securities traded at a Brazilian organized over-the-counter market entity, the company must report any event that is likely to affect stocks' price and/or investors' decisions on whether to buy or sell a company's stocks and/or to exercise any of their rights as shareholders. Controlling shareholders or company's officers are allowed to decide not to report the breach if such public notification affects company's legitimate interest.

MUST DAMAGE TO THE DATA SUBJECTS BE PROVEN TO TRIGGER NOTIFICATIONS AND/OR SANCTIONS?

Yes, according to Article 48 of the LGPD. However, the ANPD has yet to publish specific guidance on the topic.

WHICH COMPETENT AUTHORITIES AND SUBJECTS MUST BE NOTIFIED?

The ANPD and the data subjects. There is no distinction as to the triggers between the ANPD and the data subjects (e.g., higher level of risk). Also, some private agreements may require one party to notify the counter party if any data breach occurs. Also some other sectorial regulatory authorities may have to be notified, such as CVM, ANEEL, ANATEL and BACEN.

WHO HAS THE NOTIFICATION OBLIGATION?

The data controller is required to report any breach. Therefore, in an incident involving a vendor or other third party, analysis is required to determine which entity is the data controller responsible for providing the relevant notifications.

HOW QUICKLY MUST THE NOTIFICATION BE MADE?

Notification to the ANPD and the data subjects: **Two business days from the time the data controller becomes aware of the breach**. The ANPD may review this term in the near future.

ARE DELAYS IN NOTIFICATION PERMISSIBLE? IF SO, WHAT ARE THE POSSIBLE JUSTIFICATIONS FOR THE DELAY?

Delays in notification to the ANPD and the data subjects may be permitted and as long as the delay was necessary in order to remediate an incident and determine its scope and the controller is able to thoroughly evidence to the ANPD the reason for the delay.

IS THERE ANY GUIDANCE OR RESOLUTION FROM THE COMPETENT AUTHORITIES ABOUT WHAT MUST BE IN A DATA BREACH ANALYSIS?

There's no specific ANPD guidance or resolution about data breaches.

POINTS OF CONTACT FOR DATA BREACHES NOTICES

Brazilian Data Protection Authority (ANPD) – https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca

ARGENTINA

WHAT TRIGGERS NOTIFICATIONS?

It is highly recommended to report the incident to the Argentinean Data Privacy Agency , although it is not mandatory. While data breach notifications are not required, agencies are required to keep records of data breaches in case they are requested during an investigation or audit.

The Argentinean Data Privacy Law of 2000 establishes that security shall be guaranteed within the processing of data. To this extent, security also includes the avoidance of any loss of information/date.

According to the Data Privacy Law and its implementing rules, it is not mandatory to report a breach of security or incident.

However, the Argentinean Data Privacy Agency issued in 2018 Resolution 47/2018, where several security measures were recommended, including notifying the agency of security incidents. Therefore, reporting information security incidents is more a "best practice" than a legal obligation.

However, in a quite recent case (AR Data Privacy Agency v. Cencosud SA) the local authority imposed an administrative fine of ARS 290,000.00 (approximately, USD 3000) based on the facts that Cencosud had a breach of security that became publicly known and the company did not take the recommended measures to prevent, notify and remedy the effects of such a breach nor did the company notify the clients/users whose data had been breached.

Resolution 47/2018 of the Argentinean Data Privacy Agency establishes that any security incident should be notified: "G - Security incidents - Related to the treatment of events and consequent security incidents that may affect personal data, their detection, evaluation, containment and response, as well as escalation activities and correction of the technical and operational environment."

MUST DAMAGE TO THE DATA SUBJECTS BE PROVEN TO TRIGGER NOTIFICATIONS AND/OR SANCTIONS?

No, as explained in the previous column, any security incident can be notified as a good practice.

WHICH COMPETENT AUTHORITIES AND SUBJECTS MUST BE NOTIFIED?

1) Authorities:

The AAIP National Data Protection Agency (NDPA) that works under the Public Information Access Agency (AAIP)

2) Subjects (while not mentioned in the resolution, notification can be considered a general duty to prevent damage, according to the Civil and Commercial Code, and the NDPA can audit the company's notification-to-subjects system).

WHO HAS THE NOTIFICATION OBLIGATION?

Neither law No. 25,326 nor Resolution 47/2018 specify this. But, as the responsibility for data security (art. 9) and administrative sanctions (art. 31) falls on the data controller and the processor, it can be inferred that the notification obligation falls on them as well.

HOW QUICKLY MUST THE NOTIFICATION BE MADE?

There is no specific deadline. As it is not mandatory to even notify, it is also not mandatory to do so by a certain time.

ARE DELAYS IN NOTIFICATION PERMISSIBLE? IF SO, WHAT ARE THE POSSIBLE JUSTIFICATIONS FOR THE DELAY?

Yes, seeing as there is no deadline.

IS THERE ANY GUIDANCE OR RESOLUTION FROM THE COMPETENT AUTHORITIES ABOUT WHAT MUST BE IN A DATA BREACH ANALYSIS?

The notification should contain a report on the breach, identification of the affected users, measures taken to mitigate the incident and measures that will be applied to avoid incidents in the future. (From **Resolution 47/2018**, titled "*Medidas de seguridad recomendadas para el tratamiento y conservación de los datos personales en medios informatizados.*")

POINTS OF CONTACT FOR DATA BREACHES NOTICES

incidente.seguridad@aaip.gob.ar

CHILE

WHAT TRIGGERS NOTIFICATIONS?

There is no notification obligation since there is no data protection authority in Chile and the law does not establish this requirement.

However, there is a legislative initiative, a bill that regulates the protection and processing of personal data and creates the Agency for the Protection of Personal Data: Bulletin 11,144-07, consolidated with Bulletin 11,092-07 (Data Protection Bill). Though there is no clear timeline for when to expect this bill to pass, companies should follow its progress.

The Data Protection Bill establishes mandatory notification for when the data breach (i) causes accidental or illicit destruction, filtration, loss or alteration of the processed personal data or (ii) involves unauthorized communication or access to this personal data when there is a reasonable risk to the rights and freedoms of the data subjects.

When data breaches involve sensitive personal data; data relating to children under the age of 14; or data relating to economic, financial, banking or commercial obligations, there must also be a notification to the data subject. This notification must address every affected data subject, and be made in clear and simple language, identifying the personal data affected, the possible consequences of the breach and protective measures taken.

MUST DAMAGE TO THE DATA SUBJECTS BE PROVEN TO TRIGGER NOTIFICATIONS AND/OR SANCTIONS?

Not applicable, seeing as there is no notification obligation.

And, under the Data Protection Bill's perspective, no. That is because only in a situation that meets the second criteria is proof of damage to the data subject needed.

WHICH COMPETENT AUTHORITIES AND SUBJECTS MUST BE NOTIFIED?

Not applicable, seeing as there is no notification obligation.

However, a special data protection authority is to be created by the Data Protection Bill—the Data Privacy Agency. This will be the Chilean authority responsible for receiving breach notifications. Though, as noted, there is no clear timeline for when to expect this bill to pass.

WHO HAS THE NOTIFICATION OBLIGATION?

Not applicable, seeing as there is no notification obligation at this moment nor good, specific practice recommendations on the matter.

The Data Protection Bill establishes the notification obligation for the controller and the processor.

HOW QUICKLY MUST THE NOTIFICATION BE MADE?

Not applicable, seeing as there is no notification obligation. It is also not specified in the Data Protection Bill.

ARE DELAYS IN NOTIFICATION PERMISSIBLE? IF SO, WHAT ARE THE POSSIBLE JUSTIFICATIONS FOR THE DELAY?

Not applicable, seeing as there is no notification obligation. It is also not specified in the Data Protection Bill.

IS THERE ANY GUIDANCE OR RESOLUTION FROM THE COMPETENT AUTHORITIES ABOUT WHAT MUST BE IN A DATA BREACH ANALYSIS?

No.

POINTS OF CONTACT FOR DATA BREACHES NOTICES

Not applicable.

COLOMBIA

WHAT TRIGGERS NOTIFICATIONS?

Law 1581 of 2012 requires both the data controllers and processors to notify the CDPA in case of violations of security codes or the existence of risks associated with the processing of the personal data of data subjects (Article 17, "n" and Article 18, "k").

Chapter V of the Single External Circular of CDPA defines a "security incident" as "the violation of security codes or the loss, theft and/or unauthorized access of information from a database managed by the Data Controller or its Processor." Another definition, from the non-binding Accountability Guidelines of the CDPA: "any incident in the information systems or in manual or systematized databases that threatens the security of the personal data stored in them."

The aforementioned guidelines make no distinction concerning the security incidents that need to be reported to the CDPA. Therefore, regardless of their impact on data subjects, all security incidents must be reported to the CDPA.

MUST DAMAGE TO THE DATA SUBJECTS BE PROVEN TO TRIGGER NOTIFICATIONS AND/OR SANCTIONS?

No, the mere occurrence of a security violation that affects them triggers notification. The CDPA has indicated in the Accountability Guidelines that Law 1581 of 2012 does not make any distinction regarding the impact of the security incident that triggers the obligation to report to the CDPA. Therefore, regardless of their impact, all security incidents must be notified to the CDPA. Likelihood of risks on data subjects' rights and/or freedoms are not taken into account by the CDPA.

WHICH COMPETENT AUTHORITIES AND SUBJECTS MUST BE NOTIFIED?

1) The Delegatura para la Protección de Datos Personales from the Superintendencia de Industria y Comercio (SIC), or Superintendence of Industry and Trade (which is the Colombian data protection authority, "CDPA").

2) The data subjects affected (not mandatory under Law 1581 of 2012 but recommended under the non-binding Accountability Guidelines of the CDPA).

WHO HAS THE NOTIFICATION OBLIGATION?

The controller if it is obligated to register the database in which the security incident occurred at the National Databases Registry.

If the controller is not obligated to register the database in which the security incident occurred, the report shall be made by both the controller and the processor.

HOW QUICKLY MUST THE NOTIFICATION BE MADE?

15 business days.

ARE DELAYS IN NOTIFICATION PERMISSIBLE? IF SO, WHAT ARE THE POSSIBLE JUSTIFICATIONS FOR THE DELAY?

Chapter V of the Single External Circular of CDPA sets forth that the notification should be made within 15 business days "following the date [the incident] was detected and brought to the attention of the person or area in charge of assisting them," which should be the data protection officer or area of the company.

The delay in the detection and knowledge of the incident by the data protection officer or area could be used as a justification for the delay in the report to the CDPA.

IS THERE ANY GUIDANCE OR RESOLUTION FROM THE COMPETENT AUTHORITIES ABOUT WHAT MUST BE IN A DATA BREACH ANALYSIS?

Yes, the non-binding Accountability and the Managing Security Incidents guidelines of the CDPA would serve this purpose.

POINTS OF CONTACT FOR DATA BREACHES NOTICES

Registro Nacional de Base de Datos, the National Data Base Registry.

https://www.sic.gov.co/preguntas-frecuentes-rnbd

https://www.sic.gov.co/sites/default/files/files/Manual-de-Usuario-5-RNBD-01032017.pdf

MEXICO

WHAT TRIGGERS NOTIFICATIONS?

There must be a report when data vulnerabilities significantly affect the rights of the holders, patrimonial or extrapatrimonial.

Examples of "vulnerabilities" are unauthorized loss or destruction; theft, loss or unauthorized copying; unauthorized use, access or processing, damage, unauthorized alteration or modification.

MUST DAMAGE TO THE DATA SUBJECTS BE PROVEN TO TRIGGER NOTIFICATIONS AND/OR SANCTIONS?

Yes.

WHICH COMPETENT AUTHORITIES AND SUBJECTS MUST BE NOTIFIED?

All affected subjects must be notified.

Notifying the *Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales* (the National Institute of Transparency, Access to Information and Protection of Personal Data or "INAI") is mandatory for entities in the public sector. For the private sector, although it is not mandatory to notify the INAI, it is considered good practice.

WHO HAS THE NOTIFICATION OBLIGATION?

The controller.

HOW QUICKLY MUST THE NOTIFICATION BE MADE?

There is no specific deadline, only "without undue delay."

ARE DELAYS IN NOTIFICATION PERMISSIBLE? IF SO, WHAT ARE THE POSSIBLE JUSTIFICATIONS FOR THE DELAY?

This is not applicable as there is no deadline. It is only necessary that the notification be done promptly, without unnecessary delay.

IS THERE ANY GUIDANCE OR RESOLUTION FROM THE COMPETENT AUTHORITIES ABOUT WHAT MUST BE IN A DATA BREACH ANALYSIS?

Yes, the Recommendations For Handling Personal Data Security Incidents, which can be found here: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/Recomendaciones_Manejo_IS_DP.pdf.

POINTS OF CONTACT FOR DATA BREACHES NOTICES

INAI can be contacted through their website: https://home.inai.org.mx/

PERU

WHAT TRIGGERS NOTIFICATIONS?

Emergency Decree No. 007-2020, which has approved the Digital Trust Framework, requires that digital service providers report any security incident for entry in the National Registry of Digital Security Incidents.

The decree describes a Digital A security incident as "an event or series of events that can compromise trust, economic prosperity, the protection of people and their personal data, information, as well as other assets of the organization, through digital technologies."

Under the aforementioned decree, a digital service provider is any public entity or private sector organization, regardless of its geographic location, that is responsible for the design, provision, and/or access to digital services in Peru.

Note: Law No. 29733 - Personal Data Protection Law and its regulations do not require incidents affecting the integrity of the data to be reported. Article 6 requires that personal data collected online, through electronic communications networks, is processed solely for the purpose publicly disclosed by the company via its privacy notice, i.e. preventing the loss of personal data.

MUST DAMAGE TO THE DATA SUBJECTS BE PROVEN TO TRIGGER NOTIFICATIONS AND/OR SANCTIONS?

No. According to Article 9 of Emergency Decree No. 007-2020, section "9.1", "a," any security incident must be reported.

The occurrence of a digital security incident that involves personal data, triggers an obligation to report according Article 9. e) of Emergency Decree No. 007-2020 regardless of whether the incident has caused damage to the data subjects.

WHICH COMPETENT AUTHORITIES AND SUBJECTS MUST BE NOTIFIED?

a) For companies in the banking sector (mandatory):

Authority of Banks, Insurance and Pension Fund Administrators

b) For providers of internet use, digital services in the financial sector, public administration entities, essential services (electricity, water and gas), health and transportation of persons, educational services (recommended, according to Decree on Digital Trust):

The Peruvian National Digital Security Center.

c) For digital service providers (according to Decree on Digital Trust):

The Peruvian National Digital Security Center.

The Peruvian ANPD.

2) For data subjects: They are advised to report when a data breach "affects their property or their moral rights."

3) Third parties: They are advised to report depending on each case, according to the subjects' specific characteristics and/or companies that may be directly or indirectly affected.

WHO HAS THE NOTIFICATION OBLIGATION?

The data base owners.

HOW QUICKLY MUST THE NOTIFICATION BE MADE?

To data subjects: As soon as data breach is confirmed (according to the Security Directive security measures recommendations).

No concrete deadlines are provided for other notification requirements.

ARE DELAYS IN NOTIFICATION PERMISSIBLE? IF SO, WHAT ARE THE POSSIBLE JUSTIFICATIONS FOR THE DELAY?

Yes, as there is no official deadline. In cases of delay, a reasonable technical difficulty can be argued.

IS THERE ANY GUIDANCE OR RESOLUTION FROM THE COMPETENT AUTHORITIES ABOUT WHAT MUST BE IN A DATA BREACH ANALYSIS?

Not specifically, however we suggest referring to the "Security Directive National Authority for the Protection of Personal Data APDP.". First Edition, November 2013. Ministry of Justice and Human Rights (Source: https://cdn.www.gob.pe/uploads/document/file/1401560/Directiva%20de%20seguridad.pdf).

POINTS OF CONTACT FOR DATA BREACHES NOTICES

Centro Nacional de Seguridad Digital.