Global Data and Cyber Handbook - Argentina

Security Requirements and Breach Notification

| Contents |
| --- |
| To generate table of contents, right-click here and select **Update Field.** |

# Do data privacy laws or regulations impose obligations to maintain information security controls to protect personal data from unauthorized access or processing?

*Last reviewed: 2 December 2024*

Yes.

☒       general obligation to take appropriate / reasonable technical, physical and/or organizational security measures
☒       other

DPA Resolution No. 47/2018 provides the recommended security measures for the processing and conservation of personal data in computerized and non-computerized media, such as the necessary confidentiality measures to guarantee effective control of access, backups and recovery systems and detection of possible security breaches, among others.

# Do other laws or regulations impose obligations to protect systems from cyberattack?

*Last reviewed: 2 December 2024*

☒       public company obligations (e.g., duties to maintain sufficient information security measures or ensure operational resilience to cyberattacks)

☒       financial services requirements

☒       telecommunication requirements

☒       providers of critical infrastructure

Resolution No. 580/2011 creates the National Program on Information and Cybersecurity Critical Infrastructure and Resolution No. 1523/2019 defines Critical Infrastructure.

The National Communications Entity issued the "Regulation for the Collection of Personal Data and Identity Validation of Users of Mobile Services that Hold a Mobile Number" that requires mobile services providers to adjust their existing protocols for the registration of new mobile numbers and for changes of certain conditions in which the services are provided. This means implementing new guidelines for the collection of personal data and identity validation of users to mitigate risks of fraud and impersonation.

The Argentine Central Bank issued Communication 'A' 7724, which updated the technology and information security risk standards to strengthen the cyber resilience of financial institutions. Generally, the Argentine Central Bank aims for regulated financial institutions to develop and implement governance programs that include, among other things: (i) risk identification and management; (ii) design of internal policies and procedures; (iii) continuous evaluation and audit of policies to identify and correct errors; (iv) internal awareness and training; and (v) proper documentation and backup of data and information, as well as of any security incident or event.

# Has there been regulatory activity – including enforcement action, investigations, regulatory guidance or other public statements by the regulator – relating to cybersecurity by the following regulators in the last 12 months?

*Last reviewed: 2 December 2024*

☒  Data privacy

☒  Securities or public company

☒  health

☒  financial services

☒  telecommunications

# Does data privacy or cybersecurity law impose obligations to make notifications about personal data security breaches?

*Last reviewed: 2 December 2024*

**No**

However, DPA's Resolution No. 47/2018, which sets forth the "Recommended security measures for the processing and retention of personal data in computerized and non-computerized media," refers to security incidents and recommends the preparation of a report including, at least, the following information: (i) nature of the incident; (ii) category of personal data affected; (iii) identification of affected users; (iv) measures adopted to mitigate the breach, and (v) measures adopted to prevent future incidents. It also recommends notifying the DPA of the security incident and attaching the aforementioned report. *There is no timeframe provided to send the mentioned notice to the DPA.*

Also, DPA's Resolution No. 332/2020 includes legal and technical guidelines to be considered by inspectors when carrying out the inspection of personal data processing activities. The implementation of an incident notification notice to the DPA and the data subjects will be considered when conducting an inspection. It will also be considered if the individual or entity responsible for the database implements, among others, *an incident notification system* to the DPA and data subjects.

The Personal Data Protection Bill of Law introduced in Congress includes the obligation to report to data subjects and the DPA certain security incidents within 72 hours of acquiring effective knowledge. A similar approach is followed under other Bills of Law being discussed in Congress.

# Controllers/Owners have to notify:

*Last reviewed: 2 December 2024*

N/A

# Processors/Agents have to notify:

*Last reviewed: 29 December 2023*

N/A

# Are there any additional sector-specific or non-personal data security breach notification requirements?

*Last reviewed: 2 December 2024*

**☒ Yes**

☒      public company obligations (e.g., to notify security incidents that may materially affect an investor's decision)
☒       financial services requirements
☒      other

**If so, please provide brief details of the relevant law / guidance and indicate which body/bodies must be notified of the breach.**

Some sector-specific regulations are not explicitly clear as to the obligation to report a data security breach.

Although the National Securities Commission (*Comisión Nacional de Valores*, or CNV) regulations do not define or refer to "security breach," they establish that every act or situation that, due to its importance, is able to substantially affect the placement of negotiable securities, the course of their negotiation, or the development of the activity of who suffered the event, must be reported to the investors and the CNV (Title XII, Chapter I, Section II of the CNV framework). There is no specific timeframe established to inform investors and the CNV. The regulations only provide that the notification should be done immediately upon acknowledgment of such breach.

Moreover, the Argentine Central Bank issued Communication "B" No. 11847 related to technology and systems incidents, which sets forth that financial entities must report to the External Systems Audit Management (*Gerencia de Auditoria Externa de Sistemas)* when financial information or customer personal data is compromised.

In addition, Communication "A" No. 7266 of the Argentine Central Bank establishes that financial entities, payments service providers, and financial market infrastructures must report relevant information on cyber incidents to the authorities as required and in accordance with the timeframes established by applicable laws.

Communication "A" No. 7724 of the Argentine Central Bank establishes that financial institutions must implement effective control and management practices in accordance with the complexity of the financial services offered and the technology used. In this sense, among other obligations, they must develop cyber incident management policies, including roles and responsibilities of the areas involved in their response, and keep a complete record of the cyber incidents suffered in such a way that allows the identification, traceability and evidence of the actions taken until their closure. In terms of communication and notification, they should establish effective procedures for a timely and planned response, as well as designate a point of contact for reporting cyber incidents and mitigating the impact in a timely manner.

Copyright © 2025 Baker & McKenzie. All rights reserved. **Ownership:** This documentation and content (Content) is a proprietary resource owned exclusively by Baker McKenzie (meaning Baker & McKenzie International and its member firms). The Content is protected under international copyright conventions. Use of this Content does not of itself create a contractual relationship, nor any attorney/client relationship, between Baker McKenzie and any person. **Non-reliance and exclusion:** All Content is for informational purposes only and may not reflect the most current legal and regulatory developments. All summaries of the laws, regulations and practice are subject to change. The Content is not offered as legal or professional advice for any specific matter. It is not intended to be a substitute for reference to (and compliance with) the detailed provisions of applicable laws, rules, regulations or forms. Legal advice should always be sought before taking any action or refraining from taking any action based on any Content. Baker McKenzie and the editors and the contributing authors do not guarantee the accuracy of the Content and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the Content. The Content may contain links to external websites and external websites may link to the Content. Baker McKenzie is not responsible for the content or operation of any such external sites and disclaims all liability, howsoever occurring, in respect of the content or operation of any such external websites. **Attorney Advertising:** This Content may qualify as “Attorney Advertising” requiring notice in some jurisdictions. To the extent that this Content may qualify as Attorney Advertising, PRIOR RESULTS DO NOT GUARANTEE A SIMILAR OUTCOME. **Reproduction:** Reproduction of reasonable portions of the Content is permitted provided that (i) such reproductions are made available free of charge and for non-commercial purposes, (ii) such reproductions are properly attributed to Baker McKenzie, (iii) the portion of the Content being reproduced is not altered or made available in a manner that modifies the Content or presents the Content being reproduced in a false light and (iv) notice is made to the disclaimers included on the Content. The permission to re-copy does not allow for incorporation of any substantial portion of the Content in any work or publication, whether in hard copy, electronic or any other form or for commercial purposes.