Global Data and Cyber Handbook - Uruguay

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 review date: 30 December 2024*

Yes.

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

Regulating Decree N° 64/020 states that data controllers and processors should consider national and international standards in information security, such as the Cybersecurity Framework prepared by AGESIC, when determining the security measures to adopt. However, the regulation does not mandate specific security controls.

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

*Last review date: 30 December 2024*

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

☒        providers of critical infrastructure

If yes, please provide brief details of the relevant law or regulation.

# 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 review date: 30 December 2024*

☒      Data privacy

☒      financial services

☒      critical infrastructure

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

*Last review date: 30 December 2024*

Yes.

Both data controllers and processors must immediately report a data breach upon learning about it. The report shall detail the breach and the measures undertaken to address the breach. In the case of data controllers, the notification should be addressed to the Regulatory and Personal Data Control Unit (*Unidad Reguladora y de Control de Datos Personales (URCDP)*) within a maximum of 72 hours[1] and to all affected individuals. Although the legislation provides that the notification to the data subjects whose rights have been significantly affected must be made immediately, no specific term has been indicated for this. In addition, the regulation provides that in case the breach has been known by a data processor, it will immediately[2] notify the data controller. Once notified, the URCDP will coordinate the course of action with the unit in charge of security breaches (*Centro Nacional de Respuesta a Incidentes de Seguridad Informática, CERTUY*).

Within the first 24 hours of a breach being verified, controllers and processors must initiate the necessary procedures to minimize the impact of such incidents.

Once the violation has been solved, the controller must prepare a detailed report of the breach and the measures adopted and communicate it to URCDP.

--------------------------------------------------------------

[1] Article 4 of Decree No. 64/020:

*Communication of security breaches. The data controllers, once they verify the occurrence of a security breach that affects data protection, must notify the Regulatory and Control Unit of Personal Data within a maximum period of 72 hours after the breach is known.*

[2] Article 38 of Law No. 19,670:

*When the data controllers or processors become aware of the occurrence of the security breach, they must immediately and in detail report it and the measures adopted, to the data subjects and to the Regulatory Unit and Control of Personal Data, which will coordinate the corresponding course of action, with the National Center for Response to Computer Security Incidents of Uruguay (CERTuy).*

# Controllers/Owners have to notify:

*Last review date: 30 December 2024*

☒      data protection authorities

☒      affected individuals

# Processors/Agents have to notify:

*Last review date: 30 December 2024*

☒      controller/ owner

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

*Last review date: 30 December 2024*

Yes.

☒   other

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.