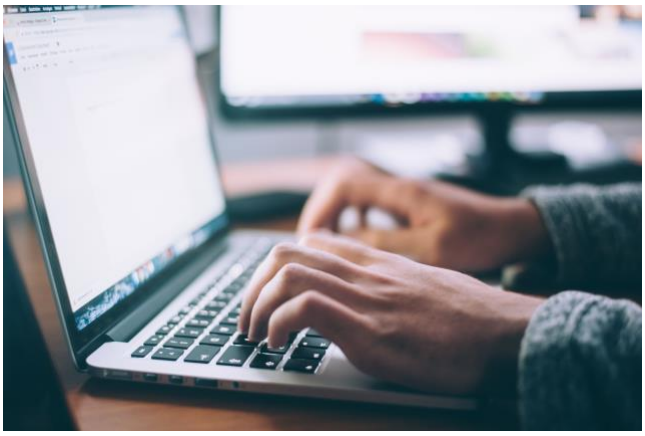
Employee Data Privacy – Argentina

Security Requirements

What security obligations are imposed on data controllers and data processors?

Security requirements may not always be included in the data protection law, but are key to guaranteeing lawful processing of personal data. The entity processing the data must take all useful precautions with respect to the nature of the data and the risk presented by the processing, to preserve the security of the data and, prevent alteration, corruption or access by unauthorized third parties.



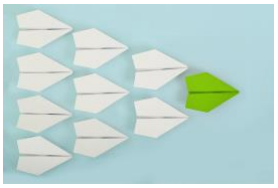
Appropriate technical and organizational measures should be implemented to ensure a level of security appropriate to the risk. Argentina's Protection of Personal Data Law sets some basic requirements relating to securing personal data. Under the Law, employers must adopt technical and organizational measures that are necessary to guarantee the security and confidentiality of personal data and, prevent the data's adulteration, loss, consultation or unauthorized treatment. The measures should also enable the ability to detect if the data has been changed in any way, whether intentionally or erroneously.

The Security Measures – Treatment and conservation of personal data in computer media (Resolution 47/2018) sets more detailed requirements relating to protecting personal data, including:

- **Data Collection:** Implementing necessary processes to ensure the completeness and integrity of data collection, minimizing errors and implementing technical measures to ensure confidentiality and limit access to personal information.
- **Access Control:** Implementing security measures, authentication mechanisms, segregating roles and functions and taking other measures to control access to systems.
- **Change Control:** Implementing processes that reliably identify individuals who make changes in production environments (i.e., active databases) that contain personal data, guaranteeing their identification, authentication and authorization.
- **Backup and Recovery:** Implementing backup processes which allow data to be recovered if an incident occurs.
- **Vulnerability Management:** Implementing a continuous review process that identifies, analyzes and corrects vulnerabilities in the system through integrity control techniques, registration, traceability and verification.

- **Destruction of Information:** Ensuring that confidential data is properly destroyed using secure deletion methods and applying effective control processes.

- **Security Incidents:** Implementing processes in the event of a security incident, including detection, evaluation, containment and response processes along with escalation and correction processes.



HR Best Practices:

Review current employee and job applicant data processing practices to confirm whether appropriate steps are being taken to protect the security and confidentiality of personal data. In addition, regularly train employees who may have access to personal information, to ensure that they are following all technical and organizational security measures that have been put in place.

Last updated October 2022.