SECURITY REQUIREMENTS

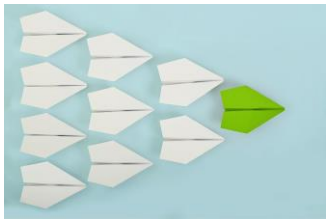
What security obligations are imposed on data controllers and data processors?

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.

The General Data Privacy Law (LGPD) requires that those who process personal data adopt security, technical and administrative measures to protect personal information from unauthorized access, accidental or unlawful destruction/loss/alteration/communication or other unlawful processing. More detailed rules may be issued by the data protection authority in the future.

When handling personal employee data, recruiting data, and communications, employers should consider the following as a best practice:

- Limit who can access personal data and private communications and, develop mechanisms to authenticate individuals (and prevent unauthorized access).
- Protect data through IT security programs and mechanisms, such as encryption.
- Use detailed access logs which track the records accessed, the time and duration of access and the identity of the individual who viewed/modified data.
- Train employees on data processing procedures, security measures and data breach procedures.
- Implement data processing agreements with vendors and service providers.
- Ensure incident response and remediation plans are in place.
- Establish policies and safeguards based on systematic assessments of potential privacy risks and impacts.



HR Best Practices:

Regularly review personal information that you maintain for your employees and take all reasonable measures to protect personal information, such as limiting access to data and training employees on security measures.

Last updated November 2021.