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. Employers in Portugal should follow the general security standards listed in Article 32 of the General Data Protection Regulation. When protecting employee and applicant data, consider the sensitivity of the information, the technology available, the expense of protecting the data and the risk to individuals if the data is compromised. Then take organizational and technological measures, including:

- pseudonymization/encryption;
- measures to ensure the confidentiality, integrity, availability and resilience of information processing systems
- measures to restore the system and access in case of an incident (such as a power outage)
- processes to regularly test and assess the system to ensure continued security.

Prior to the implementation of the GDPR, Portugal's data protection authority, the Comissão Nacional de Proteção de Dados (CNPD) issued guidelines that employers should follow when implementing security measures relating to HR data privacy. The CNPD Guidelines were issued by the older, now revoked, version of the Portuguese Data Protection Act (Law no. 67/98 of 26 October). These guidelines contain general principles applicable to data processing. Though outdated, these can still be used as a reference for best practices.

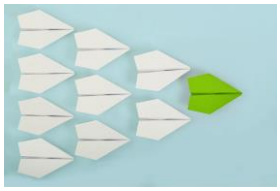
When protecting employee and applicant data, employers should consider the sensitivity of the information, the technology available, the expense of protecting the data and the risk to individuals if the data is compromised. Then, take appropriate organizational and technological measures, including measures to protect against accidental or unlawful:

- destruction;
- loss or alteration;
- disclosure or access; or,
- other illegal processing.

When handling sensitive employee information, employers should implement appropriate measures, including:

- measures to prevent data from being viewed, copied, altered, deleted or transferred;

- controlling physical entry to areas where sensitive personal data is processed;
- limiting access to authorized individuals;
- validating the identity of the recipients during data transfers; and,
- maintaining detailed logs (such as time/date stamps, etc.)



HR Best Practices:

The CNPD plans to update the data processing guidelines that were outlined in the former Portuguese Data Protection Act.

As a best practice, employers should take all appropriate security measures based on the sensitivity and confidentiality of the 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.

Ensure contracts with service providers detail the security and confidentiality measures that will be implemented.

Last updated December 2019.