SECURITY REQUIREMENTS

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

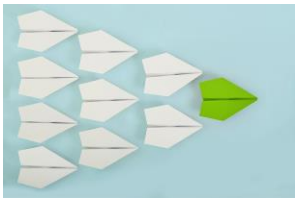
Security requirements may not always be included in the data protection law, but are key to guaranteeing lawful processing of personal data. The entity processing the data must take all useful precautions with respect to the nature of the data and the risk presented by the processing, to preserve the 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 Austria 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.

The Austrian Data Protection Act (Datenschutzgesetz - DSG) sets the additional requirement that employers (and other data controllers/processors) contractually commit their employees to ensure data secrecy and process personal data for specific purposes only, and only transfer data as directed by the employer. This is usually done through a short confidentiality and data secrecy agreement that is signed by each employee (DSG, Sec. 6).

While Austria does not currently have special security requirements specific to HR data, the Austrian legislator is regularly passing special data protection and data security provisions for certain areas. It is expected that specific data protection rules will follow for the processing of HR data.



HR Best Practices: Take all appropriate security measures based on the sensitivity and confidentiality of the data. 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. In addition, contractually commit employees to limit processing to specific purposes and to ensure data secrecy. Ensure contracts with service providers detail the security and confidentiality measures that will be implemented.

Last updated January 2021.