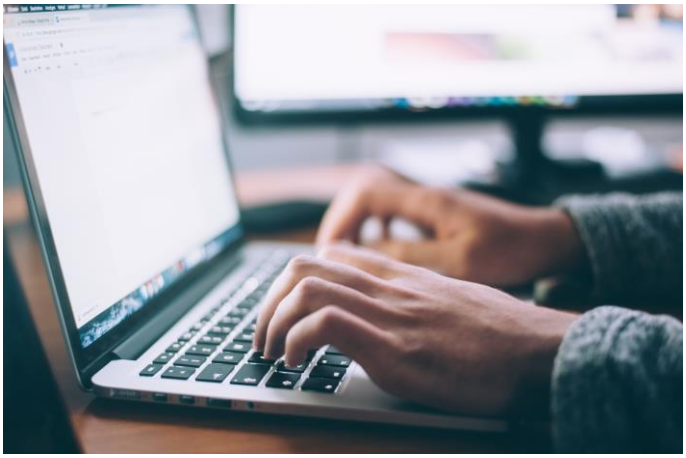
SECURITY REQUIREMENTS

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.

In the US, there are no general rules, restrictions or registration requirements related to employee personal data. Instead, security requirements are generally designed to protect specific types of personal information. For example, the Health Insurance Portability and Accountability Act (HIPAA) Security Rule requires that employers take certain steps to safeguard Protected Health Information (PHI) obtained or created by HIPAA-covered employer group health plans. When handling PHI under HIPAA, employers are expected to implement detailed administrative, physical and technical safeguards.

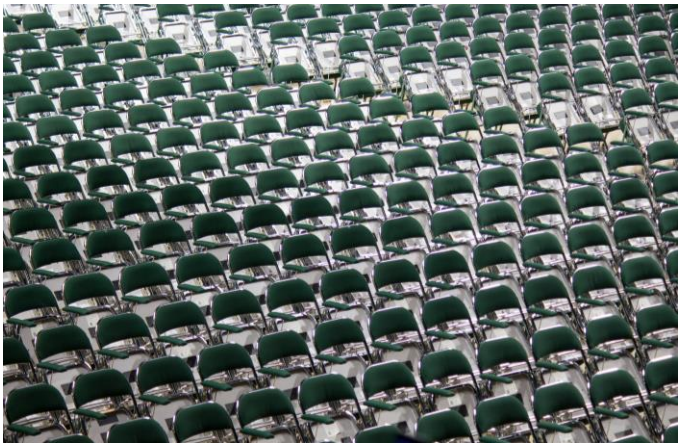
Several states require data owners to place reasonable and appropriate safeguards on personal information, particularly Social Security Numbers (SSNs) and driver's licenses. Massachusetts and Oregon require data owners, including employers, to implement comprehensive, written information security programs for personal data, including SSNs and driver's licenses. In recent years, some states have expanded the definition of personal information to include data such as health information, biometric information and online account credentials.

Information security laws in the United States often include the following practices:

- designating an employee or employees to coordinate a comprehensive information security program;
- identifying reasonably foreseeable internal and external risks and assessing the sufficiency of safeguards to address such risks, including (a) employee training and management (with disciplinary procedures for violations), (b) information systems design, and (c) detection and responses to attacks, intrusions, or other system failures;
- developing, implementing, and maintaining a comprehensive information security program designed to: ensure the security and confidentiality of personal information, protect against any anticipated threats or

hazards to the security or integrity of such information, and protect against unauthorized access;

- administrative, technical, and physical safeguards that are appropriate given the size, complexity, nature and scope of the company's activities;
- appropriate oversight of any service providers, including due diligence concerning the selection and retention of providers and requiring service providers by contract to implement such safeguards;
- ongoing evaluation and adjustments to the information security program; and
- encryption of all transmitted records containing personal information that will travel across public networks and/or is transmitted wirelessly, to the extent technically feasible, and encryption of personal information on portable storage media.



In addition, there are certain requirements around securely deleting data. The large majority of states have document destruction laws in place. While the laws differ by state, there is generally a requirement that SSNs and/or driver's license numbers are destroyed in a secure manner. The Fair Credit Reporting Act (FCRA) includes regulations that require background check reports and associated personal information are also securely destroyed.

Last updated May 2021.