ISO/IEC 27001:2013 Information security management systems
-Compliance with legal and contractual requirements-

Security category – 18.1. Compliance with legal and contractual requirements

Control – 18.1.1. Identification of applicable legislation and contractual requirements
Identify, document and keep up to date all legal, regulatory and contractual requirements applicable to each information system of the organization.

Identification of legislation and contractual requirements – including a short description of the organization's approach to fulfill the requirement.

More difficult in case of organizations that operate in several countries.

Legal and contractual requirements change – so they need to be updated.

ISO/IEC 27001:2013 Information security management systems
-Compliance with legal and contractual requirements-

Control – 18.1.2. Intellectual property rights
There should be procedures to ensure compliance with requirements related to intellectual property rights and use of proprietary software.

The risk is for legal action against the organization for unauthorized use of copyright material.

The organization should implement rules on the use of intellectual property.

Guidelines:
- software should be acquired only from known sources;
- awareness of personnel on intellectual property rights and using the disciplinary process in case of breaches;
- make inventory checks at least once per year to ensure all software in use is licensed;
- keep proof and evidence of ownership for all software;
- have regulations for disposing of software or transfer of software to others.

ISO/IEC 27001:2013 Information security management systems
-Compliance with legal and contractual requirements-

Control – 18.1.3. Protection of records
The organization should protect records according to legislation, regulatory, contractual and business requirements.

Records have to be protected from breach of confidentiality, from loss or modification.

There is legislation defining retention periods for many types of records and the organization is required to comply.

When keeping records for long periods consideration should be given to the risk of deterioration.

ISO/IEC 27001:2013 Information security management systems
-Compliance with legal and contractual requirements-

Control – 18.1.4. Privacy and protection of personally identifiable information
The organization needs to protect the privacy of personally identifiable information in line with applicable legal requirements.

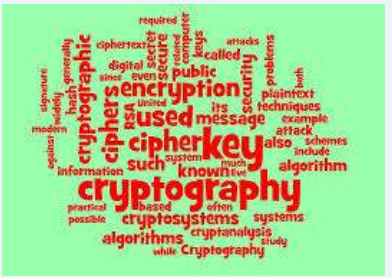
Most countries have legislation on the protection of personally identifiable information.

The organization should have a policy to ensure the compliance with relevant legislation related to privacy and personally identifiable information**.**

A solution is to nominate a "*Privacy officer".*

ISO/IEC 27001:2013 Information security management systems
-Compliance with legal and contractual requirements-

Control – 18.1.5. Regulation on cryptographic controls
The use of cryptography should respect legislation, regulations and relevant agreements.



Legislation on the use of digital signatures and other uses of cryptography.

Some countries prohibit the export of cryptography software, some restrict the import of such software; some legislations require licensing for the use of cryptography software.

Look for legal advice to make sure it complies with specific legislation on all the markets where it activates.