TECDT80651

Develop and implement strategies for privacy and data protection compliance

Overview

This standard is about developing and implementing strategies to manage privacy and data protection.

This involves creating policies and procedures to deliver the required privacy and data protection assurances across the organisation and acting as the primary point of contact for regulators and relevant organisations. This also includes planning and leading data protection Impact assessments.

This standard is for those who need to develop and implement strategies for privacy and data protection compliance as part of their duties.

Develop and implement strategies for privacy and data protection compliance

Performance criteria

You must be able to:

1. Create, implement and maintain the organisational privacy and data protection policies and procedures related to gathering, storing, processing and disseminating information

2. Manage the ongoing organisational compliance with privacy and cyber security legislation

3. Report to senior stakeholders regarding privacy and data protection compliance, risks and issues

4. Monitor and evaluate changes to privacy and data protection laws and regulations to maintain compliance

5. Plan, manage and communicate Data Protection Impact Assessments (DPIA) for organisational information management projects

6. Manage responses to data subject access requests (SAR) and queries as required

7. Act as the primary point of contact for data protection regulators and relevant organisations

8. Manage Records of Processing Activities (ROPA) to document all processing of personal data

9. Lead the delivery of organisational advice and guidance for privacy obligations and ethical requirements of all employees

Knowledge and understanding

You need to know and understand:

1. How the General Data Protection Regulation (GDPR) and other data protection information privacy laws describe obligations toward the handling of personal identifying data

2. The organisational roles and responsibilities of those who manage data policies and procedures

3. What is meant by subject access requests (SAR), Data Protection Impact Assessments (DPIA), and Records of Processing Activities (ROPA)

4. How handling data ethically is an organisational-wide responsibility

5. How to identify the risks associated with misuse of personal data

6. How to draft and implement privacy and data protection policies and procedures

7. The need to define an organisational commitment to handling data that protects individuals and defines the responsibilities of data ownership

8. The principles of privacy by design and how to implement them

9. The need to educate all employees about privacy and data protection practices

10. How to implement data protection metrics

11. How metadata can help optimise data protection and guide business data usage in processing and storage

12. The importance of maintaining records of processing operations

13. The need to identify the location of all sensitive information, to enable effective data protection strategies to be developed

14. The need to continuously monitor data management procedures and compliance within the organisation

15. The importance of identifying the role of contact point for regulators data and the Information Commissioner's Office (ICO)

16. The importance of delivering proactive and pragmatic advice to maximise compliance and minimise disruption and costs to the business

17. The need to provide guidance and data protection training across the organisation

18. The importance of ensuring that the organisation addresses all queries and subject access requests within legal timeframes

Develop and implement strategies for privacy and data protection compliance

Glossary

Subject Access Requests (SAR)

A Subject Access Request (SAR) is the right of access allowing an individual to obtain records on their personal information, held by an organisation.

Record of Data Processing Activities (ROPA)

Records of Processing Activities (ROPA) is an internal record that contains the information of all personal data processing activities carried out.

*Data Protection Impact Assessments (DPIAs) *

A Data Protection Impact Assessment (DPIA) is a process to help identify and minimise the data protection risks of an information systems project.

Develop and implement strategies for privacy and data protection compliance

Developed by	e-skills
Version Number	1
Date Approved	30 Mar 2022
Indicative Review Date	30 Mar 2025
Validity	Current
Status	Original
Originating Organisation	ODAG Consultants Ltd.
Original URN	TECDT80651
Relevant Occupations	Information and Communication Technology Professionals
Suite	IT and Telecoms Professional (procom)
Keywords	Data management, data protection