isms.online

Data Privacy Week

FIVE STEPS TO BETTER DATA PRIVACY

IN YOUR ORGANISATION

1 ADOPT A STANDARDS-BASED APPROACH TO DATA PRIVACY

Creating a whole new privacy framework can seem daunting, but the good news is that you don't have to start from scratch. You can adopt several established privacy frameworks to integrate privacy management into your company. Some frameworks you can adopt are:

ISO/IEC 27701
International Standard for Privacy Information Management

NIST Cybersecurity Framework

Adopting a privacy framework can help you more quickly identify privacy weaknesses, mitigate risks, easily monitor your information assets and ensure the continuous development of data privacy practices within an organisation.

2 ESTABLISH A CULTURE OF PRIVACY

Achieving effective data privacy practices in any organisation is only possible if you have a culture that supports it. A privacy culture starts at the very top of your business. If your senior leadership doesn't live and breathe privacy, your staff certainly won't see the need to.

A practical tool to achieve this privacy culture buy-in can be as simple as building a business case for why you need a privacy culture, focusing on the following:

- The legal and regulatory implications of poor privacy
- The ROI of adopting a culture of privacy
- The importance of privacy to your customers
- How a privacy culture would support company goals

3 EDUCATION EMPOWERS YOUR PEOPLE

An organisation's people are the first line of defence in protecting customer data privacy, and with practical training and education, they can be invaluable in ensuring a robust privacy culture.

One of the most potent tools available to organisations is an effective and accessible data privacy policy coupled with a training program that suits your company and specific goals and covers topics such as:

- How to manage personal data
- How data privacy applies to every staff member's role
- How to recognise and report potential breaches
- Best practices to improve privacy

Privacy is not a one-and-done activity; therefore, additional training, engagement and updates to privacy policies and procedures should be regularly undertaken to ensure compliance with any updates or changes to regulation.

4 ENSURE CONSENT AND PREFERENCE MANAGEMENT IS STANDARD PRACTICE

Consent management is a significant part of managing privacy in any company. Getting clear consent from customers about any data being collected improves transparency and can help ensure compliance with several laws, including GDPR.

GDPR clearly outlines what does and doesn't constitute consent in collecting data. Ensuring clarity in this area is fundamental to ensuring adequate data privacy. Should an organisation be audited, it's essential to provide clear records of obtaining valid consent. Therefore, using consent and preference management tools to ensure compliance is a vital step every organisation should consider.

5 IMPLEMENT EFFECTIVE TECHNICAL CONTROLS

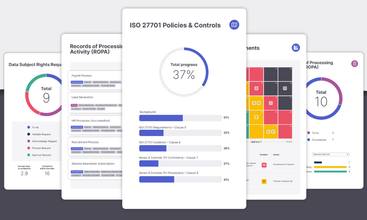
Organisations should implement technical controls, which help to protect personal data, comply with data privacy regulations, and reduce the risk of data breaches.

ENCRYPTION
to secure sensitive information whilst it is being transmitted or sorted.

FIREWALLS
to provide a barrier between an internal network and the external network, preventing unauthorised access to data.

ACCESS CONTROL
to limit who can access sensitive information and what actions users can take with sensitive data.

INTRUSION DETECTION SYSTEMS
to monitor network activity for signs of malicious activity, alerting security teams to potential threats.



TAKE CONTROL OF YOUR DATA PRIVACY MANAGEMENT

ISMS.online's platform enables a simple, secure and sustainable approach to information management with ISO 27701 and other frameworks.

Start your journey to better data privacy today.

Get started →

isms.online