Privacy protection

How to build security that respects privacy

Physical security doesn't mean giving up privacy. By taking a comprehensive, step-by-step approach to privacy protection, you can defend individual rights and gain better control over your data.

Privacy and data breach stats

11 seconds
another business falls victim to a ransomware attack
[Source: Cybersecurity Ventures]

315 days
the average data breach lifecycle from a malicious or criminal attack
[Source: IBM]

$150
the cost per compromised record containing customer personal identifiable information (PII)
[Source: Capita]

€1,059,520,456
the total amount of fines issued under GDPR legislation
[Source: Privacy Affairs]

Take the steps to keep your data private

Step 1

Identify goals and hire the right people

- Hire a Data Protection Officer (DPO) to help guide your strategies and comply with regulations
- Map out how data is collected, where it's stored, how long it's kept, and who has access to it
- Categorize the various types of data that you're collecting (high, medium, low risk)
- Identify the people outside your organization who might need access to your data
- Assess the level of risk that your data processing operations pose to citizens' rights

75%
of customers strongly associate privacy with trust
[Source: Salesforce]

107
countries have legislation to secure the protection of data and privacy
[Source: UN]

Step 2

Build your data protection strategy

- Conduct a gap analysis to identify potential improvements in your data processing operations
- Evaluate existing systems to determine whether they effectively address privacy without draining resources
- Implement new processes and document all your privacy policies and procedures
- Educate your employees on cybersecurity and privacy best practices
- Be more transparent and inform the public about your data and privacy initiatives

52%
of incidents involve a malicious attack versus 25% caused by system glitches and 23% caused by human error. [Source: IBM]

75%
of CEOs will be personally liable for cyber-physical security system attacks by 2024
[Source: Gartner]

Step 3

Choose the right system and vendor

- Find out what tools your vendors offer to help businesses uphold privacy and data protection
- Ask what certifications vendors have and what steps they are taking to comply with privacy legislation themselves
- Assess the level of transparency each vendor provides about their data policies and practices
- Invest in or upgrade to solutions that are built with Privacy by Design, where privacy features are enabled by default
- Consider solutions that allow you to standardize processes and policies across different regions

Only 59%
of organizations say they are currently meeting all GDPR requirements
[Source: Cisco]

75%
of public safety technologies will have policy-based regulatory and ethical specifications as a result of pressure from data transparency advocates [Source: IDC]

Step 4

Set up your system with privacy in mind

- Enable varied layers of defense to protect personal information collected by your physical security systems
- Define user access and privileges to restrict who can log into your applications and what they can see or do
- Implement add-on privacy features such as video anonymization that blurs identities in footage
- Automate your data retention policies to ensure data is automatically deleted as required
- Invest in a digital evidence management system to securely share information during investigations or when a citizen requests it

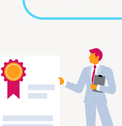
56%
of organizations are working toward a single, global data protection and privacy strategy which can be tailored to jurisdictional requirements when needed [Source: IAPP]

Breach costs are 95% higher
for organizations that had not deployed security automation versus those with fully-deployed automation [Source: IBM]

Step 5

Stay alert and effective at maintaining privacy

- Keep up with data privacy laws and evolve your policies and processes as needed
- Leverage hardening tools to actively monitor cybersecurity compliance and keep up with firmware and software updates
- Monitor user activity logs to see who accessed what data, systems, and files at any time
- Use health-monitoring features to receive automatic alerts for devices going offline or other system vulnerabilities
- Consider hybrid cloud to streamline access to the latest cybersecurity and data privacy measures



84%
of customers are more loyal to companies with strong security controls.
[Source: Salesforce]

97%
of companies recognized they were realizing benefits such as competitive advantage or investor appeal from their privacy investments.
[Source: Cisco]

Work with a vendor you can trust

As cyber threats and privacy regulations continue to evolve, businesses will need to stay vigilant. Investing in security solutions that are built with privacy and cybersecurity in mind gives you the tools to adapt privacy and data protection measures and stay compliant.

To learn about our approach to privacy and cybersecurity and how we help you keep personal data safe, visit the Genetec Trust Center at

genetec.com/trust

Genetec