ProvePrivacy

GUIDE

Avoiding the Common Pitfalls of Data Sharing Risks

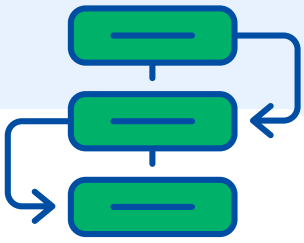
In our interconnected world, data sharing is crucial for business operations and personal interactions. Whether sharing customer information, collaborating with partners, or using cloud services, data is always on the move. However, this convenience comes with the responsibility to ensure data is shared securely and responsibly.

In data protection terms there are two considerations which need to be addressed:

1. Whether there are adequate legal safeguards in place to allow the transfer to take place; and
2. Whether there are adequate organisational and technical measures in place to protect the data being shared In this guide we look at both of these considerations, starting with the first and how we can lawfully share personal data.

Lawfully sharing personal data

Data Processors



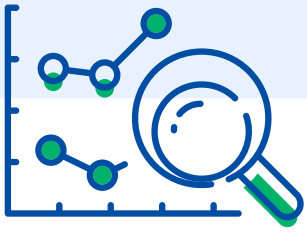
Article 28 of the GDPR requires data controllers to use processors who provide sufficient guarantees to protect personal data. These guarantees must be included in a binding contract with specific clauses outlined by the GDPR.

Unlike 'Standard Data Protection Clauses,' (see International Transfers) the wording of these clauses is not mandated and can vary, making verification difficult. Using a checklist and seeking legal help is advisable.

These clauses ensure appropriate technical and organizational measures are in place to meet GDPR requirements and protect data subjects' rights. The contract ensures the processor acts only on the controller's instructions, maintains confidentiality, implements security measures, and obtains consent for sub-processing.

A Data Processing Agreement (DPA) must also be in place, specifying the nature, purpose, types of personal data, and duration of the processing. The DPA can be part of the contract, usually as a schedule.

Joint Data Controllers



Joint Data Processors are explicitly mentioned in the regulation, requiring a Data Sharing Agreement (DSA).

Joint Controllers are two controllers using the same data for similar purposes, such as two organizations sharing data collected at a trade show for marketing. This might confuse data subjects about who controls their data or handles complaints.

A DSA sets the terms of data sharing, ensuring transparency and cooperation between parties when a data subject makes a request. It also puts safeguards in place to protect data subjects. A DSA is required under Article 26 of the GDPR and must not be omitted.

Data Controllers

Data protection between Data Controllers is usually covered in a contract. For example, an organization engaging a pension provider should address data protection concerns in their contract. Since both parties control the data for their own purposes, these clauses are typically limited and not mandated by regulation. However, having a sharing agreement is good practice.

Data protection regulation requires 'Accountability,' so documenting and recording assessments is crucial for compliance. A solution like ProvePrivacy can help with this.

International Data Sharing

To share personal data internationally, additional safeguards are needed. These vary depending on whether the destination is an "Adequate Country" or a "Third Country."

Adequate Countries

An "adequate country" is a country that the European Commission has determined provides data protection equivalent to the EU. This is decided through an adequacy decision, assessing the country's data protection laws, enforcement, and commitments.

Countries with an adequacy decision include Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the UK, and Uruguay. This list can change so it is worth checking the most up to date version on the European Commission website.

https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

Data transfers to these countries can occur without additional safeguards, similar to within the EU.

Third Countries

A "third country" is any country outside the European Economic Area (EEA), which includes EU member states, Iceland, Liechtenstein, and Norway. When transferring personal data to a third country, special rules and safeguards must ensure data protection.

An adequacy decision by the European Commission confirms that a third country provides comparable data protection to the EU, allowing transfers without additional safeguards. If no adequacy decision exists, appropriate safeguards like Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs) must be in place. These pre-approved clauses cannot be altered, or they become invalid.

Other safeguards, such as codes of conduct, are less common. If no safeguards exist, data transfers may still be possible with consent from data subjects or limited approval from the regulator for one-off transfers with a compelling legitimate interest.

Regular audits and assessments should ensure ongoing compliance and address potential risks associated with data sharing.

United States

The United States is not an 'adequate country,' but the EU-U.S. Data Privacy Framework (DPF) provides a level of assurance at the organizational level. This framework, developed by the U.S. Department of Commerce and the European Commission, allows U.S. organizations to self-certify their adherence to privacy principles, ensuring EU data subjects' rights are protected. The UK has adopted this framework for its own purposes.

Data Protection Professionals should remain vigilant about changes to this framework, as it is considered by some to be on thin ice. Legal scrutiny and potential invalidation, similar to the EU-U.S. Privacy Shield's fate in the Schrems II decision, could jeopardize the framework's validity and disrupt data transfers. Concerns about U.S. government surveillance and the adequacy of privacy protections for UK data subjects remain contentious issues.

Conclusion: Prioritise Security, Responsibility, and Awareness

In conclusion, data sharing is essential, but it comes with the responsibility to ensure lawful and responsible handling. Legal safeguards and technical measures are crucial for lawful data sharing.

For data processors, Article 28 of the GDPR mandates binding contracts with specific clauses to protect personal data. Joint Data Controllers require a Data Sharing Agreement (DSA) to ensure transparency and cooperation. Data Controllers should have contracts addressing data protection concerns, emphasising accountability.

International data sharing requires additional safeguards, varying by destination. Adequate countries have EU-equivalent data protection, while third countries need specific safeguards like Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs). Regular audits and assessments are vital for compliance.

The EU-U.S. Data Privacy Framework provides assurance for U.S. data transfers, but vigilance is needed due to potential legal challenges. Ensuring robust data protection practices is key to maintaining trust and compliance in data sharing activities.

Technical Considerations

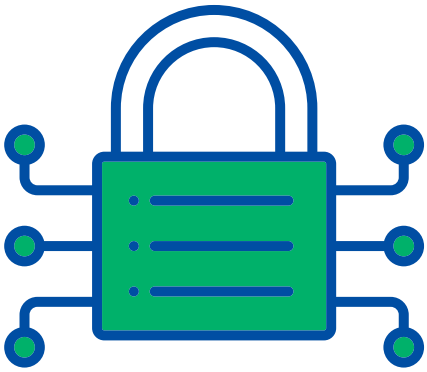
Many organisations and individuals fall into common traps when it comes to sharing sensitive data. Here we explore these pitfalls and offer tips on how to avoid them, protecting your data while maintaining trust and compliance.

Lack of Data Encryption

One of the most critical mistakes organisations make when sharing data is failing to encrypt it properly. Encryption ensures that even if data is intercepted, it cannot be accessed without the decryption key. Without encryption, sensitive data is vulnerable to cyberattacks, unauthorised access, and data breaches.

How to avoid it:

- Always use end-to-end encryption for data transfers.
- Use secure methods such as HTTPS or SFTP to ensure the integrity of the data during transit.
- For stored data, employ encryption protocols like AES (Advanced Encryption Standard) to protect it at rest.



Failure to Define Access Permissions

When sharing data with third parties, organisations often fail to clearly define who can access specific pieces of information. This opens the door for data to be misused, either accidentally or intentionally. Sometimes, too many people or systems are given access to sensitive information, creating unnecessary risks.

How to avoid it:

- Implement strict access controls based on the principle of least privilege (POLP). Only give access to individuals who absolutely need it to perform their duties.
- Regularly review and update access permissions to ensure that outdated or unnecessary access is revoked.
- Use role-based access control (RBAC) systems to define and restrict access levels based on roles.

Not Auditing Data Sharing Practices

Data sharing is not a "set it and forget it" practice. Organisations should regularly audit how and with whom their data is being shared. This includes tracking data flow, checking who has access to what data, and identifying potential vulnerabilities. Without regular audits, it's easy for risky behaviours or unauthorised access to go unnoticed.

How to avoid it:

- Set up automated logging and monitoring tools that track data access and sharing activities.
- Perform periodic audits to ensure compliance with internal policies
- Address any anomalies or gaps in your audit logs immediately.

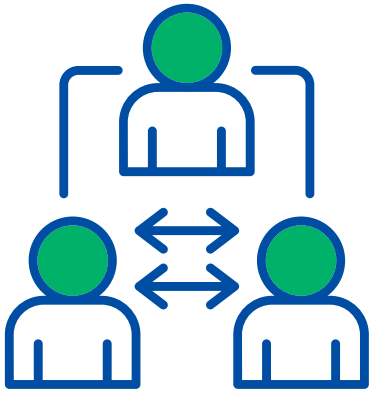
Neglecting Legal and Compliance Obligations

Different countries and industries have varying legal frameworks surrounding data privacy and sharing. Neglecting to account for these laws can lead to costly fines, lawsuits, and reputational damage. Regulations like GDPR in the EU mandate how data should be handled, shared, and protected.

How to avoid it:

- Familiarise yourself with the relevant data protection laws in your jurisdiction and industry.
- Ensure that any third parties you share data with are also compliant with applicable regulations.
- If sharing data across borders, ensure that international data transfer agreements, like the Standard Contractual Clauses (SCCs) under GDPR, are in place.

Over Reliance on Third-Party Providers



While third-party services like cloud providers or data processors can offer convenience and scalability, relying too heavily on them can expose you to risks. A third-party vendor may not implement the same level of security protocols, or worse, they may be a target for cyber criminals. Data breaches that occur within third-party systems can directly affect your organisation.

How to avoid it:

- Perform due diligence before choosing any third-party vendor. Ensure that they follow industry best practices for data security and have a clear data protection policy.
- Regularly review the security measures and compliance status of any third-party service providers.
- Consider a contract that outlines data protection obligations, breach notifications, and audit rights.

Inadequate User Education and Training

A significant portion of data breaches stems from human error—whether it's employees falling for phishing attacks, improperly handling data, or mistakenly sharing information with unauthorised parties. The best technology won't be effective if the people using it aren't properly trained.

How to avoid it:

- Implement a continuous education program that trains employees on data security best practices, phishing awareness, and proper data handling procedures.
- Run regular security drills and simulated phishing attacks to test employee readiness.
- Make data privacy and security a core component of your organisation's culture.

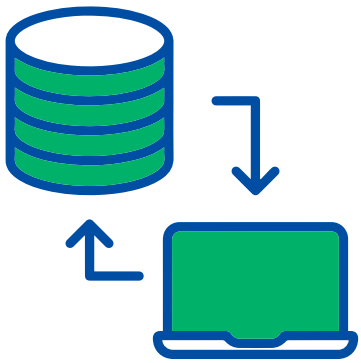
Ignoring the Risks of Shadow IT

Shadow IT refers to the use of unauthorised devices, applications, or services to store or share data, often without the knowledge or approval of IT departments. It's an increasing issue in modern workplaces, where employees may bypass official tools to streamline their work or avoid red tape. Unfortunately, shadow IT can create significant vulnerabilities, especially when sensitive data is involved.

How to avoid it:

- Implement a clear and easy-to-follow data-sharing policy that encourages employees to use approved tools and systems.
- Use software that detects and flags unapproved applications or cloud services being used on your network.
- Educate employees on the risks of shadow IT and the importance of compliance with company data policies.

Over-Sharing or Under-Sharing Data



Another common pitfall is sharing too much or too little data. Over-sharing can lead to privacy violations, regulatory breaches, and unintended exposure of sensitive information. On the other hand, under-sharing can create operational inefficiencies and may hinder collaboration.

How to avoid it:

- Assess the needs of the recipient and share only the data necessary for the task or project at hand.
- Use data masking or anonymisation techniques when sharing sensitive information that doesn't require full disclosure.
- Communicate clearly with recipients about the data being shared and any limitations or restrictions associated with its use.

Conclusion: Prioritise Security, Responsibility, and Awareness

As we continue to generate and share vast amounts of data daily, the risks associated with improper data sharing will only grow. But by being proactive about implementing secure sharing practices, defining access controls , and adhering to legal obligations, we can significantly reduce the risk of data breaches and privacy violations.

Ultimately, protecting data is not just a technical challenge but a cultural one. Ensuring that all stakeholders—from employees to third-party vendors understand the risks and responsibilities surrounding data sharing is key to safeguarding sensitive information in an increasingly complex digital landscape.

By avoiding these common pitfalls and fostering a culture of awareness and responsibility, organisations can protect their data and maintain the trust of their partners, customers, and employees.