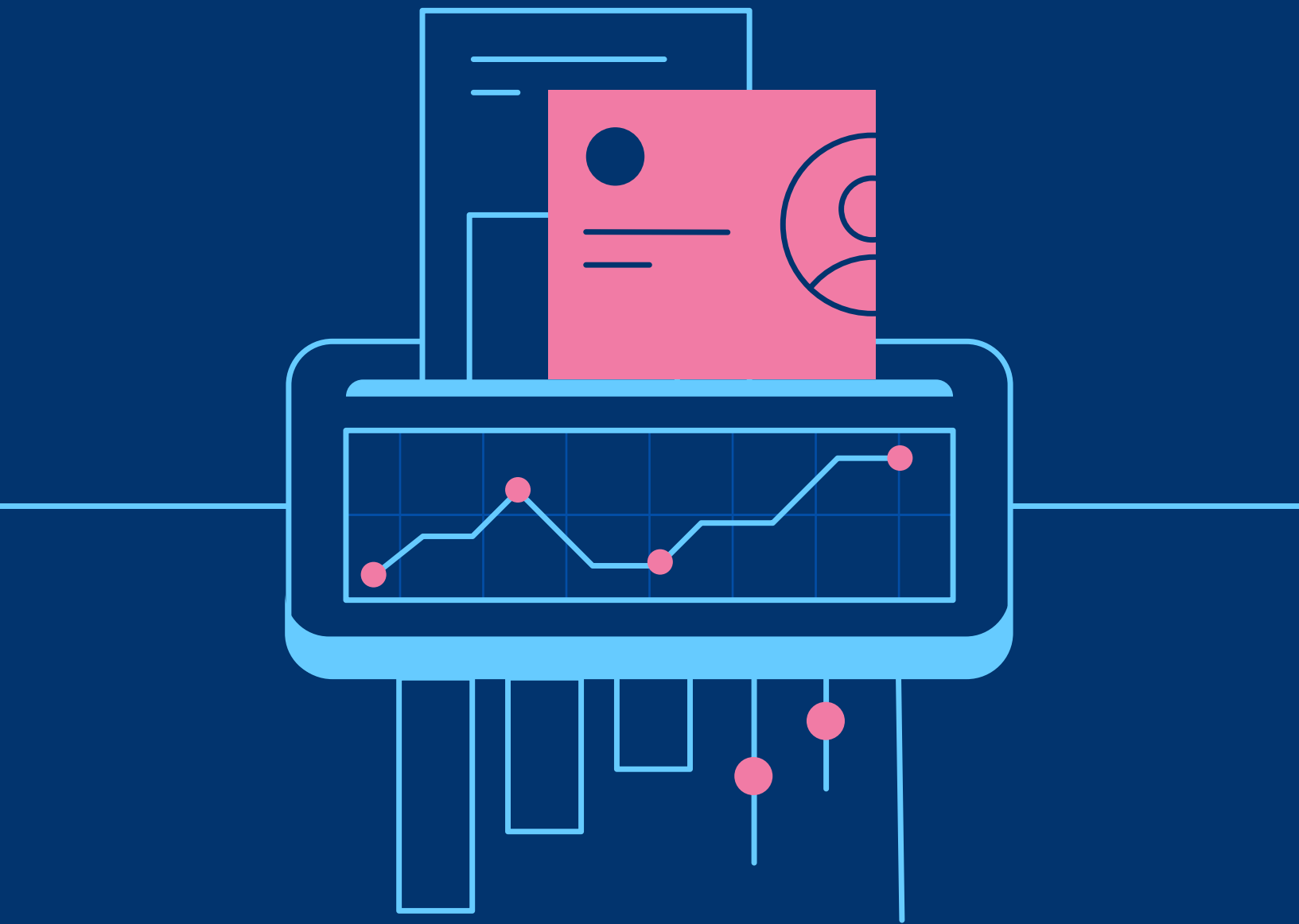
1Password

A guide to securing your business data



Your data is important. So is the data of your customers, suppliers and employees. Data of all kinds is desirable to hackers, scammers and criminals, and a data breach of any kind could be devastating to your company.

This guide aims to help new businesses who are just starting out in thinking about how to be safe and smart in the ways they handle data. It will help you to:

- Understand compliance
- Know where your data is, and where it comes from
- Classify data
- Protect and use data
- Have an end-game

Though the security of your physical data is important, this guide will focus on digital data because the risk of breaches and losses is higher in the digital realm.

Understand compliance

The laws that govern how you must handle data will depend on a number of things.

Complying with the law should be the minimum requirement of your data handling policy. You may wish to go further so you can reassure customers, clients and employees that the way you use data is ethical, responsible and secure.

Location

Your compliance needs will depend on where you do business. This may include locations where you have customers but no formal presence. *For example:*

- The California Consumer Privacy Act to companies that operate in California in the United States

- The California Consumer Privacy Act to companies that operate in California in the United States

Industry sector

Your needs may also depend upon the nature of your business, and the kind of data you're likely to handle. *For example,* if you operate in the healthcare sector in the United States, you may need to comply with the Health Insurance Portability and Accountability Act.

Every business is different, so only you can determine how you need to comply. Be aware that in some places, such as the United States, data handling is not governed by one law, but by many.

Know where your data is, and where it comes from

For your data policy to have value, it must apply to all the data you handle. Knowing where your data is, and where it comes from, is harder than it sounds. Many digital platforms can passively accrue large quantities of sensitive data when they're up and running.

Digital data

Where digital data comes from and where it is stored are sometimes the same. *Consider:*

- Company servers
- Cloud file storage
- Customer and client communication tools and CRM
- Cloud services, including specialist tools
- Email servers, and data synced to local devices
- Internal communication tools

- Digital archives
- Employee hard drives and devices
- Banking services *(e.g. records of transactions)*
- Contact forms
- Web forums
- Postal services
- Voice and video call recordings
- Files, folders and physical archives

Capture everything

Go beyond your most obvious stores of data and think about every touch point you have with your customers, clients and employees – each will likely have implications for your data policy.

Tip: *Involve every team in your organization. Not everyone will have access to everything, so you need help to make sure you capture everything.*

Classify data

Not all data is created equal – especially so far as compliance is concerned.

Here are three classifications you could use:

- **Public Information:** any data already available online or in the real world.
- **Proprietary Information:** data about your company that is known only to your company.
- **Customer Information:** data about, or belonging to, you customers. This may include customer email addresses, customer communications, or analytics gathered about customers.

Note: *It's tempting to classify data by confidentiality, or whether it's personally identifiable information (PII). But this can muddy what is and isn't confidential, or what constitutes PII. We recommend keeping data classification simple and guarding all non-public information as safely as possible, and giving access to particular data only when needed. How you classify data may depend on your company's compliance needs, and how it operates.*

Protect and use data

When it comes to actually using your data, we recommend using the principle of least privilege. This is the idea that no person or thing *(such as a service, or workflow)* has access to information it doesn't strictly need. *Put simply:* you can't use or misuse what you don't have. Choose services that give you the flexibility you need to control access to data.

Plan ahead for removing permissions as well as granting them, such as when an employee changes role or leaves your company.

Choose secure services

Increasingly, companies rely on third-party servers to store and handle data. Do the due diligence necessary to make sure the services you choose have robust security appropriate to the data stored. Consider:

- The mode and strength of encryption used
- Support for single sign-on using an identity provider
- Support for two-factor authentication *(especially where SSO isn't an option)*
- The geographical location of servers *(which may affect compliance)*

Use safe passwords

Use a password manager to make sure all passwords are randomly generated, unique and strong. In the event that passwords need to be shared, use a password manager with secure password sharing built in.

Be safe on site

Consult with security and IT professionals to make sure that data is used and stored safely on your work premises.

Have an end-game

Your data compliance needs may mean you need to delete data, or keep it for a considerable time. Both have implications for the safety of that data.

Deleting data

Even if data is not part of your routine, you may sometimes need to permanently delete data to comply with the data laws that apply to you.

Erasing digital data is harder than erasing data stored physically – you have to make sure it's really gone. Some hosting and archive services help to permanently erase data as a feature – particular for any data storage or archiving services. Make sure your IT team understands how to permanently erase any data stored locally on company hardware and devices.

Archiving data

As well as making sure archived data is secure, you also need to be sure you can access it, and erase it, should you need to. Make sure that digital archives give you the flexibility you need.