Zettaset

Data Protection Checklist

for Organizations Looking to Secure Their Data Environment

Organizations handle inordinate amounts of sensitive information in nearly all aspects of their operations. Individuals freely (or in some cases are compelled to) give personal information to organizations, but there is an unspoken expectation that business and government will safeguard that data. And, as data breaches and cyber attacks continue to rise (in both quantity and intensity), the number of international laws and regulations for data protection is also increasing.

We've put together a checklist to jumpstart your planning so you can build an up-to-date data protection strategy that meets regulations and exceeds customer expectations. The last thing you want is another costly data breach that exposes sensitive information and ruins your company's reputation.

But before we get into the details, let's go over what data protection actually is, and why it's become so important.

What is data protection?

Data protection is the process of securing sensitive information from theft, corruption, compromise, or loss. In this case, sensitive information refers to data that is unavailable in directories or government records that are accessible by the public, such as:

- Personally Identifiable Information (PII)
- Financial information
- Medical records
- Educational records
- Intellectual property
- Trade secrets, private business documents
- Classified government documents

Data protection is increasingly important because the sheer volume of data being created and stored is growing astronomically. Sensitive information that is compromised in some way carries an enormous cost and disruption for those affected – emotional, financial, reputational … you name it.

The devil's in the details, so let's dive in. The data protection checklist is a great place to start as you build your cybersecurity plans, but it's by no means exhaustive. Some are best practices while others are regulatory mandates and are governed by law.

Data Protection Checklist

Obtaining data

You need to know about the data you’re protecting. Where did you get it? How did you get it? Why do you need it?

❑	Obtain and process personal data fairly
	❑ Provide notice when acquiring data
	❑ Receive consent (mandatory within the European Union (E.U.) or when collecting an E.U. citizen’s information from anywhere in the world)
❑	Keep for a specific purpose
❑	Keep secure and up-to-date
❑	Use multiple containers/repositories for archiving (tape, disk, cloud)
❑	Catalog your data – know what you have, how you acquired it, and what it’s used for
❑	Delete data once you’re done with it

Ensuring data is protected

Cybercriminals are ruthless and will scour their targets for any exploitable weakness, so make sure you have all of your bases covered with a comprehensive data security plan. Not only do you want to safeguard your data and render it unreadable to outsiders, you also need to ensure the data is recoverable, and easy to restore after any corruption or loss. Have a data recovery plan in place – just in case. Here are some technologies that can help provide a level of data-centric protection.

Software	
❑	**Data encryption** — Renders information unreadable without a special key, so in the event of a breach, the data can’t be used by an unauthorized individual
❑	**Anonymization** — Removes personally identifiable information from the data sets so they cannot be traced back to an individual
❑	**Data masking** — Maintains the format and functionality of data but changes the values when the real data is not required, such as with user training or software testing
❑	**Data backups** — Allows for restoration in case of data loss or tampering.

Hardware

□ **Tokenization** — Substitutes sensitive data with a non-sensitive equivalent (the token") containing no exploitable value

□ **Two-factor authentication** — Provides an additional layer of security beyond a password to pass an authentication check. Examples include knowledge factors, possession factors (ID, smartphone, secure token, etc) and biometrics

□ **Biometric technology** — Used in multi-factor authentication, biometrics map physical characteristics or speech patterns to identify authorized individuals

Human Resources

□ Regular system tests — Running frequent tests, such as vulnerability or penetration testing, enables you to assess the security and robustness of your system and data processed by it. There are pros and cons to using live data in a live environment, so it's preferable to use anonymized or masked data when testing

□ Data Protection Officer (DPO) — For many organizations, appointing a DPO is a mandatory requirement under the E.U. GDPR (General Data Protection Regulation)

□ Establish controls for confidentiality — Design and clearly define the internal procedures aimed to protect data confidentiality for all staff, employees, volunteers, trustees, contractors, etc.

□ Build a top-tier IT department — Carefully choosing your IT team is critical. A cohesive team that combines strong skill-sets makes for a more secure environment

□ Training — Offer data protection training for all employees (especially if they bring their own devices)

□ Communicate — Strengthen communication between IT security teams and executives

Know the rules

Find out which data protection standards apply to your business, and make sure you hold your organization accountable. For example, the GDPR affects all companies handling sensitive information of people within the E.U., regardless of where the company is located. Many multinationals headquartered in the U.S. and China, for example, find that they must adhere to the GDPR, which requires public notification of a data breach within 72 hours.

Here are some examples of high-profile data protection mandates and regulations. This is far from an exhaustive list.

□	General Data Protection Regulation (GDPR)
□	Payment Card Industry Data Security Standard (PCI DSS)
□	Health Insurance Portability and Accountability Act (HIPAA)
□	Health Information Technology for Economic and Clinical Health (HI-TECH)
□	Data Protection Act: U.K.

What to do in case of a data breach

Time is of the essence here, and any missteps can be costly. If you've suffered a data breach, here are five steps to take immediately:

1. Contain the threat
2. Identify and secure the vulnerability
3. Determine what information was stolen
4. Announce the breach immediately
5. Offer your consumers recourse

We've put together a useful data theft survival guide that expands on these points in more detail. Hopefully, you'll never have to use it, but it might be helpful to bookmark it just in case! Read in full here.

As your team works to strengthen your organization's data protection plans and cybersecurity practices, keep this checklist handy!

About Zettaset

A leader in data protection, Zettaset's XCrypt™ line of encryption products are optimized for unmatched performance and infinite scalability to address the demanding data protection requirements of today's high-volume compute, storage, and cloud environments.

Zettaset

465 Fairchild Drive, Suite 234, Mountain View, CA 94043 // USA: +1.650.314.7920
Fax: +1.650.314.7950 // sales@zettaset.com // www.zettaset.com