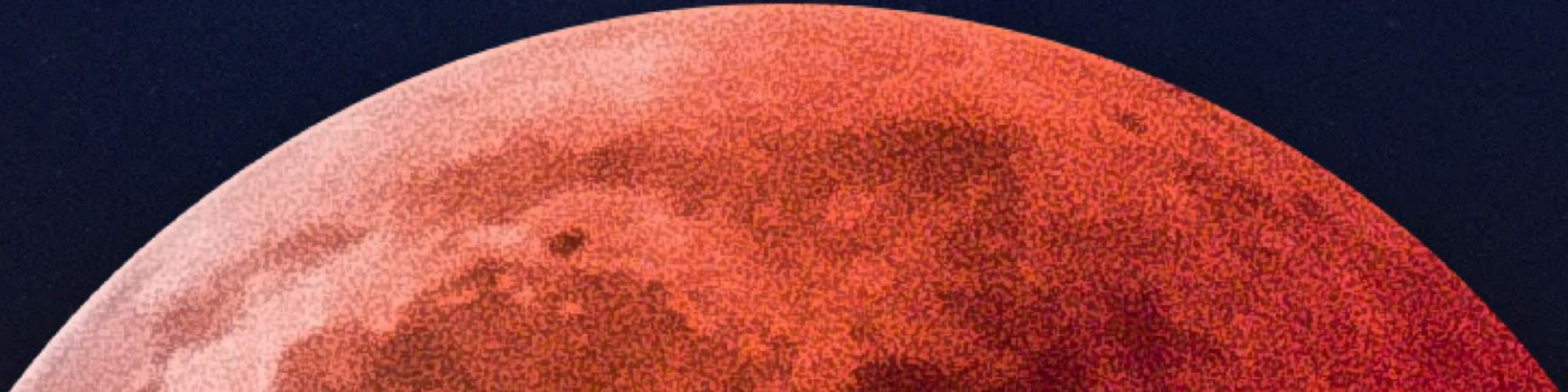
Data
Privacy

Privacy Essentials Training

BY SPRINTO

Welcome

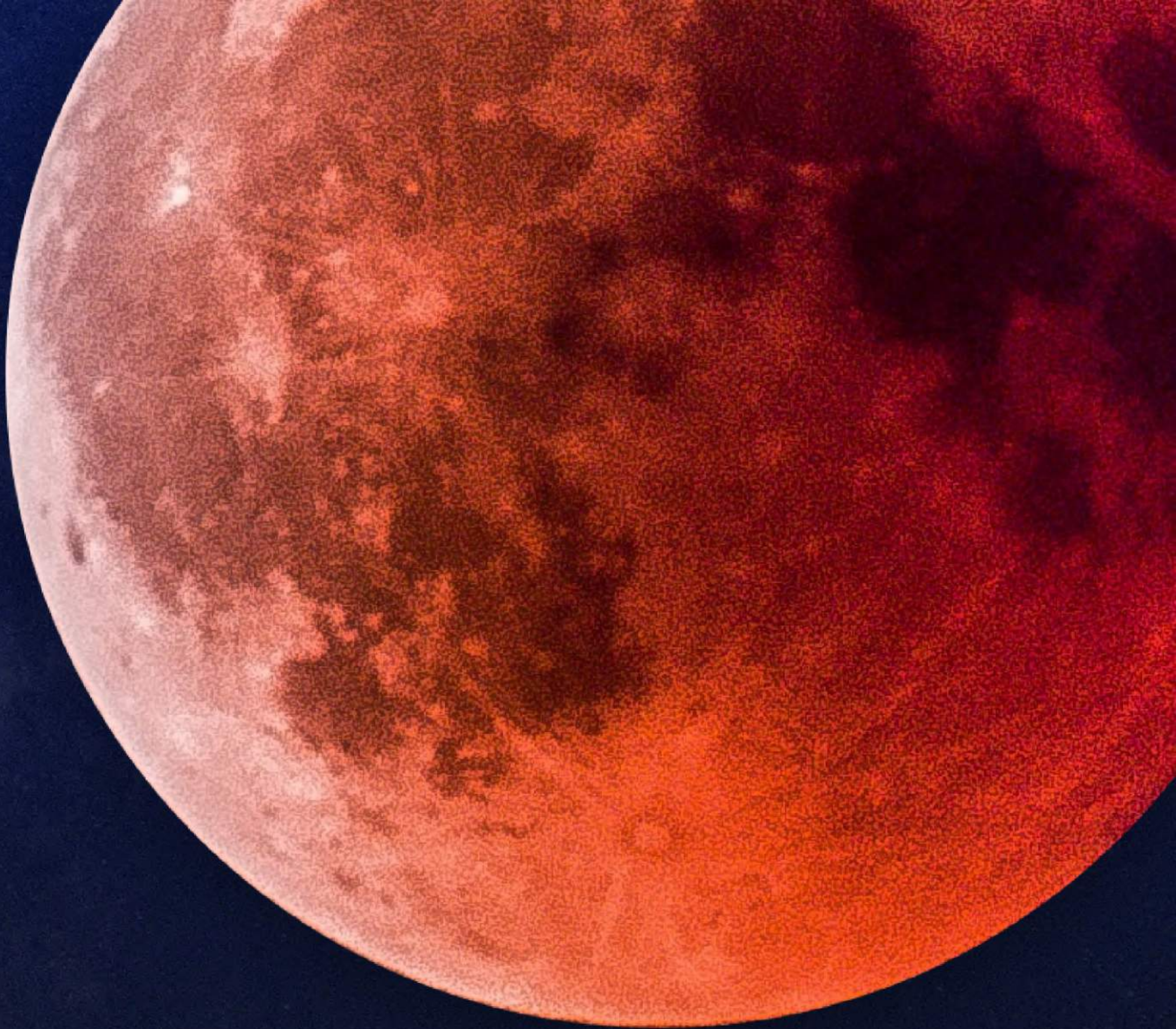


WHY?

Data Protection of private information is highest priority

Our customers depend on us to protect their information.

It is critical for all staff to understand what private information is, and how we can protect the security, availability and confidentiality of private information. As a company, we have committed to safeguarding our customer’s data and other assets they share with us.

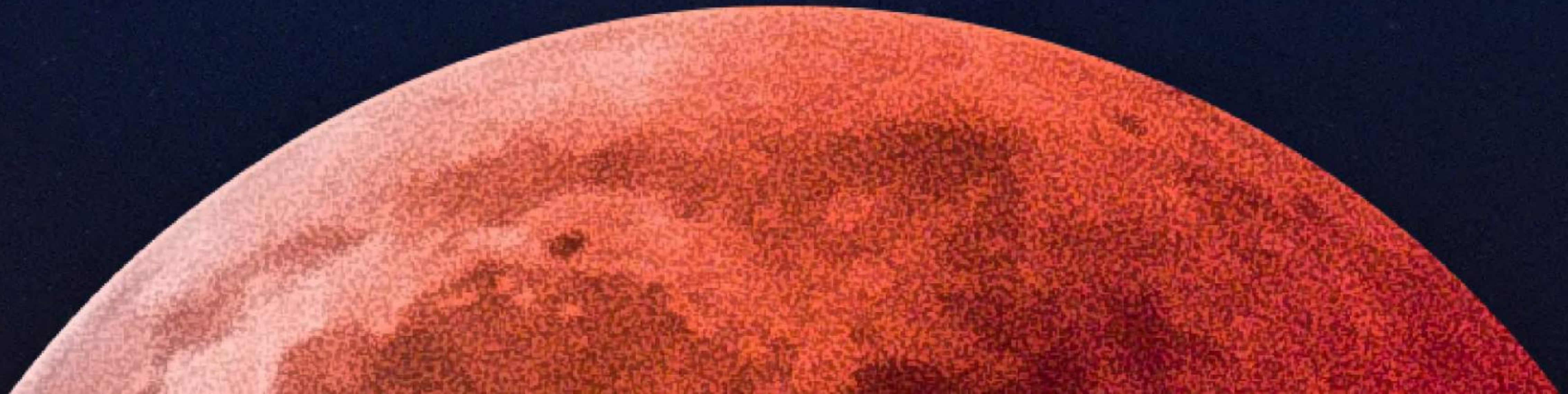


OUR MISSION: DEVELOP...

A basic understanding of privacy and our responsibilities in protecting personal data

SECTION 01

Data Privacy



What is data privacy?

- Data privacy, also called information privacy, is an aspect of data protection that addresses the proper storage, access, retention, immutability and security of sensitive data.
- Data privacy is typically associated with the proper handling of personal data or personally identifiable information (PII), such as names, addresses, Social Security numbers and credit card numbers.
- However, the idea also extends to other valuable or confidential data, including financial data, intellectual property and personal health information.

Elements of Data Privacy

Legal framework - Prevailing legislation enacted and applied to data issues, such as data privacy laws.

Policies - Established business rules and policies to protect employees and user data privacy.

Practices - Best-practices put in place to guide IT infrastructure, data privacy and protection.

Third-party associations - Any third-party organisations, such as cloud service providers, that interact with data.

Data governance - Standards and practices used to store, secure, retain and access data.

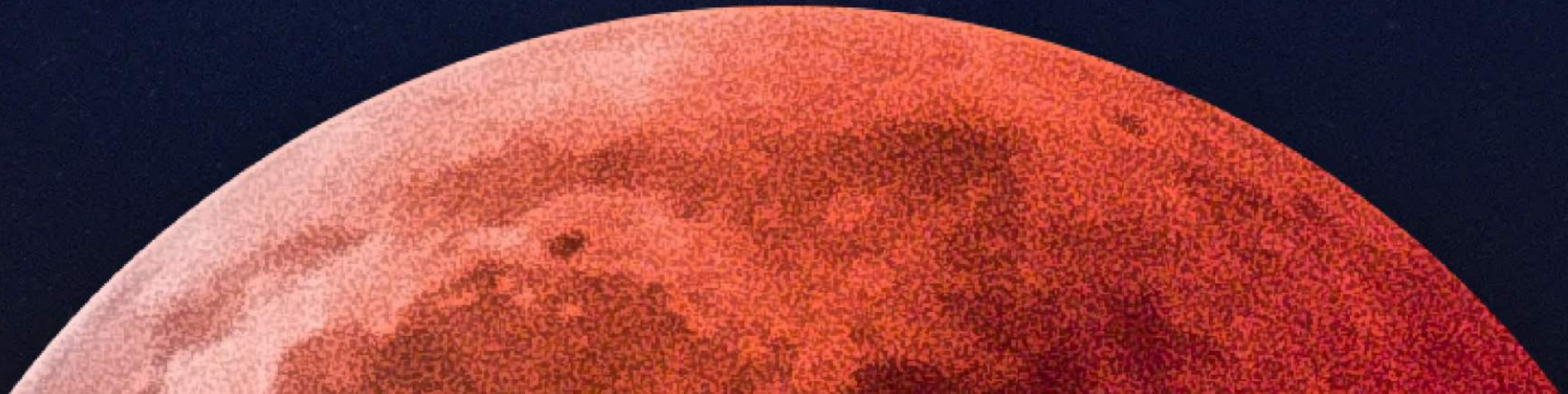
Global requirements - Any differences or variations of data privacy and compliance requirements among legal jurisdictions around the world such as the U.S. and European Union (EU).

Importance of Data Privacy

- Data privacy is a discipline intended to keep data safe against improper access, theft, or loss. It's vital to keep data confidential and secure by exercising sound data management and preventing unauthorised access that might result in data loss, alteration, or theft.
- For individuals, the exposure of personal data might lead to improper financial and credit activity, privacy intrusions, or identity theft.
- For businesses, unauthorised access to sensitive data can expose intellectual property, trade secrets, and confidential communications.
- A business may face significant regulatory consequences, such as fines, lawsuits, and irreparable damage to its brand and reputation.

SECTION 02

How to Protect Personal Data?



Principles for Processing Personal Data

LAWFULNESS, FAIRNESS AND TRANSPARENCY

Personal data shall be processed when it is necessary and meets one of the lawful basis for processing.

PURPOSE LIMITATION

Personal data shall be collected for **specific, explicit, legitimate** and **limited** purposes. We should not process this information for any other purpose other than its original intent unless it is permitted by law.

INTEGRITY AND CONFIDENTIALITY

Personal data shall be processed in a manner that ensures appropriate security including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage using technical or organizational measures.

STORAGE LIMITATION

Personal data shall be kept in a form which permits identification of the person for no longer than is necessary for the processing purpose.

DATA MINIMISATION

Personal data shall be adequate, relevant and limited to what is necessary to properly fulfil the processing purposes.

ACCURACY

Personal data shall be accurate and, where required, kept up to date.

ACCOUNTABILITY

The controller shall be responsible for, and be able to demonstrate compliance with the Data Protection Principles.

For Individuals

- Select strong passwords and change them frequently
- Use multi factor authentication (MFA) or biometric identification for critical accounts
- Don't click on links and buttons within emails from unknown senders
- Avoid providing PII that's unnecessary or not required
- Use malware tools and keep those tools updated
- Use only trusted apps and websites

For Businesses

- Collect only necessary private data to accomplish a task.
- Use strong authentication and MFA, such as user passwords or app credentials for APIs.
- Understand data sources, users, and storage locations.
- Employ access monitoring and logging to track data access.
- Use encryption and other security technologies to protect data.
- Back up data and test restoration.
- Ensure any third-party storage providers, such as cloud storage providers, share data privacy requirements and technique.
- Regularly educate partners and customers about data privacy guidelines.

My responsibilities as an employee

All employees hold a personal responsibility for ensuring that personal information is used fairly and lawfully. These include:

- Appropriate and secure storage for paper and electronic records
- Encrypt data on laptops, tablets, memory sticks, etc.
- Authorised access only, no password sharing
- Double-check your correspondence addresses and attachments
- Do not share information with third parties without data sharing agreements approved by the Data Protection Officer / Privacy Officer
- Destroy records appropriately and securely
- Be aware of your cloud usage
- If you are aware of a security incident (or a near miss), report the incident immediately to the designated officer so that the incident can be investigated and managed.

THANK YOU

Stay Safe