Data Protection for Migration Readiness

Any information that your organisation stores digitally needs to be properly protected. From financial information and payment details to contact information for your staff, data usage could be protected by law.

Data protection is not just a legal necessity, but crucial to protecting and maintaining your organisation.

Why is data protection so important?

Key pieces of information that are commonly stored by organisations, be that employee records, customer details, loyalty schemes, transactions, or data collection, needs to be protected. This is to prevent that data being misused by third parties for fraud, such as phishing scams, and identity theft.

What data needs to be protected?

Common data that your organisation might store, include:

- Names
- Addresses
- Emails
- Telephone numbers
- Bank and credit card details
- Health information
- Financial status
- DOB

This data contains sensitive information that could relate to your: current staff and their partners or next of kin; business partners and clients; members and beneficiaries; donors and other members of the public.

Protecting all this information, in accordance with the Data Protection laws, requires organisations to adhere to specific principles.

Law

The European Union General Data Protection Regulations (GDPR) contains a set of principles that organisations, government and businesses have to adhere to in order to keep someone's data accurate, safe, secure and lawful.

These principles ensure data is:

- Only used in specifically stated ways
- Not stored for longer than necessary
- Used only in relevant ways
- Kept safe and secure
- Used only within the confines of the law

- Not transferred out of the European Economic Area
- Stored following people's data protection rights

This comes into practice in business particularly when you recruit staff, amend staff records, market your products or services, or use CCTV.

Security

The principles of GDPR help businesses ensure the details of their staff, clients, partners and beneficiaries are properly protected.

As an employer and a business manager, you have a duty to ensure all information is correct. You should also confirm it is correct with the party in question (staff, when you create their employee record, or with donors if they sign up to give of their money, for example).

Following proper data protection procedures is also crucial to help prevent cybercrimes by ensuring details, specifically banking, addresses and contact information are protected to prevent fraud. For instance, your clients or donors' bank accounts being hacked into.

A breach in your data protection can be costly. And affected people, can pursue compensation against your organisation. You can also leave yourself open to punishments for failing to comply with data protection.

Non-compliance

Data Protection laws are key. Failure to comply can have serious consequences. Violating data protection law can see you and your organisation prosecuted, resulting in harsh punishments. These can include sizeable fines or action being taken that could result in a prison sentence.

Ensuring you adhere to data protection policies is crucial as the effects of non-compliance can be devastating for you and your business.