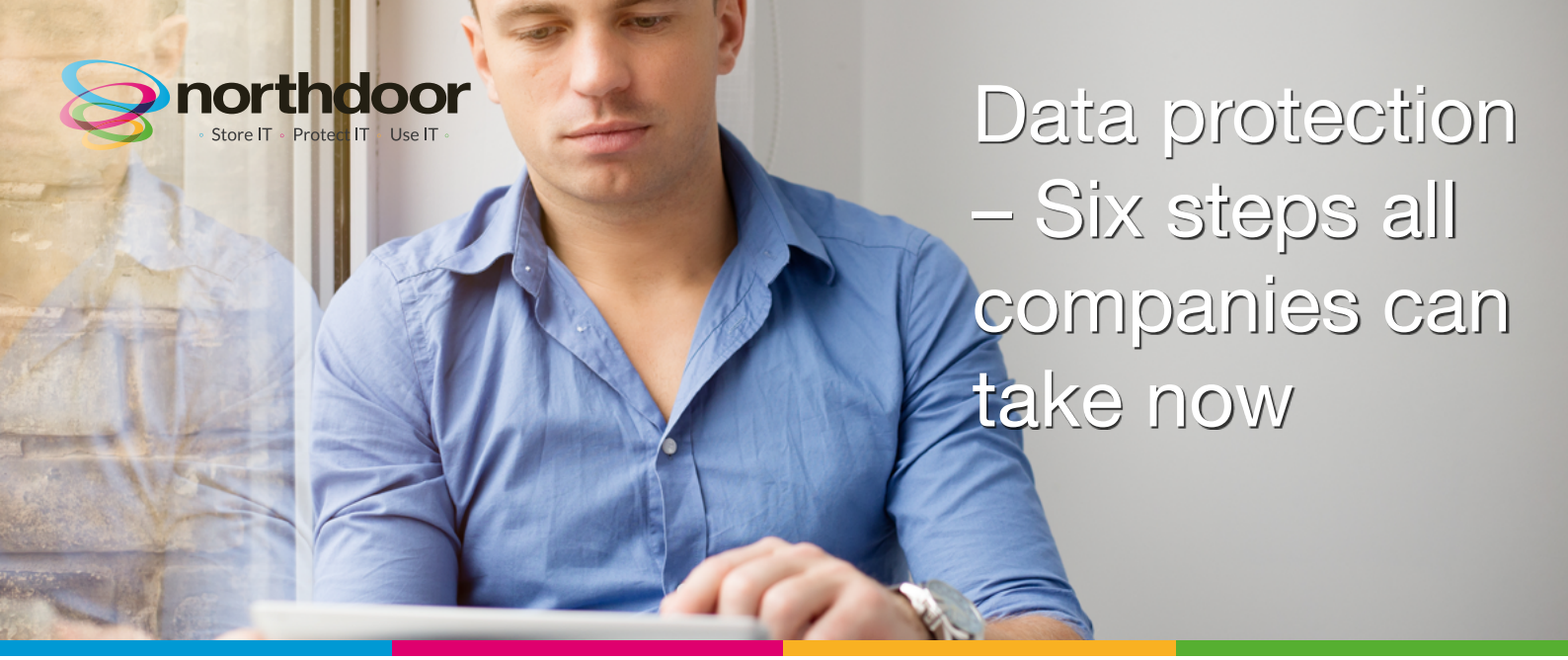

Data protection – Six steps all companies can take now

To avoid potential fines and reputational damage under legislation such as the EU's General Data Protection Regulation (GDPR), companies with European customers must understand the key obligations. Equally, companies are obliged under UK law (UK GDPR and DPA18) to apply essentially the same protections to UK customers. In this short paper, Northdoor outlines the six main steps to ensuring ongoing compliance.

Your business must fully understand what personal data it holds on both UK and EU citizens, where this data is stored and who has access to it, throughout the full information lifecycle.

Step one: the information you hold

Under current UK legislation, any information that could conceivably identify a person must be protected against loss or exposure. The challenge for businesses is to work out what data they hold and in which systems – both paper-based and electronic. In a networked world, you must also think about data you own and have shared with partners. The first stage in step one is simply to start the conversation with the business people who own the data and start to work out exactly what you have.

At Northdoor, we call this stage **Find IT**. Once you've found the data, you can **Classify IT**, and then you will need to create the right compliance structures around people, processes and technology: **Comply to IT**.

Even if you haven't yet precisely determined data ownership or risk, you can use simple solutions to encrypt everything at step one. The law requires you to protect data in the event of accidental loss, and full encryption is a fast and easy way to address this.

Step two: individuals' rights and consent

Once you have established what personal data you hold and taken the first steps to protect it through encryption, you should move on to understand the rights that individuals have over their data under the law. In short, these are: to access the data, have inaccuracies corrected, have some or all information erased, have it transferred to another organisation, have it removed from marketing lists and have it protected from automated profiling. Naturally, you will need to have measures in place for responding to requests to access, amend, transfer or delete data, and you will need to understand the legal deadlines.

This is also a good point at which to consider how you seek, obtain and record consent from individuals to hold their data. Consent must be a positive agreement – you may need to review your processes and put in place an effective audit trail for demonstrating that consent has been given.

Step three: subject access requests

UK GDPR and other regulations have strict rules for dealing with subject access requests, and you will need to check that your procedures are up to scratch. You should consider how you will comply with access requests, and you may also need to establish policies for rejecting unfounded or excessive requests for access or changes.

If your organisation is dealing with large numbers of access requests, you should consider creating an automated, self-service portal as a way to reduce logistical costs and delays.

Find IT

- Find the information you hold.
- Determine each individual's rights.

Classify IT

- Decide how to handle subject access requests.
- Determine legal basis for processing personal data.
- Ensure (and maintain) consent.

Comply to IT

- Encrypt data and protect it by design.
- Run data protection impact assessments.
- Build compliance awareness into all processes.
- Create an organisational culture of compliance.

Step four: the legal basis for processing personal data

As you examine the different types of processing you carry out on personal data, the UK GDPR requires you to identify and document the legal basis for that processing. For example, individuals will have a stronger right to request deletion of their data in cases where you use consent as your legal basis for processing.

For all activities, you should take care to document all actions, decisions and policies to help you comply with your accountability requirements under all relevant legislation.

Step five: data breaches

Under UK GDPR, breach notification applies universally to all organisations – though only those breaches where the individual is likely to suffer some form of damage will need to be notified.

During this step, you should ensure that you have the right procedures in place to detect, investigate and report on personal data breaches. You need to have the ability to notify individuals impacted by the breach within set timescales, and you should be aware that failure to follow breach-reporting guidelines could result in an additional fine on top of any penalty levied for the breach itself.

Step six: data protection by design and Data Protection Impact Assessments

The ICO has provided detailed guidelines on Privacy Impact Assessments (PIAs) which show how they can link to organisation processes such as risk management and project management. All companies should consider which scenarios may necessitate a data PIA (DPIA) and how such an exercise would be run.

In the past, a "privacy by design" approach to personal data was always considered best practice, and an implicit element in data protection. Under the current law, it is an explicit legal requirement, and as a result you need to verify that such an approach is embodied in your standard practices.

Kick-start your journey to compliance

To find out how Northdoor can help you comply with all relevant data protection legislation faster and more effectively, please contact us for an informal assessment. We'll review your existing approaches to data protection and security, and provide a clear checklist of recommended next actions, helping you get started quickly.