In May next year, the Data Protection Act (DPA) will be replaced by the EU's General Data Protection Regulation (GDPR), a framework with greater scope and much tougher punishments for those who fail to comply with new rules around the storage and handling of personal data.

While this new framework comes into place as the UK enters the process of uncoupling from the EU, the Great Repeal Act means it it is likely to be converted into British law.

General Principles

"a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and

against accidental loss, destruction or damage, using appropriate technical or organisational measures."

Article 5(2) requires that:

"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

What does GDPR mean for SMEs?

Among many new conditions, one of the biggest changes SMEs will face concerns consent. Under the new regulations, companies must keep a thorough record of how and when an individual gives consent to store and use their personal data.

And consent will mean active agreement. It can no longer be inferred from, say, a pre-ticked box. Companies that control how and why data is processed will have to show a clear audit trail of consent, including screen grabs or saved consent forms.

Individuals also have the right to withdraw consent at any time, easily and swiftly. When somebody does withdraw consent, their details must be permanently erased, and not just deleted from a mailing list. GDPR gives individuals the right to be forgotten.

GDPR forces SMEs to know exactly what personal data they hold and where it is located (whether on PCs, on servers, or in the Cloud), and have procedures in place to ensure its complete removal when a request to do so is made. Monitoring protocols must be able to recognise and act on breaches as soon as they happen, and an incident recovery plan put in place to deal with the repercussions.

"Privacy by design and default is the cornerstone of the GDPR," says Anita Bencsik, data security senior consultant at BT, which provides a consultancy service for businesses to check if they have got the right security in place.

She adds: "This stipulates that — from the initial stages onwards — organisations must consider the impact that processing personal data can have on an individual's privacy. This means, for example, that every new business

process or product that could involve personal data or impact the privacy of an individual, must be designed in accordance with data protection requirements."

Preparing for all this will require a full information audit and, for man

BT document

Data protection Already a good practice requirement, GDPR requires data protection (or privacy) "by design and by default" as a legal obligation.

To comply with this, organisations must embed data protection at every level of their enterprise and incorporate it into their processes. It means they have to take privacy into account throughout the whole lifecycle of any activity, to minimise privacy risks and avoid infringing data-protection rules.

To achieve this, a combination of detective, preventative, proactive and reactive security controls are needed. Every process, IT application, and area of infrastructure has to revolve around protection of privacy.

So, to adapt existing security infrastructure and ensure data is secure, organisations need to:

• gain a thorough understanding of how data moves around their organisation (and the associated processes) • have a specific workstream dedicated to security review (gap analysis and assessment) within their data-protection programmes • address gaps and (where necessary) redesign security architecture • implement technical and organisational security controls, including the development of security processes to detect and mitigate data leaks.

It doesn't end there, though. Monitoring and security are ongoing processes that organisations need to stay on top of to protect data and meet regulatory requirements.

GDPR essentials Here are the basics organisations need to know about this new EU regulation

Scope The new data-protection regulation — like the current DP Directive — affects all industries and organisations that process the personal data. It's also applicable to both public and private sectors.

Timings With its publication in the Official Journal of the EU, the regulation will come into effect on 25 May 2018.

Penalties In the event of a compliance breach, supervisory authorities can impose fines of up to four per cent of an organisation's worldwide annual turnover, or €20 million — whichever is higher.

Notification of data breaches Organisations have to notify their supervisory authority within 72 hours of any data breach, and they may also have to notify their customers.

Data Protection Officer (DPO) In certain cases GDPR requires organisations to appoint a DPO. A DPO must be an independent person who reports directly to management and has the responsibility to highlight any issues or concerns around the organisation's data protection compliance. Appointing an experienced data protection professional to head your data protection compliance, even if not legally mandated, is good practice and can be an effective way of demonstrating accountability.

Rights of the citizens Anyone who deals with a European controller will have the right to access and rectify their data, the right to be forgotten and the right to be informed about the purpose of any processing their data requires.

Data security As per existing regulations, organisations have to ensure they have technical and organisational security controls in place to guarantee the safety of any data they process. The GDPR is a good opportunity to review and tighten these controls.

The key trends of cloud computing, Big Data and IoT continue to cause major headaches when it comes to data security — but there's nowhere to hide when a breach occurs, and no excuses are acceptable if the breach is a result of security failings such as not implementing appropriate data-protection measures.

When the new EU regulation comes into force in May 2018, we'll see an increase in the level of fines that can be imposed for a data-security breach. But laws and regulations across the world (including within the EU) already enable regulators to impose fines and allow individuals to seek compensation via the courts.

Compliance should involve a holistic review of risk — looking at the classic trio of people, processes and technology. It will also need to be an ongoing effort and not just a one-off review. The new GDPR and the Digital Single Market Directive essentially mandate that security is built-in, not bolted-on as an afterthought, and that data is protected by design and by default.

In a nutshell, security is not just about complying with the rules, it's about protecting your customers, protecting your reputation, and protecting your future.