Progress
with Assure UK

GENERAL DATA PROTECTION REGULATION (GDPR)

11 Steps you need to take

11 WAYS IN WHICH YOU CAN PREPARE FOR THE GENERAL DATA PROTECTION REGULATION (GDPR)

1 Awareness

You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have and identify areas that could cause compliance problems under the GDPR. It would be useful to start by looking at your organisation's risk register, if you have one. Implementing the GDPR could have significant resource implications, especially for larger and more complex organisations. You should particularly use the first part of the GDPR's two-year lead-in period to raise awareness of the changes that are coming. You may find compliance difficult if you leave your preparations until the last minute.

2 Data security breaches

Start establishing a clear framework and policies to report any data breaches as quickly and efficiently as possible. This could involve assessing the types of data you hold and documenting which ones would fall within the notification requirement if there was a breach. Data controllers must notify most data breaches to the DPA within 72 hours of awareness. The data controllers must also notify the affect data subjects as soon as is feasibly possible.

3 New accountability requirement

A significant addition the GDPR imposes is the accountability principle. The GDPR requires you to show how you comply with the principles – for example by documenting the decisions you take about a processing activity. The measures should minimise the risk of breaches and uphold the protection of personal data. You also need to check that your staff are trained to understand their obligations. This is likely to mean more policies and procedures for organisations.

4 Incorporate privacy by design

Implement data protection by design and maximize privacy in any new process or product. Going forwards data controllers will need to maintain certain documentation and in some cases conduct data protection impact assessments (DPIA). By incorporating privacy by design you can gain a competitive advantage and demonstrate compliance.

5 Analyse the legal basis on which you use personal data

You should look at the various types of data processing you carry out, identify your legal basis for carrying it out and document it. For example, if you need to obtain consent, review whether your documents and forms of consent are adequate and check that consents are freely given, specific and informed. The GDPR is clear that controllers must be able to demonstrate that consent was given. You should therefore review the systems you have for recording consent to ensure you have an effective audit trail.

6 Children

You should start thinking now about putting systems in place to verify individuals' ages and to gather parental or guardian consent for the data processing activity. For the first time, the GDPR will bring in special protection for children's personal data, particularly in the context of commercial internet services such as social networking. In short, if your organisation collects information about children – in the UK this will probably be defined as anyone under 13 – then you will need a parent or guardian's consent in order to process their personal data lawfully. This could have significant implications if your organisation aims services at children and collects their personal data. Remember that consent has to be verifiable and that when collecting children's data your privacy notice must be written in language that children will understand.

7 Check your privacy notices and policies

The GDPR requires that information provided should be in clear and plain language. Your policies should be transparent and easily accessible. You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation. Under the GDPR there are some additional things you will have to tell people. For example, you will need to explain your legal basis for processing the data, your data retention periods and that individuals have a right to complain to the ICO if they think there is a problem with the way you are handling their data.

8 Data subjects and their rights

You should check your procedures to ensure they cover all the rights individuals have. The main rights for individuals under the GDPR will be:

> subject access,
>
> to have inaccuracies corrected,
>
> to have information erased,
>
> to prevent direct marketing,
>
> to prevent automated decision-making and profiling, and
>
> data portability.

On the whole, the rights individuals will enjoy under the GDPR are the same as those under the DPA but with some significant enhancements. If you are geared up to give individuals their rights now, then the transition to the GDPR should be relatively easy. This is a good time to check your procedures and to work out how you would react if someone asks to have their personal data deleted, for example. Would your systems help you to locate and delete the data? Who will make the decisions about deletion?

9 Data processors will have new obligations

One of the key changes in the GDPR is that data processors have direct obligations for the first time. These include an obligation to: maintain a written record of processing activities carried out on behalf of each controller and to designate a data protection officer where required. These obligations will need to be built into your policies.

10 Stricter cross-border data transfers rules

With any international data transfers, it will be important to ensure that you have a legitimate basis for transferring personal data to jurisdictions that are not recognised as having adequate data protection regulation. The consequences of non-compliance could be severe.

11 Data Protection Officers

You should designate a Data Protection Officer (DPO), if required, or someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. The important thing is to make sure that someone in your organisation, or an external data protection advisor, takes proper responsibility for your data protection compliance and has the knowledge, support and authority to do so effectively.

More information can be found on the Information Commissioner's Office website:

https://ico.org.uk/media/for-organisations/data-protection-reform/overview-of-the-gdpr-1-4.pdf

ANDREW RILEY
andrew.riley@assureuk.co.uk
Tel. 020 3540 3171

GARETH BURTON
gareth.burton@assureuk.co.uk
Tel. 020 3540 3170

PETER ENNIS
peter.ennis@assureuk.co.uk
Tel: 020 7112 8300

Assure UK
107 Cheapside, London, EC2V 6DN
T. 020 7112 8300