data|hq

GDPR CLIENT SURVIVAL GUIDE

Are You On Track To Meet The 2018 Deadline?

As of 25th May 2018, every organisation that does business in the EU will have to meet the new General Data Protection Regulation (GDPR) rules. This new law will be regulated by the ICO and the repercussions could be damaging with fines of up to 4% of global revenues. Compliance requires precise knowledge of the data you store and process, and the right data management policy across your organisation.

DataHQ DataHQ data-hq-ltd

10 Step Essential Guide

To ensure you are prepared, here is a checklist:

1. General Awareness

The first step in the process should be to ensure all key decision makers within the organisation are aware the law is changing to the GDPR and there is a deadline to ensure the organisation is compliant.

2. Is GDPR applicable to your organisation?

Understand what markets your organisation operates in. You might think because your organisation or head office is not based in the EU it's not relevant to you. However, its worth noting the GDPR does not only affect businesses within the European Union. Any organisation processing personal data related to the offering of goods and services (even if for free) to, or monitoring the behaviour of, data subjects within the EU are also affected. So this will affect many organisations outside the EU too!

3. Understand what personal data you hold

In this era of big data organisations hold vast amounts of data across numerous sources. We recommend organising a data audit to help understand and, in-turn, document what you have, where it came from and who you share it with.

4. Understand how GDPR affects your processes, data and systems

Organisations must identify and document the business processes where personal data is involved and also document how this data is processed. You must understand and assess the (privacy) risks associated to the business processes as well as supporting IT systems, plus you must implement controls and procedures to ensure data is kept confidential, is accurate, and is available when needed. And documentation only is not sufficient, you need to evidence the effectiveness of your measures, requiring continuous auditing and testing activities.

5. Check your Suppliers

Unfortunately; outsourcing processes to third party suppliers does not remove the organisations responsibility towards GDPR compliance. Where third parties are involved in your processing operations, you need to make sure they have the right control measures in place to secure and safeguard data privacy as well.

6. Ensure explicit and transparent consent of data

GDPR requires that people explicitly consent to the acquisition and processing of their personal data. Pre-checked boxes and implied consent are, in most cases, not acceptable anymore. Undertake a comprehensive review of how your organisation is seeking, obtaining and recording consent and where required, make sure changes are implemented.

With regard to children, consent from a child in relation to online services will only be valid if authorised by a parent (a child is someone under 16 years old). Member States can reduce this age to 13. There are other protections for children, including limiting the situations in which the 'legitimate interests' condition applies and providing them with a stronger "right to be forgotten".

7. Prepare for access requests

A general requirement is to make it easy for customers to withdraw consent if they wish. There is a new statutory "right to be forgotten" for data subjects who want their data erased. Under the GDPR, organisations have the obligation to also ensure deletion with all other parties with whom this data is shared. Also, the right of individuals to receive a copy of their data in a readable, portable format (data portability) aims to increase user choice of (online) services.

8. Implement processes for reporting data breaches

Ensure the correct procedures are in place to detect, report and investigate a personal data breach. A GDPR-defined personal data breach is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."

Notice must be provided "without undue delay and, where feasible, not later than 72 hours after having become aware of it."

9. Check your cross-border data transfers

Many of our clients operate across numerous territories. In case of international data transfers, it's 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.

10. Take accountability

The new GDPR legislation states that any organisation whose core activities involve "regular and systematic monitoring of data subjects on a large scale," or large-scale processing of "special categories of personal data" need to appoint a suitable, competent Data Protection Officer (DPO).

Frequently Asked Questions: GDPR

In order to support our clients we have summarised the most frequently asked questions, in relation to GDPR, together with answers:

When will the GDPR go live?

The GDPR becomes enforceable starting 25th May 2018. Its worth noting, the new regulation retains the same core rules as the Data Protection Directive (DPA) hence if you are already compliant you are in a strong position.

Our company is based out of the EU. Do we need to comply?

Yes. If you offer your goods or services to any EU residents, then you must comply with GDPR.

Do we need to comply given the upcoming Brexit?

Yes. The GDPR will go into effect before the 2-year leave deadline of Brexit (April 2019). Hence, barring new legislation, UK firms must comply with the GDPR. In addition, even after Brexit concludes, UK firms that offer goods or services to EU residents still need to comply.

We do not charge for services we offer. Do we need to comply?

Yes. The GDPR applies to firms that offer goods or services to EU residents irrespective of if payment is exchanged.

What happens if I do not comply?

You may be fined for up to 4% of your worldwide turnover (revenue). You may also be subject to lawsuits by affected data subjects.

What type of data is considered to be personal data?

The GDPR categorises a broad range of data, such as name, email, location, IP address, and online behaviour as personal data.

How do I obtain consent?

In general, consent needs to be explicit, opt-in, and freely given. This means popular opt-out based consent of today will no longer be acceptable.

Does my organisation need a Data Protection Officer (DPO)?

You must appoint a DPO if you represent public authorities or organisations that process large scale monitoring or processing of sensitive personal data.

How is B2B data affected by GDPR?

As it stands, B2B data for Sole Traders and Partnerships will be treated in the same way as B2C data and therefore, opt-in is required. For registered businesses, then the current guidelines from the ICO state that 'opt-out' will remain the standard.

However, you will have to comply with other rules to use opt-out; such as providing easy route to opt-out, the sender clearly identifies themselves and includes their registration number and contact details and the message is of a B2B nature.

Summary

GDPR is something you cannot run away from but if you plan and prepare carefully you should be ready before the new law becomes enforceable. Hopefully, the above checklist and FAQ's help with your planning.

If you require more advice, support or general guidance then please arrange a consultation with one of our data experts.

data|hq

DataHQ DataHQ data-hq-ltd

www.datahq.co.uk