The General Data Protection Regulation

Active Group Client Update

The General Data Protection Regulation ("GDPR") is a far-reaching piece of legislation designed to protect European Union ("EU") citizens from abuse of their personal data.

The GDPR replaces the current EU legislation which was enacted in 1995; a lot has changed since then. The advent of the digital age has drastically changed how we use our own personal data, and in turn what businesses use it for.

The GDPR does not only cover EU citizens; any country wishing to be considered by the EU as a trusted third party for data transfers will have to adopt its own local version of the GDPR requirements. This means that many countries will also have revised their data protection laws to protect their own citizens to the same standard. Any individual covered by a data protection law is referred to as a "Data Subject".

So, what does this mean for firms like yours?

Any firm which controls or processes personal data of either EU citizens or citizens covered by their local GDPR-equivalent legislation will need to review the end-to-end journey of this data. Additionally, data subjects will have greater rights to their personal data, and therefore it is in firms' interests to ensure they are able to act quickly and efficiently should they receive a Subject Access Request.

GDPR Project Guide

This paper is a guide to what your review project should include. At Active, our team of data protection specialists are well-placed to work in partnership with you on this project.

The below questions will help you gain an understanding of where to start, and where any gaps may need to be addressed:

1. *What personal data does the company need in order to provide its services?*

All business activities of the company, including any internal activities such as accounting and Human Resources, should be identified and addressed. The Data Protection Principles include Data Minimisation, which requires personal data to be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed". You should not be collecting personal data which is not necessary for your services.

2. *Under which lawful condition(s) has the personal data been collected?*

This question refers to the legal basis which has been used to obtain the personal data in the first place. Options include consent of the data subject, performance of a contract, and compliance with a legal obligation among others. It is important that this is defined, as this will then dictate what declarations need to be made to the data subject.

3. *What disclosures/declarations are made to data subjects when personal data is collected? And is the data being used solely for the purpose as disclosed?*

Tying up with question 2, it is important that data subjects are aware of what personal data the company is controlling/processing, and why. The company is then not able to use the data for any other purpose without the data subject's consent (barring compliance with a legal obligation, e.g. reporting suspicious activity under anti-money laundering laws).

4. *Where is this data obtained from?*

There are different provisions in the GDPR whether data is collected directly or indirectly from the data subject. If data is transferred to the company from an agent (e.g. an insurance broker to an insurer), then the agent also needs to ensure it is compliant with the requirements.

5. *Where is this data held? And does the company transfer any of this data to anyone else?*

It is really important to know where all relevant personal data is held, including where it may be transferred to other parties. This has to include outsourced service providers. Make sure that your agreements and contracts include the relevant terms and conditions.

6. *What security controls are in place for the data held?*

The company should consider not only electronic security such as password rotation, firewalls and server backups, but physical security too. In this age of digital data, it is easy to forget that a criminal still has the option to break into your office and walk away with your computer, if you give them the opportunity.

7. *What is the risk of personal data being hacked or lost?*

Human error is the top cause of data loss, so it is important that staff know what the company's vulnerabilities are. Ensure the Board assesses the risks of data loss either by internal or external factors. Your IT service provider will be best placed to help you. It is also worth investing in cyber security awareness training for your staff.

8. *What controls and reporting lines are in place to identify and report any data breaches?*

In the event of a breach, the company must be in a position to report to the relevant data protection authority in its jurisdiction. There will now be a legal obligation to report relevant breaches, and the time limit will be 72 hours after becoming aware. Firms need to ensure their breach reporting procedures are up to date to take account of this.

9. *How quickly could the company respond to a Subject Access Request?*

Data subjects have the right to request a copy of all the personal data a company holds on them. This has always been the case, except under the GDPR firms are no longer allowed to charge for this service (except in limited circumstances). This could mean it is be more likely to receive a request. The provision of information needs to be in a "concise, transparent, intelligible and easily accessible form, using clear and plain language", so firms need to ensure they are able to locate and convert any personal data if needed. The time limit for a response will also be shortened to within 1 month of receipt of a request.

10. *Do I need a Data Protection Officer ("DPO")?*

Any firm can choose to appoint a DPO, who would be responsible for monitoring compliance with the GDPR on an ongoing basis. The GDPR states that a DPO must be appointed if a firm is conducting regular and systematic monitoring of data subjects on a large scale, or processing special categories of data on a large scale. It is important to ensure that, should you need a DPO, a contract is in place which meets the requirements set out in the Regulation.

Responsibilities

Firms need to take ownership of their GDPR/Data Protection project, as no outside party will have insider knowledge of where data is held. It is also not a role to bolt-on to the Compliance Officer. It really needs to be a joint effort coordinated between all departments.

At Active, we can work in partnership with your project team/individual to guide them through the necessary requirements and help them manage what can become an overwhelming review. Our data protection specialists can help to map out data flows, assist in data audits, and draft policies and procedures. We can also write reports in order to help your staff to get buy-in from the Board.

Your Active consultant can talk you through all of the above steps and questions, and outline a project plan which will be tailored to your needs.

For more information, either speak with your Active Group Consultant, or email us on enquiries@activeoffshore.com for Guernsey, Jersey and Isle of Man enquires, and on info@active.com.mt for Malta and Cyprus enquiries.