March 2018

PROJECT SCOTLAND
THE SCOTTISH CONSTRUCTION NEWS MAGAZINE

Constructing compliance: what the industry needs to know about GDPR

POSTED ON MARCH, 2018 BY PROJECT SCOTLAND IN COMMENT

Lynn Richmond

By Lynn Richmond, associate in BTO Solicitors LLP's data protection team

COMING into force on 25th May 2018, the General Data Protection Regulation (GDPR) will change the way organisations within the EU must process personal data.

However, despite its imminence, the recent Cyber Security Breaches Survey 2018, commissioned by the UK Government, found that just 38% of businesses had heard of the GDPR, with businesses operating in the construction sector demonstrating the lowest rate of awareness at just 25%.

In 2016, 99.5% of the 5.5 million businesses in the UK were small and medium sized enterprises, of which nearly a fifth operated in the Construction Industry, providing three million jobs in the UK.

That is a lot of personal data and the chances are that if you operate in the construction industry you will be affected by GDPR. You will need to act fast to ensure compliance with this reasonably complex piece of legislation.

What is the GDPR?

In a nutshell, the GDPR focuses on six key elements that all data Controllers and Processors need to abide by:

1) *Lawful and Transparent Processing*: Processing of personal data must be conducted in a lawful but also fair and transparent manner, with an emphasis on the latter two.

2) *Purpose*: There has to be a specific and legitimate reason behind the collection and processing of personal data. It can only be stored and used for a specific, well defined purpose.

3) *Minimisation*: In order to reduce the impact of any potential data breach, the minimum possible amount of data necessary should be collected and stored.

4) *Accuracy*: Personal data should be precise and continuously updated. Data subjects have a right to demand data be corrected or no longer processed.

5) *Storage*: As soon as the data is no longer necessary for its defined purpose, it has to be deleted.

6) *Security*: Data should be stored in a secured manner. This includes not just encryption of files and limiting access to only a select number of staff, but also not sharing it with countries not deemed to uphold the same standard of security imposed by the regulation.

Does it affect me?

Personal data is defined as any piece of information that can ultimately lead to the identification of an individual, such as:

• Name or contact details;

• Address;

• Location data;

• Personal identification number;

• Website, apps and/or software identifiers;

• IP address;

• CCTV footage of an individual;

In short, if you store any personal data of individuals, be it employees, applicants, customers or potential customers, among various others, you need to understand how the GDPR affects you.

How does it affect me?

Considering the UK Government's statistics, that in 2015, 15% of construction business premises were affected by online crime with the Home Office figure of 77,000 incidents of online crime against construction companies, the question of personal data being compromised might not be 'if' but 'when'. Aside from legal compliance, following the rules set out in the GDPR can contribute to what is arguably the most important part of a successful business – a good reputation and customer trust.

However, while the GDPR gives you an opportunity to enhance your business, the Information Commissioners Office (ICO) now has vastly increased powers to fine those who do not comply. Those fines can reach up to 20 million euros or 4% global turnover.

What do I need to do about it?

Adapting the way you control and process personal data to comply with the GDPR could be a serious endeavour which will likely require professional advice and assistance. In the meantime, consider the following as a good starting point:

1) *Policies and Procedures*: Carefully adapt your data protection policies to reflect the GDPR requirements and review and update them regularly.

2) *Training*: Having policies in place is one thing, but the staff need to know what they mean in practice. Invest in regular training, to ensure they are well prepared and informed.

3) *Inspections*: Systematic internal audits can help you ensure that your procedures and policies follow the GDPR guidelines.

4) *Assign a DPO (Data Protection Officer)*: Some organisations will be required to have DPO as standard, but even those that don't should consider the practical benefits this will provide for their business. This service may also be outsourced.

5) *Security*: Revise your security methods, encrypt data, and install updates and security patches. Determine who has access to your data, and with whom (and where) you share any data.

6) *DPIA (Data Protection Impact Assessment)*: Conducting a DPIA is the first thing you want to do before you start adapting your policies and updating your systems. Find vulnerabilities, and find a way to fix them.

Hopefully business will view the GDPR not as a 'nuisance' or a 'tick box' exercise to avoid fines, but as an opportunity to implement positive change that will enhance reputation and customer trust, leading to a better, safer and more aware company growth.