

A BEGINNER'S GUIDE TO

GENERAL DATA PROTECTION REGULATION

Edenhouse Solutions

www.edenhousesolutions.co.uk

info@edenhousesolutions.co.uk



What is GDPR?

The General Data Protection Regulation (GDPR) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union. GDPR furthermore addresses the export of personal data outside of the EU. Applicable as of 25 May 2018, The General Data Protection Regulation will replace the Data Protection Regulation 1995 with its primary objective to give individuals back control and protection of their personal information and what happens to it.

When will the new law come into force?

On 27 April 2016 The General Data Protection Regulations were adopted by the EU and entered into force on 24th May 2016. There is then a two-year transition before it is applicable on 25 May 2018

Who does the new law affect?

GDPR applies to EU and non-EU companies that manage or process personal data of individuals' activities in the EU.



What are the main changes under the regulation?

- If your business is not in the EU, you will still need to comply with the regulation.
- The definition of personal data is broader. Data privacy encompasses other factors which could be used to identify an individual, e.g. genetic, mental, economic, cultural or social identity.
- The rules surrounding valid consent have been clarified, clear and affirmative consent must be provided, silence or inactivity does not constitute as consent.
- Processes must be built on the principle of privacy by design, there has always been the requirement that systems and processes must comply with the principles of data protection.
- The right to be forgotten enables an individual to request the removal of personal data if there is no compelling reason for its continued processing.
- For companies where the core activities involve regular and systematic monitoring of data subjects on a large scale, it will be mandatory to appoint a Data Protection Officer.
- There are new requirements for data breach notifications, all data breaches should be reported to the data protection authority unless it is unlikely to represent a risk to rights and freedoms of the data subjects in question. The notice must be made within 72 hours of data controllers becoming aware of the breach.
- There are new restrictions on international data transfers, organisations should be made aware of the risk of transferring data to countries which are not part of the EEA.
- Data processors share the responsibility for protecting personal data, which means that processors can be held liable for data breaches.

What are the penalties of non-compliance?

Failure to comply with GDPR may result in considerably tougher penalties. Organisations found in breach of the regulation can expect administrative fines of up to 4% of annual global turnover or €20 million – whichever is greater.

What about Brexit? Does that mean that we still need to comply?

Regardless of Brexit, UK organisations handling personal data will still need to comply with the GDPR. The GDPR will come into force before the UK leaves the European Union, and it has been confirmed by the government that the regulation will apply.

What core business areas will be impacted by GDPR?

Any business area which involves personal data will be impacted by the new regulation e.g.

- BW – personal data held in data warehouses
- E-commerce, purchase and sales orders
- HR and employee records e.g. sickness records
- Expenses – invoice and bank details, including credit card details



What should I do first?

Firstly, organisations need to understand where and how their personal data is stored across their entire IT landscape. Organisations should then review and audit their data to see whether any information could be used to identify an individual either directly or indirectly, then a process should be put in place to implement data and procedures management, securing the data within the organisation and any third parties. Lastly organisations need to ensure that policies are in place with regards to breach notifications, consent and security.

Are there any SAP Solutions that can help me comply with GDPR?

There are a number of SAP solutions that can help you identify and manage your data - helping you to comply with the GDPR regulations.

How can Edenhouse help?

For more information on what services and solutions are on offer and how our consulting team can help you understand the impact of GDPR on your business, then please contact your Service Delivery Manager or Account Director for more details.

Disclaimer:

This document does not constitute as legal advice or other professional advice and is provided for general information purposes only. No warranty, whether expressed or implied is given.



Head office
Quartz Point
Stonebridge Road
Coleshill
Warwickshire
B46 3JL

Farnborough office
Cody Technology Park
Ively Road
Farnborough
Hampshire
GU14 0LX

Manchester office
Parkway 4
Parkway Business Park
Princess Parkway
Manchester
M14 7HR

+44 (0) 121 767 9280 | info@edenhousesolutions.co.uk | www.edenhousesolutions.co.uk

Registered address: as head office | Registered in England and Wales No. 6498946 | VAT Number 177 9275 53

