VinciWorks

GDPR: 10 things to do now

Your 10 step guide to GDPR

Introduction

The General Data Protection Regulation (GDPR) will officially come into force on 25 May 2018. GDPR's reach is global. Any company that offers goods or services to anyone in the EU will be required to comply.

If you haven't started to comply, or are not sure what to do next, following these steps will help ensure you are ready for GDPR day.

1. Undertake a data audit

Organising an in-depth data audit across your organisation and all parts of the business is crucial to understanding where data exists, how it is used, and what should be done next. Think of data like oil running through an engine; it powers your organisation and makes it function, but it can also leak if the various conduits are not working properly. After an audit, you should be better able to identify risks, weak spots and priority areas to address.

2. Identify and document the lawful basis for data processing

To legally process data under GDPR you must have a 'lawful basis' to do so. For example, it is a lawful basis to process personal data to deliver a contract you have with an individual. There are a number of different criteria that give you lawful basis to process and crucially, different lawful basis' give different rights to individuals. If, for instance, you rely on consent as a lawful basis, individuals have stronger rights to have their data deleted.

3. Update your privacy policy

People need to know why their data is being collected, why it is being processed and who it is shared with. You should publish this information in your privacy notice on your website and with any information you send to people. The information must be concise, transparent, intelligible and easily accessible. It must be written clearly and in plain language, and must be provided free of charge.

4. Ensure all staff are trained

Training is crucial to a successful transition to GDPR. Different people in the organisation will require different kinds of training. For example, people in the marketing team will need to know about things like consent and direct marketing, while the IT department will need some extra technical level training to update and secure your systems.

5. Review how you collect consent

You don't always require consent for handling data, but if you are relying on it and asking people for consent to use their data, it must comply with GDPR. Consent must be freely given, kept separate from other terms and conditions, requires positive opt-in, not be a precondition of the service, and inform people that they can withdraw their consent at any time. If the current consent you are relying on does not meet GDPR standards or is poorly documented, you must seek new consent, rely on a different lawful basis, or stop the processing altogether.

6. Appoint a data protection officer (DPO)

Most businesses will need to appoint a DPO. The function can also be outsourced, but the DPO must report to the highest level of management, have adequate resources to do their job, and have special protections from being easily dismissed. Public authorities, organisations that process large scale or systematic monitoring or carry out large scale processing of special categories (sensitive) data are required to appoint a DPO.

7. Review third party contracts

If you send data to someone external for processing, there needs to be a contract in place with some specific clauses mandated by GDPR. You are liable for your processor's compliance with GDPR and must only appoint processors who can assure they have sufficient guarantees in place to protect the data in accordance with GDPR.

8. Get your subject access request process compliant

Data subjects are entitled to find out what personal data is held about them by an organisation, why the organisation is holding it and who else knows the information. The information must be provided free of charge, provided in an electronic format if requested, and the organisation has one month to respond.

9. Implement more privacy procedures into your workflow

There is a specific obligation to implement appropriate technical measures to integrate maximum privacy features into what you do. For example if you are undertaking a new process that collects data, you must implement privacy and data protection procedures from the design of the project. If it is a new feature or product, then privacy settings must be set to maximum by default. Conducting a Data Protection Privacy Impact Assessment (DPIA) can help you identify the best way to comply with your data protection obligations and meet people's expectations of privacy. You must carry out a DPIA when you are using new technologies or when the processing is high risk.

10. Get ready to delete or move people's data

People have the right to obtain and reuse their data across different services. They can request that their data be moved, copied or transferred from one organisation to another in a safe, secure way, free of charge. Data must be provided in a structured, machine readable format such as CSV or XML files, sent to another organisation where this is possible, and be completed within one month. People also have the right to be forgotten and can request that their data be erased.

To learn more, email training@vinciworks.com or call +44 208 815 9308.

www.vinciworks.com