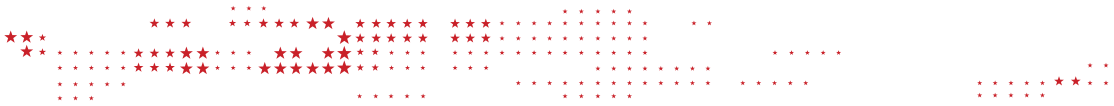
redstor

Working with GDPR *compliant vendors*

SEPTEMBER 2017 | WWW.REDSTOR.COM

Contents



What is the GDPR?

The primary focus of the General Data Protection Regulation (GDPR) is to improve the security of data for data subjects and to update outdated regulations across all of Europe.

The GDPR replaces the previous Data Protection Directive (DPD), which was adopted in 1995. In the UK, the GDPR will also replace and strengthen the Data Protection Act (DPA). The regulation will be passed into UK law in the form of the New Data Protection Bill.

Key points under GDPR include:

- **More focus on the protection of personal data**
- **Higher fines for non-compliance (€20 million or 4% of global revenue)**
- **Breaches must be reported within 72 hours to the relevant supervisory authority**
- **Will apply to any organisation that does business with or holds data on any EU subject**

What's new?

There are several areas under the GDPR that are significantly different to previous data acts, specifically ones that relate to the protection of personal data.

The definition of personal data has also been updated and now refers to **'any information relating to an identified or identifiable person (data subject)'**. This now includes information such as an IP address.

To help ensure the protection of personal data, there are now circumstances where organisations must appoint a **Data Protection Officer (DPO)**, including all public-sector organisations.

In addition to this, breaches must be reported to the Data Regulatory Authority (The ICO in the UK), within 72 hours and fines for non-compliance are much larger. Companies also have an obligation to respond to any EU's individual's (data subject's) requests about their personal data within one month.

What do vendors need to do to be compliant?

Historically, data protection has been the responsibility of the Data Controller. In the event of a data loss or breach that was caused by the Processor, only the Controller would be accountable. Along with the renewed focus on personal data, there is now a greater focus on any person or organisation that handles data i.e. data processors.

Processors will be jointly and separately liable with controllers for compensation claims by individuals.

GDPR365

Redstor has entered into a strategic partnership with GDPR compliance experts, GDPR365, to provide customers with a technical compliance software tool to measure and facilitate GDPR compliance. As a Data Processor, Redstor understands the enhanced level of responsibility it has under GDPR to ensure the security of individual's personal data. We are committed to working with end-users and partners to ensure their adherence to the regulation.

GDPR365 was started by lifelong software entrepreneurs who have built successful cloud-based businesses involving large volumes of sensitive personal data, including services built on the Redstor Pro technology.

GDPR365 always compliant

GDPR365 has an intuitive interface and thoughtful workflow that will simplify the compliance journey and organizes it into clear, simple tasks that improve collaboration across departments through a cloud based hub. It provides visibility and accountability with complete oversight of all compliance issues that are in process.

Each company receives a customized data protection journey and governance documentation based on an initial self-assessment. Tools to manage subject access requests, data breach incidents, records of processors and client and employee notices make sure the risks related to regulator compliance are reduced.

GDPR365 is a one of a kind application that assists marketers in ensuring ongoing compliance with GDPR.

GDPR365 reduces the risk of non-compliance by assisting with:

- Understanding how to be GDPR Compliant
- Assessing organisational compliance
- Understanding requirements for appointing a DPO
- Governance
- Processor and Data Sharing
- Training of staff and employees
- Subject access requests
- Data breach incidents
- Maintaining records of processors
- Client and employee notices

Supplier checklist

This short checklist should be completed per supplier (data processor) and will quickly help you understand their level of compliance and how they can assist in your compliance.

- **Has the processor taken measures to ensure they are GDPR compliant?**
- **How will the processor help your organisation become GDPR compliant?**
- **Are solutions/services ISO 27001 certified?**
- **Do they have any certifications around data security?**
- **Where does the processor store data?**
- **Who within the processor can access data?**
- **Does the processor need a DPO? If so, who is it?**
- **What is the process if the organisation suffers a data breach or data loss?**
- **What organisational measures have they taken to ensure a level of security appropriate to the risk?**

Glossary

All definitions under the GDPR are listed under Article 4

Personal Data – Any information relating to an identified natural person ('data subject').

Processing – Any operation or set of operations which is performed on personal data or on sets of personal data.

Pseudonymisation – The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information.

(Data) Controller – The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

(Data) Processor – A natural or legal, public authority, agency or other body which processes personal data on behalf of the controller.

Consent – Any freely given, specific, informed and unambiguous indication of the data subjects wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.