The 12 step
GDPR Compliant Checklist

By Richard Moore

OrbusSoftware

Orbus Software can help you start down the road to compliance. Perform step one (Awareness) today with the purchase of Orbus Software's GDPR Action and Implementation online course. Specifically designed for mobile learning, you can study on your phone, tablet and laptop.

The General Data Protection Regulation (GDPR) will come into force on the 25th May 2018. Currently many organizations are considering the actions to take to become compliant before the deadline. To help them, the UK's Information Commissioner's Office (ICO) has published 12 steps to take on your road to GDPR compliance. Orbus Software presents them here.

1 Awareness

The GDPR will have implications across any organization; sales, marketing, HR, IT and many other departments will need to understand how it might affect their day-to-day work. Employees from the senior decision-makers downwards will need to be aware of their own responsibilities and obligations.

2 Information you Hold

One of your first steps in compliance will be to survey the personal data that you currently hold, possibly in the form of a data audit. Document the source of your data, and any further sharing of the data you currently conduct.

3 Communicate your Privacy Information

Any data audit should be accompanied by a survey of your current Privacy Notices. Document any changes you may need to make in content (what is your legal basis?), location, format and timing.

4 Your Data Subject's Rights

Review your procedures in light of the rights of the Data Subject established under the GDPR. How long are you retaining data? How is data deleted? Are you able to provide information in a "portable data format"?

5 Subject Access Requests (SARs)

Preparing your organization for the efficient handling of Subject Access Requests will be a key part of implementing the GDPR. You might consider creating GDPR-compliant response letters to ensure that Subject Access Requests are properly replied to. Look at establishing the technical procedures necessary to compile an individual's data quickly and in a compliant format. Staff awareness will need to be high. Subject Access Requests may arrive anywhere in the organization, across many departments. It is essential that the first response is considered and well thought out.

6 Your Lawful Basis for Processing Personal Data

Review your processing activity in light of the legal bases for processing set out under the GDPR. Document the lawful basis of your data processing, and make it plain in your Privacy Notice.

7 Consent

As part of an initial personal data audit, review how you are currently seeking consent, and how you record and manage it and, ultimately, whether you need to make changes. If you have current consents that do not stand up under the GDPR, then actively seek out new consents from the Data Subjects.

8 Children

Consider whether your organization processes the data of vulnerable Data Subjects (especially children). You may need to take measures to make sure you are verifying Data Subject's ages, and whether your processing requires parental or guardian consent.

9 Data Breaches

The GDPR contains new legal obligations regarding data breaches and notifications. Take a look at your measures todetect, report and investigate a breach of personal data.

10 Privacy by Design and Data Protection Impact Assessments (DPIAs)

Organizations should be assessing risks to Data Subject's rights when conducting any project planning or business modeling. Organizations are also obligated to demonstrate their compliance with the GDPR. To this end, you should familiarize yourself with the current guidance on implementing Data Protection Impact Assessments. Look at how to implement them, when to implement them, and what they should cover.

11 Data Protection Officers (DPOs)

At an early stage organizations should identify someone whose role is to take responsibility for GDPR compliance. Work out where this role sits in your organizational structure. Study the current guidance on the Data Protection Officer, seek counsel, and decide if you are required to appoint one.

12 International Aspects

Should your organization conduct operations across more than one EU member state, you must seek counsel on which local supervisory authority is most relevant (the ICO in the UK, for example). Look to WP29 to help you do this.

ORBUS SOFTWARE RESOURCES:
https://www.orbussoftware.com/resources/