Ten steps to GDPR
A compliance checklist

Ascentor Ltd
5 Wheatstone Court
Waterwells Business Park
Quedgeley
Gloucester
GL2 2AQ

www.ascentor.co.uk

Ten steps to GDPR compliance checklist

The launch date of 25th May 2018 is fast approaching and the General Data Protection Regulation (GDPR) will be on every organisations priority list.

Do you know where to start?

If you're not sure, the following steps will help you prepare for compliance.

This checklist is a summary of our recent article Ten steps to GDPR compliance which contains additional information on each step.

1. Data Protection Officer

The Data Protection Officer (DPO) will play a key role in ensuring compliance with GDPR – but it's not immediately obvious what is involved. If you are a public authority then you're obliged to appoint one - and many private sector organisations will require one too.

The role of the DPO is covered at length in the Ascentor blog article Do you really need a Data Protection Officer (DPO)?

2. Train your staff

People are the one of the biggest risks you face in terms of failure to comply. Once all your staff are onboard with GDPR and understand what they need to do, you'll be in a better position to ensure compliance is built in to day-to-day processes and isn't seen as an additional burden.

3. It's got to be fair

You'll probably need to update your fair processing and privacy notifications to customers and maybe even your staff. Review whether or not the information you provide to individuals is explicitly clear. Ensure you put in place a process for regularly reviewing and if necessary updating your fair processing information.

4. With your permission

The new Regulation is designed to ensure you gain consent for every purpose (when you rely on it as the condition for carrying out processing). Consent needs

to be opt-in (not opt-out) and customers need to genuinely understand your conditions and agree. The key consideration here is that consent must be freely given.

5. Another legal basis

If you can't rely on consent for processing some or all of your personal data, you must find another legal basis on which to carry out your processing. Aside from consent, the Regulation sets out additional bases (covered in more depth in the full article). If you cannot meet any of them for the personal data you're processing, then the particular activity has no legal basis and cannot continue.

6. Privacy impact assessments

Privacy impact assessments (PIAs) are now mandatory for processes and systems processing high risk data. One of the key ways of determining whether or not a process or solution will present a high risk to the rights and freedoms of data subjects is to carry out a PIA. You should consider having in place a means of standardising these into your assurance processes.

7. Forget me (The right to be forgotten)

The right to be forgotten (Article 17) is the new data subject right causing most discussion. If you are required to action a request for data removal under this right it's essential that you are able to remove the data from all sources where you hold it. This includes backups. It is wise to develop a process now to ensure you are able to action such requests.

8. Review and update agreements

Data sharing and processing agreements you have or are party to are likely to reflect current data protection law. The legal basis you are currently using for these agreements may change or cease to exist. It is essential to review the agreements you have in place and take time to amend these to reflect the requirements of the new Regulation.

9. Secure IT (and manual data too)

Providing adequate protection for the data you process is essential for compliance with the Regulation. Data subjects will expect that their information

will be held in ways which it cannot be accessed by those without appropriate authority. Physical and procedural security controls will be just as important as technical ones.

10. Map your data flows

If you don't know what data is going where, you'll struggle to comply with the requirements of the Regulation. Mapping your data flows provides a clear picture to your organisation of how data are travelling around, helps you identify abnormalities or non-compliances with your policies and procedures and facilitates your taking appropriate steps to manage information risk.

Additional GDPR resources

From Ascentor

Ten steps to GDPR compliance

Do you really need a Data Protection Officer (DPO)?

GDPR: What does it really mean for your organisation?

From the Information Commissioner's Office

Getting ready for the GDPR

Preparing for GDPR: 12 steps to take now

GDPR guidance: What to expect and when

For further information

If you'd like to discuss the topic of GDPR and data protection in more depth or any aspect of IA and cyber security, please contact Dave James, MD at Ascentor.

Email: info@ascentor.co.uk
Office: 01452 881712
Web: www.ascentor.co.uk