Are you prepared for the EU General Data Protection Regulation (GDPR)?

In many countries, there are laws and regulations in place to protect the privacy of people. But they differ from country to country hampering the exchange of personal data between public and private sectors, associations and enterprises. When it comes to the digital world, the topic needs to be handled on a supra-national level.

Therefore the European Union has adopted the General Data Protection Regulation (GDPR), which entered into force on 5 May 2016 and will be enforced from 25 May 2018 onwards in all EU countries. The GDPR regulates how government institutions and organisations in private, public and semi-public sectors should handle and process personal data in order to respect the privacy of individuals living in the EU.

The GDPR will have a large impact on the operations of all organisations handling personal data.

How to prepare for the GDPR?

Secura offers support from creating awareness to verifying if the GDPR has been implemented correctly with the services as shown in the figure on the next page.

1. GDPR Awareness Session

We can organise an interactive workshop for you to explain the GDPR, the impact and the reach. This will help to scope the next phases.

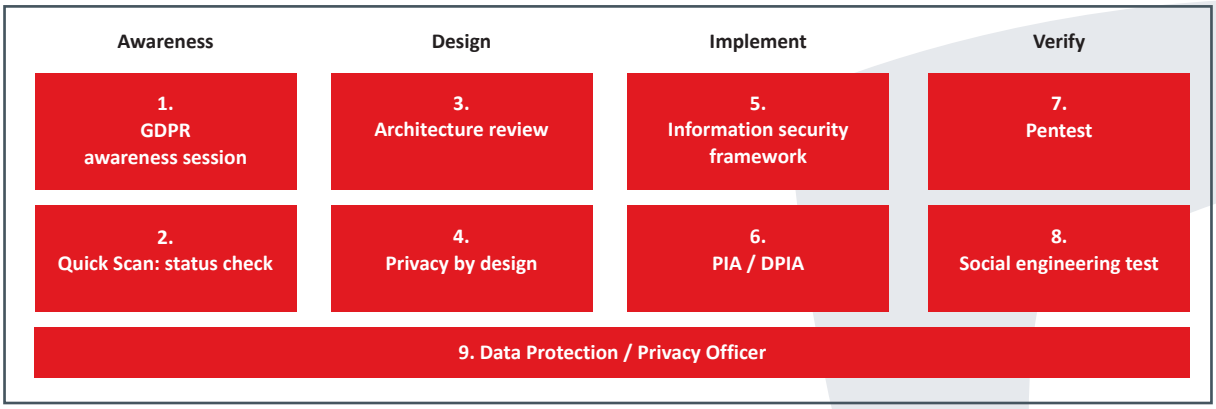
2. Quick Scan: status check

Perform a Quick Scan to get a clear overview on the work that needs to be done to prepare for the GDPR. Secura can execute a Quick Scan by interviewing stakeholders and reviewing documentation. The deliverable is a gap analysis including a concise plan of actions that need to be taken to comply with the GDPR (technical, legal & governance).

3. Architecture review

Perform an architecture & design review

a. Identify the data flows, categorizing (3rd party) processors, sub-processors, shadow IT, back-up infrastructure, etc.



b. Identification and Access Management check: Is authorization and authentication well-organised laid down in procedures and have they been well-defined?
c. A scope check of personal data processing: Review encryption and pseudonymization (GDPR Article 4.5) policies & implementation.
d. Perform a risk analysis to determine if your processing is considered high risk to data subjects.
   You will receive a detailed report identifying areas of risks as well as improvement suggestions.

4. Privacy by design

Data Protection by design and by default. A more structural, future proof approach is security or privacy by design (GDPR Article 25). Principles like lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation and integrity & confidentiality can then be implemented straight from the start. Secura can help you to train your staff and/or design your systems for data protection and privacy.

5. Information security framework

Implement an Information Security Management System (ISMS) containing a framework (such as ISO 27001 or the NIST Cyber Security Framework). This is mandatory for controllers and processors in the GDPR (article 32). This includes:

a. putting the privacy & security organisation in place (RACI)
b. procedures for data breach notification (GDPR, Article 33)
c. Plan-Do-Check-Act cycles
d. Regular Risk Assessments
e. Certification according to the standard

Secura provides support to implement ISO 27001 and can perform ISO 27001 pre-audits.

6. PIA / DPIA

Conduct Data Protection Impact Assessments (DPIA, GDPR Article 35) – In case of a major change in the procedures or systems or an upgrade of the applications in use a DPIA needs to be performed which focuses on providing a clear description of the processing, processor agreements, risks & mitigations, security measures, etc. Secura can perform the DPIA and provide a compliancy report on this.

7. Pentest

Perform regular penetration tests, social engineering tests and Red Teaming exercises on your infrastructure and applications to ensure that security of systems and procedures is implemented well in reality.

8. Social engineering test

Secura can provide professional and creative social engineering services to test the human factor and raise awareness.

9. Data Protection / Privacy Officer

Secura can also offer you a professional interim Data Protection Officer. The DPO will support you to implement the GDPR quickly and effectively.

Interested?

Would you like to learn more about our services?
Please do not hesitate to contact us.

Secura

Vestdijk 59
5611 CA Eindhoven
Netherlands

Karspeldreef 8
1101 CJ Amsterdam
Netherlands

T +31 (0)40 23 77 990
E sales@secura.com
W www.secura.com

Follow us on