Scoping the Compliance Task for GDPR : 12 Areas of Activity

At the outset, the General Data Protection Regulation (GDPR) may look like an imposing and costly exercise, but the value for business and economies has the potential to be enormous for those that get it right. Companies today collect vast amounts of data. The GDPR compliance effort can be used to create opportunity by cleaning house, honing processes to collect the right information at the right time, and developing a stronger bond with the customers, partners, suppliers and employees we collect it from. Simply put, it is an opportunity to take stock and make improvements.

Companies must begin by developing an understanding of what really matters to their business or organization. Any company that currently holds and works with personal data of EU citizens today should be instructing every department to ask some basic questions around how and why they collect and use this personal data and its value for a given function or product line, before they consider what is needed to ensure they can continue to work with it. Such an approach will inherently allow the development of a business case for the changes ahead and motivate the support required to devote the resource and budgets to enable the change.

The following 12 areas of activity and related tasks are described to offer a guide for scoping the task ahead and communicating requirements for all stakeholders. To benchmark progress, members are encouraged to consider whether their organizations have plans in place and, if so, where they are in their stage of implementation: scoping/engagement; audit/review; or documentation/change.

1. Stakeholder Support: Board & Business units

Tasks:

- Identify seasoned professionals either from within the organization or externally (from your industry).
- Senior stakeholders who can support the GDPR implementation need to be identified in each business unit/operation.

- Senior management must understand and champion GDPR requirements and the impact of non-compliance
- Adequate resources such as budget and workforce need to be allocated
- Responsibility for GDPR is required to be with the C-suite and executive management
- Look for opportunity to create value with the exercise, review of processes; structuring of data, etc

Workshop Tip: Involve the people on the floor who are managing all the devices and ensure that your requests are specific for GDPR compliance.

2. Inventory of the personal Information you hold

Tasks

- You may need to organize an information audit (a dataflow and a data inventory analysis), across the organization, or within particular business areas.
- The analysis should be matched with the consent given by the data subjects (put in a consent register) to verify, that consent is valid for the collection and operations (see action 7).

3. Privacy Notice & Information

Tasks

- You should understand what must be communicated
- Review your current privacy notices and put a plan in place for making any necessary changes

4. Individuals' rights

Tasks

- Check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.
- Further national and international legislation may affect the rights of the data subject. For instance, accounting laws, logging

directives etc. may require the data to be stored beyond the requirements of the GDPR.

Workshop Tip: manually review exceptions in GDPR to make it workable and solve small issues. There will be gaps which will have to be explained to the Data Protection Authority (DPA).

5. Data subjects' access requests

Tasks

- Update procedures, plan and document how requests will be handled within the new timescales and provide any additional information.

Workshop Tip: Security departments should delegate responsibility to operations and other parts of the organization.

6. Data Protection Impact Assessments (DPIA)

Tasks

- Work out how to implement DPIA in your organization. DPIAs can link to other organizational processes such as risk management and project management.
- Start to assess the situations where it will be necessary to conduct a DPIA.

  •Who will do it?

  •Who else needs to be involved?

  •Will the process be run centrally or locally?

7. Consent

Tasks

- You will need to review how your organizations is seeking, obtaining and recording consent and whether changes are needed.

Workshop Tip: Also consider ways to collect data without the need for consent

8. Children

Tasks

- You should start thinking now about putting systems in place to verify individuals' ages and to gather parental or guardian consent for the data processing activity.

9. Personal Data breaches

Tasks

- You should make sure you have the right procedures in place to detect, report and investigate a personal data breach

Tip: tweak business continuity and security incident response plans that are currently in place.

10. Security of data processing & Data protection by design

Tasks

- Assure the right procedures and tools in place to comply with both security and privacy by design requirements.

Tip: companies following ISO 27001 compliance will have met much of the criteria

11. Data Protection Governance

Tasks

- Designate a Data Protection Officer, if required, or someone to take responsibility for data protection compliance and assess where this role will sit within your organization's structure and governance arrangements.

12. International Data transfers

Tasks

- If your organization operates internationally, you should determine which data protection supervisory authority you come under.
- Put simply, the lead authority is determined according to where your organization has its main administration or where decisions about data processing are made.
- In a traditional headquarters (branches model), this is easy to determine. It is more difficult for complex, multi-site companies where decisions about different processing activities are taken in different places.