REMAIN COMPLIANT WITH THE NEW DATA PROTECTION ACT

With the EU's new General Data Protection Regulation came a large number of preparatory activities focused on becoming compliant. Now that the regulation and the new Danish data protection act have entered into force, the focus has shifted from becoming to remaining compliant.

In recent years, *IT in Practice* has provided insight into which activities enterprises need to undertake to comply with the data protection regulation. The regulation was introduced on 25 May 2018, and many enterprises are still working to finalise the remaining activities needed to achieve compliance.

The transition has been preoccupying both public- and private-sector enterprises, and the focus is slowly shifting towards what they need to do to maintain compliance in future. But what does remaining compliant mean for an enterprise?

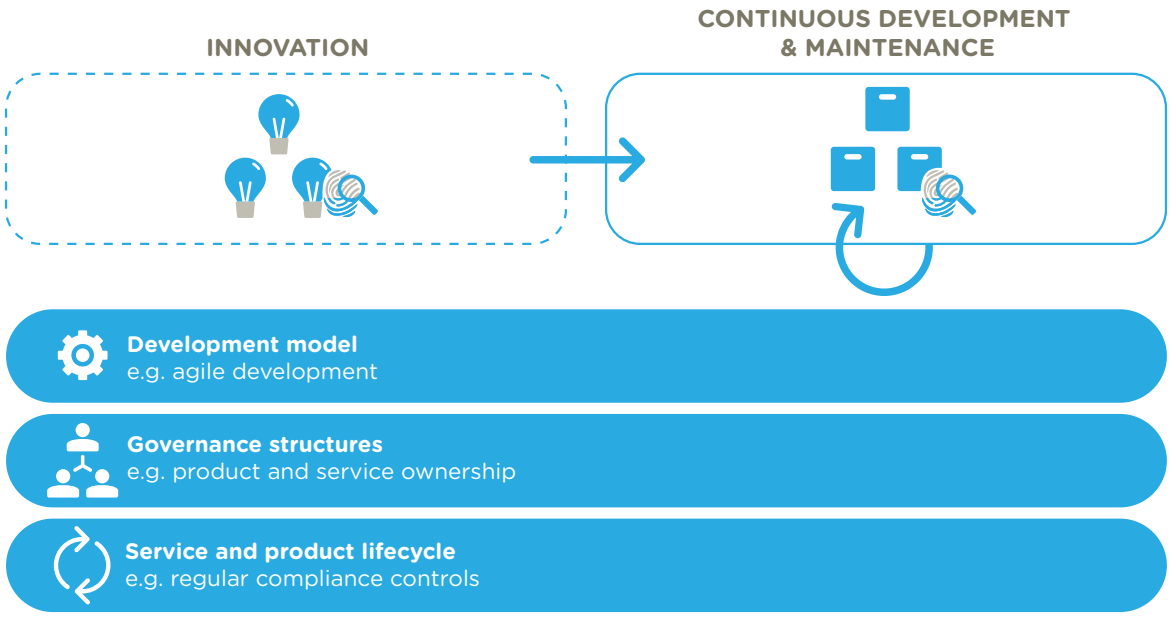
The purpose of the EU's data protection regulation is to protect data subjects and ensure they have the necessary control over their personal data.
Any personal data processing must comply with the following data protection principles:

- Lawfulness, fairness and transparency
- Purpose limitations
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

Principles have also been introduced for privacy by design and privacy by default. These principles establish some clear design requirements for future services and products that process personal data. Enterprises that develop new services and products which process personal data and further develop existing ones must adjust such service and product development in accordance with the data protection principles, etc. This adjustment applies to all development activities, governance structures and service and product lifecycle management for internal as well as external services and products. In some cases internal services, such as HR, process a range of personal data about employees.

IMPACT OF THE DATA PROTECTION ACT ON DEVELOPMENT ACTIVITIES

The data protection act affects the development of new services and products as well as existing ones, regardless of whether they are internal tools or external customer solutions.



Development model

Regardless of whether a company has used a development model that is to some degree agile, the model's phases and the decision points they contain should reflect the new data protection principles.
In the design phase, attention should be focused on the extent to which the idea concerned necessitates personal data processing and, if so, which types of personal data processing are justified by the purpose.

In the development of the service or product itself, steps must be taken to ensure it meets the level of security and functionality necessary to comply with the data protection principles and the data subjects' rights.

This entails implementing not only technical measures (eg, data minimisation through the limited collection of personal data) but also taking organisational steps (eg, procedures, and guidelines).

Governance structure

After a new service or product has been launched, it is important to establish the correct governance structure. This entails using means like procedures and guidelines to create the necessary service or product ownership, data processor and subprocessor management as well as organisation through procedures and guidelines, for example.

The governance structure must also ensure that the service and product owner keeps the enterprise's records of processing activities up to date as regards new services or products and their further development.

Thus, the enterprise ensures that the conditions required for the future compliance of the service or product are in place.

Service and product life cycle

One of the legal bases most frequently used for the processing of personal data is consent. The ongoing management of every consent given is therefore a must for all services and products that process personal data. In addition, personal data may only be processed for as long as required by the purpose. Erasure routines must be run continuously to meet this requirement throughout the life cycle of the service and product.

Ramboll recommends that enterprises review their existing development model and embed the necessary compliance elements within it in order to remain compliant with the data protection act.

Furthermore, Ramboll recommends that enterprises adjust their existing governance structure for service and product ownership or establish a new one. Ramboll also recommends that companies implement such measures as consent management and erasure routines in their service and product life cycles.

ACTION ITEMS

- **Review development model and embed activities aimed at compliance with the data protection act**
- **Adjust existing or establish a new governance structure for services and products to anchor responsibility for compliance**
- **Implement consent management and erasure routines in the service and product cycle to ensure continuous management in this respect**