DATA PRIVACY BY DESIGN – KEY CONSIDERATIONS FOR PRODUCT DEVELOPMENT

The concept of "Privacy by Design" has been a part of the data protection landscape since it was first developed in the early 1990's and has always been considered the best practice approach to product development. Article 25 of the GDPR will formally oblige companies to consider the risks to an individual's personal data at the product development stage, and to take appropriate measures to safeguard such personal data.

Privacy by Design has been identified by the government as a key element of their "Security by Design" strategy, which has been developed to address the cyber security threats which will arise with an increase in sales of connected devices and the so called "Internet of Things".

Who is affected by "Privacy by Design"?

The GDPR obligation to give due consideration to the protection of personal data in the development of products will apply widely. Put simply, if the product or service processes any personal data as part of the usage of the product or in the delivery of a related service, then the designer, developer, and/or manufacturer etc. will be expected to consider the risks to personal data.

"Privacy by Design" in practice

Data Protection Impact Assessments (DPIAs) will be the key to implementing "Privacy by Design" in practice. A DPIA is a "systematic and extensive evaluation" of the personal data implications which are likely to arise in connection with a particular product.

Upon completion of a DPIA, the product developer should have a clear understanding of all personal data that is necessary for the functioning of the product or the delivery of the services, as well as the potential risks to the personal information. Steps can then be taken to mitigate the identified risks.

All stages of a DPIA should be documented and retained as a record of the fact that data protection has been considered and integrated into a product. This can be useful evidence in the event that a product is investigated for breaches of data protection law in the future.

Risk mitigation

Upon completion of a DPIA, the developer should have a clear understanding of the risks which will arise as a result of the personal data. The onus is now on the developer to take steps to eliminate or reduce the risks identified. Whilst each case will be different, the approach to risk reduction will be to ensure that the product's functioning is aligned to the data processing principles (contained within Article 5 of the GDPR); some specific examples of which are:

- ensuring an adequate level of technical and organisational measures are in place to protect the data, which means in practice that robust cyber security protection is built into all aspects of the product
- ensuring that the product only collects such information as is necessary for undertaking the functions or providing the services
- where possible, store the data in a format that prevents an individual from being identified, such as through the use of pseudonymisation
- seek to be transparent with the end user of the product but informing them explicitly and in plain language how their personal data will be used if they choose to engage with the product.

Who to contact

MATTHEW GILHOOLY
Associate

+44 (0)131 222 9858
07712 507 886