Browne Jacobson

Top tips for implementing ‘Data Protection by Design & Default’

The GDPR requires all businesses to implement ‘Data Protection by Design & Default’ but what does that mean in practice and how can businesses practically comply?

27 April 2020

The GDPR requires all businesses to implement ‘Data Protection by Design & Default’ but what does that mean in practice and how can businesses practically comply?

The concept of ‘data protection by design’ is not a new one – in the UK the ICO has always advocated an approach that businesses should, as a matter of good-practice, consider data protection implications and implement appropriate protective measures throughout the implementation and lifecycle of business or processing activities.

Under the GDPR, this approach has now been enshrined in law.

Article 25 of the GDPR requires every business to take account of data protection and privacy at all stages in the implementation of new processing activities. Businesses must then ensure that they build appropriate technical and organisational measures to implement the data protection principles and safeguard individual’s rights into that process.

It can however be difficult for many businesses to ensure that this happens in practice. New projects and processes will often by led by teams who won’t have data protection and privacy at the forefront of their minds. Often a data protection question will be asked when a project is already at an advanced stage, technical solutions already agreed on and copy already drafted.

As well as breaching Article 25 obligations, that approach can also cause other challenges for businesses. Compliance can often require technical solutions to be put in place – either to obtain appropriate consents, to give fair processing notices or to change the types of data that are collected. Considering data protection and privacy at a late stage can therefore lead to a requirement for costly changes and delays to project implementation.

How does your organisation therefore ensure that ‘data protection by design’ is implemented across your business? Here are our top tips for businesses to meet these obligations:

1. **Appoint a person responsible for data protection**

   Even where you are not subject to an obligation to appoint a statutory Data Protection Officer, you should allocate a person within your organisation who is responsible for data protection and privacy compliance.

   Visibility is important for that individual – people responsible for implementing new projects and technologies must know where they can go to get further support on data protection issues.

   That person must also have enough capacity, knowledge and authority to take on that role and to ensure that changes are implemented where required.

2. **Training**

New ideas and processes that involve the processing of personal data can come from any part of your business.

Every person in your business must therefore understand what personal data is, what amounts to ‘processing personal data’ and where to go for further support.

It is therefore important to ensure that those individuals are sufficiently trained to recognise where data protection and privacy may impact on their proposed new business activity.

3. **Have a clear procedure in place**

   One of the first questions that you should ask when implementing any new processes or activities is ‘is personal data being processed?’

   If it is, that should trigger a process where further advice is sought about the data protection and privacy implications of that proposed process and how to address any risks.

   You should document a clear policy which sets out the initial questions that should be asked and the next steps to consider the risks.

4. **Ensure that risks are addressed**

   Once it is identified that a proposed process or activity involves the processing of personal data, any risks of non-compliance or to the rights of data subjects should be identified.

   Steps should then be taken to address those risks.

   Those steps could range from changing the personal data that is processed so that it is only that information which is necessary for the particular purpose, implementing technical measures to give notices or obtain consent (as required) or putting in place access controls or techniques such as pseudonymisation or encryption, to keep personal data secure.

5. **Make a distinction between ‘data protection by design’ and ‘data protection impact assessments’ (DPIAs).**

   Where it is determined that a processing activity is likely to result in a high risk to data subjects, a DPIA may also be required.

   ‘Data protection by design’ applies to all processing activities implemented across your organisation whereas a DPIA will only be required in limited circumstances.

   Internal policies should make a clear distinction between the two, ensuring that full DPIAs, which may require a more in-depth assessment of the risks and mitigations, are undertaken where required.

6. **Are there any third parties involved?**

   Often, when implementing a new technology designed by a third-party, that third-party will provide a copy of their DPIA as ‘proof’ they are compliant. Although it is certainly helpful and can act as a flag to consider data protection and privacy issues, organisations should ensure that they don’t rely on it. That DPIA has been undertaken from the perspective of that third-party, tailored to its proposed processing activities and considered the risks for that third party only.

   The considerations for your organisation may be different and you will have your own obligations to comply. You should therefore ensure that ‘data protection by design’ is implemented from your organisation’s perspective in relation to both the processing activity itself and the relationship with that third party.

This article was first published by Data Protection Magazine.

Contact

Henrietta Scott

Head of Marketing

PRTeam@brownejacobson.com

+44 (0)330 045 2299

Related expertise

Services

Cyber liability and data security insurance

Data protection and higher education

Data protection and privacy

Data protection for retail

Data protection guidance for schools and trusts

Digital and data