

## **GDPR & DATA PROTECTION ACT 2018 – ADDITIONAL CHECKLIST (8)**

### **DATA PROTECTION BY DESIGN AND DEFAULT**

#### **CONTEXT**

- The GDPR/DPA requires you to put in place appropriate technical and organisational measures to implement the data protection principles and safeguard individual rights. This is ‘data protection by design and by default’.
- In essence, this means you have to integrate or ‘bake in’ data protection into your processing activities and business practices, from the design stage right through the lifecycle.
- This concept is not new. Previously known as ‘privacy by design’, it has always been part of data protection law. The key change with the GDPR/DPA is that it is now a legal requirement.
- Data protection by design is about considering data protection and privacy issues upfront in everything you do. It can help you ensure that you comply with the DPA/GDPR’s fundamental principles and requirements, and forms part of the focus on accountability.

#### **CHECKLIST**

- We consider data protection issues as part of the design and implementation of systems, services, products and business practices.
- We make data protection an essential component of the core functionality of our processing systems and services.
- We anticipate risks and privacy-invasive events before they occur, and take steps to prevent harm to individuals.
- We only process the personal data that we need for our purposes(s), and that we only use the data for those purposes.
- We ensure that personal data is automatically protected in any IT system, service, product, and/or business practice, so that individuals should not have to take any specific action to protect their privacy.
- We provide the identity and contact information of those responsible for data protection both within our organisation and to individuals.
- We adopt a ‘plain language’ policy for any public documents so that individuals easily understand what we are doing with their personal data.
- We provide individuals with tools so they can determine how we are using their personal data, and whether our policies are being properly enforced.
- We offer strong privacy defaults, user-friendly options and controls, and respect user preferences.
- We only use data processors that provide sufficient guarantees of their technical and organisational measures for data protection by design.
- When we use other systems, services or products in our processing activities, we make sure that we only use those whose designers and manufacturers take data protection issues into account.
- We use privacy-enhancing technologies (PETs) to assist us in complying with our data protection by design obligations.