Companies who operate in, or are contemplating entry into, the Internet of Things (“IoT”) field should be aware of upcoming changes to the EU data protection regime, which will apply from May 2018 and may have a significant impact on their business model and the design of their products, processes and devices.

The endless potential commercial and technological applications of the IoT have been the subject of much comment in recent times. This potential, in conjunction with the extensive use made of data by IoT-based technology, has given rise to concerns that the expansion of the IoT could pose significant data protection and personal privacy risks and challenges. The data protection issues arising from the IoT were considered in an opinion of the Article 29 Data Protection Working Party issued in 2014.

The General Data Protection Regulation (“GDPR”) came into force on 24 May 2016 and will apply from 25 May 2018. The GDPR will introduce developments to a number of areas of EU data protection law that are likely to have a direct impact on the way device manufacturers, application developers, social platforms and other entities involved in the IoT field design, devise and bring to market IoT-based devices, systems and applications.

The following are 5 key changes of particular relevance to the IoT:

1. **Security breaches**

One of the principal privacy concerns that have been expressed in relation to IoT devices is that they provide soft targets for hackers and are susceptible to security breaches. The GDPR will introduce a general mandatory notification regime in the event of personal data breaches. Data controllers will be required to report personal data breaches to their supervisory authority no later than 72 hours after becoming aware of such breach and, in some cases, will also be required to report such breaches to affected individuals. Data controllers using the IoT will need to ensure that they are in a position to identify and react to security breaches in a manner which complies with the requirements of the GDPR.
2. Consent

Doubt has been expressed about the ability of IOT devices, even under the existing EU data protection regime, to obtain consent of sufficient quality from users of such devices in relation to data processing activities. The GDPR will tighten the existing requirements in relation to data subject consent, requiring data controllers to demonstrate consent has been given by way of a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject’s agreement to the processing of his or her personal data. The GDPR provides that consent cannot be presumed through the inaction of the data subject and that consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.

3. Privacy by design and privacy by default

Privacy by design and privacy by default are concepts which exist in current data protection legislation, but the GDPR will put these concepts on a firm legislative footing. It will impose obligations on data controllers to adopt significant new technical and organisational measures to demonstrate their compliance with the requirements of the GDPR. These may include conducting data protection impact assessments in certain circumstances which are likely to arise in connection with IOT systems.

4. Enhanced data subject rights

The GDPR will confer new substantive rights on data subjects in relation to their personal data. These substantive rights include an express right to be forgotten, data portability rights and the right to object to automated decision making. Thought will need to be given in the design of IOT devices, applications and systems as to whether the necessary capabilities have been built-in to facilitate the exercise of these data subject rights in compliance with the GDPR, particularly in relation to data portability.

5. Processing Personal Data relating to children

The GDPR will make it impossible for children under the age of 13 to consent on their own behalf to the processing of their personal data in relation to online services. For children between the ages of 13 and 15 (inclusive), the position will depend on legislation in each Member State (although the default position will be that children between those ages will not be able to give consent on their own behalf). These provisions pose challenges for those intending to bring to market IOT devices that may be used by children, both in relation to the feasibility of introducing parental/guardian consent mechanisms to the devices and in relation to the ability to market such devices at an EU-wide level, given that the law relating to children between 13 and 15 may not be uniform across all Member States.

Separately, it is also worth noting a more immediate development in the IOT field: the “GPEN Sweep” study on IOT, which is being coordinated by the Global Privacy Enforcement Network. The Irish Data Protection Commissioner has announced that it, along with 28 other data protection authorities around the world, will participate in the GPEN Sweep, which will examine how IOT devices use personal data and communicate such use to customers. The results of the GPEN Sweep are expected to be published in September.
This document is for general guidance only and should not be regarded as a substitute for professional advice. Such advice should always be taken before acting on any of the matters discussed.