Data Protection regulations - is your FM system compliant?

Following a number of high profile data breaches in the press in recent years, organisations are under increasing pressure to provide the required evidence and assurance of compliance to current Data Protection guidelines.

The Data Protection Act 1998 controls how an individual's personal information can be used by organisations, businesses or the government. Organisations that hold responsibility for using data are required to follow strict rules called 'data protection principles'.

They must make sure information being kept is accurate, kept safe and secure and used:

- fairly and lawfully for limited, specifically stated purposes
- in a way that is adequate, relevant and not excessive

Also;
- not kept for no longer than absolutely necessary
- handled according to people's data protection rights
- not transferred outside the European Economic Area without adequate protection

More sensitive information including: ethnic background, political opinions, religious beliefs, health, sexual health and criminal records has even more stringent legal protection.

What is personal data?
Personal data is defined as data that relates to a living individual who can be identified:
- from those data, or
- from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller

It also includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Organisations, public or private, that collect and use personally identifiable information have an obligation to handle this data according to data protection laws. This law is based on a number of basic principles:

- there should be limits on the collection of personal information, and it should be obtained by lawful and fair means, with the knowledge or consent of the individual
- the information should be correct
- personal information should be relevant to the purposes for which it is used, should be accurate, complete and up to date
- there must be no secret purposes, the purposes for which the information is to be used should be specified at least at the time of collection and should only be used for those agreed purposes
- there must be no `creeping purposes', personal information can only be disclosed, used, or retained for only the original purposes, except with the consent of the individual or under law, and accordingly it must be deleted when no longer necessary for that purpose
- the information must be secure, reasonable security safeguards are used to protect personal information from loss, unauthorised access, destruction, use, modification or disclosure;
- no secret organisations, sources, or processing, individuals must be made aware of the collection and use of their information. the purpose for its use, and we must know which organisation is the data controller
- individuals have rights to be involved and should be able to have access to their information, and the right to challenge the information held and to seek its deletion, rectification, completion or modification

Cont…/

- organisations must be held to account and the organisation that collects and manages personal information must be accountable for providing the above principles and rights

Data protection rules need to be enforced by a regulator or authority, often referred to as a Privacy Commissioner. The strength of the powers invested in these authorities varies from country to country and so does its independence from Government. These powers, for example, can include the ability to conduct investigations, act on complaints and impose fines when they discover an organisation has broken the law.

Modern technology can play a strong role in ensuring data protection rules are followed. Todays software systems are developed using the latest technological tools and using careful design, it is possible to limit data breaches.

Asckey work to stringent Data Protection Guidelines including ISO 27001 and ISO 9001. Data protection guidelines are implemented at every stage including pre-sales, implementation, installation and maintenance.

Our N3 Hosting network provides NHS Trusts with additional assurance of data protection within the boundaries of their own private data cloud. Asckey's access to the N3 cloud is dependent on our adherence to the latest IGSoC guidelines.

IGSoC

The Information Governance Statement of Compliance (IGSoC), is the process by which organisations enter into an agreement with NHS Digital to access the NHS National Network (N3) and resultant services, including terms and conditions of use.

The steps in the IGSoC process set out a range of security related requirements, which must be satisfied in order for an organisation to be able to provide assurances in respect of safeguarding the N3 network and information assets that may be accessed.

Asckey are fully IGSoC compliant with current IGSoC accreditation at level 2. To maintain this accreditation, all Asckey staff are required to complete an annual assessment via the IG Toolkit. The Information Governance or IG Toolkit is an online system which allows organisations to assess themselves or be assessed against Information Governance policies and standards.

Any external agency wishing to connect to the NHS via Asckey's N3 network are also required to be IGSoC compliant. This, combined with our recent ISO 27001 accreditation means that security is at the forefront of all that we do.

Ensure your key data is in safe hands by selecting software that has the right level of protection for your organisation.

Changes under the New EU General Data Protection Regulation (GDPR) 2018 are going to affect everyone – "get ready or pay the price". Asckey are following developments closely, call us for further information.

Contact Asckey to find out how our fmfirst® estates and facilities management software is developed using the very latest technological advances and to the highest data security standards.

Sources:

http://www.legislation.gov.uk/ukpga/1998/29/contents
https://ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles/
http://www.allenovery.com/SiteCollectionDocuments/Radical%20changes%20to%20European%20data%20protection%20legislation.pdf
https://www.privacyinternational.org/node/44
https://www.digital.nhs.uk/article/1107/Connections-to-core-NHS-services#IGSoC