Preparing for the New EU General Data Protection Regulation

Key Changes for Hospitals, Healthcare Organisations (HCOs) and Healthcare Practitioners (HCPs)

The GDPR will come into force on 25 May 2018. All HCOs and HCPs as data controllers and processors must comply with the new law by this date. This note sets out some of the main changes and obligations however this is not exhaustive and there are many other implications for organisations as data controllers or processors, A&L Goodbody can provide detailed and specific advice on request.

1. Definition of Personal & Sensitive Data

The GDPR broadens the definition of personal data and sensitive data:

- Personal data now expressly includes an identification number, location data, and online identifier.
- Sensitive personal data includes genetic data and biometric data. 'Genetic data' includes biological samples from an individual, such as chromosomal or DNA. 'Biometric data' includes fingerprints and facial recognition.
- The GDPR introduces a new concept of 'pseudonymisation', which is the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information. Such additional information must be kept separately and subject to technical (e.g. encryption) and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.
- Anonymised data (data which does not relate to an identified or identifiable natural person or to personal data rendered anonymous) falls outside the scope of the GDPR.

2. Lawful Processing Conditions, including Consent

- Consent requires some form of clear affirmative action. Silence or pre-ticked boxes will no longer be sufficient to constitute consent.
- The GDPR permits data subjects to withdraw their consent at any time.
- A record must be kept of how and when consent was given.
- Prior to giving consent, data subjects must be informed of certain rights.
- Parental consent is necessary to the processing of a child's data, where the child is below the age of 16 years old. Ireland may choose to lower this age but not below 13 years old.

The legal basis for processing sensitive data remains substantially the same, with some additional grounds[1]:

(a) the data subject has given explicit consent to the processing of personal data for one or more specified purposes; or

(b) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent; or

(c) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of law or pursuant to contract with a health professional and data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy; or

(d) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, with measures in place to safeguard the rights and freedoms of the data subject, in particular professional secrecy.

3. Subject Access Requests

- The GDPR requires the provision of specific, additional, information to data subjects when responding to access requests.
- The time period for dealing with requests has been reduced from 40 days to one month.
- The ability to charge a fee has also been removed. However, the controller may charge a reasonable fee for any further copies requested by the data subject, or where access requests are manifestly unfounded or excessive, taking into account the administrative costs of providing the information.
- It is open to the Irish Government to enact legalisation which restricts access by a data subject where necessary, for the protection of the data subject. Therefore it is likely that a similar statutory instrument (to S.I. No. 82 of 1989) will be enacted, which sets out an obligation for HCOs and HCPs to carry out a 'harm test' prior to releasing and if necessary refusing access to the medical records, where such would be likely to cause harm to the physical or mental health of a data subject.

4. Right to Erasure

Data subjects have the right to erasure, also known as 'the right to be forgotten'.

A request for erasure of personal data can be refused on a number of grounds including where processing is necessary for public health reasons, for the defence of legal proceedings, or for compliance with a legal obligation.

5. Data Breach Reporting & Security

HCOs and HCPs who are data controllers will have a mandatory obligation to report data breaches to the Office of the Data Practitioner Commissioner[2] within 72 hours, unless the breach is unlikely to result in a risk to the rights of data subjects.

Controllers will also have to notify data subjects where the breach is likely to result in a 'high risk' to them.

A 'personal data breach' is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

6. Fines

HCOs and HCPs could be subject to significant fines as data controllers or processors for non-compliance. They could be subject to fines of up to €20 million or 4% of the total worldwide annual turnover of the preceding financial year.

Fines can be imposed in addition to, or instead of, any corrective measures (such as warnings or reprimands).

7. Right to Compensation & Liability

Data subjects can sue both controllers and processors for compensation for pecuniary or non-pecuniary damage (e.g. damages for distress) suffered as a result of a breach of the GDPR.

Data subjects will have a right to recover material or non-material damages including loss of control over personal data or limitation of rights, discrimination, financial loss, damage to reputation, loss of confidentiality of personal data protected by professional secrecy and "other significant economic or social disadvantage."

Data subjects can choose to sue both the controller and the processor, with the introduction of joint and several liability between parties engaged in the same data processing.

Recommended Actions

1. All HCOs and HCPs acting as data controllers and processors established in the EU should now review their policies and procedures and update them to comply with the GDPR, in advance of the effective date.
2. Review all personal data that you currently hold and determine whether or not it is held in accordance with the GDPR. Identify and document the legal basis for processing personal data (consent, legitimate interest or a legal enactment).
3. HCOs and HCPs should now familiarise themselves with their obligations under the GDPR and take steps to ensure compliance, thereby minimising the risk of incurring fines or being sued for damages by a data subject. Ensure staff are effectively trained in the new policies and procedures.
4. Ensure that data subjects are informed of their rights under the GDPR. Certain information must be provided by HCOs and HCPs to data subjects including the legal basis for processing personal data (set out in a privacy notice and in responding to access requests), the right to withdraw consent to processing, data retention periods and the right to have inaccurate data corrected.
5. Update policies and procedures for processing data access requests. Such requests must be dealt with within one month and consider logistically whether additional resources should be designated to meet this obligation.
6. Review and update procedures for obtaining consent. Data controllers must be able to demonstrate that consent was given. Consent cannot be inferred from silence, pre-ticked boxes or inactivity.
7. Review and update procedures for processing children's data.
8. Review security measures to ensure they are robust enough to meet the requirements of the GDPR.
9. Review and revise your data breach response plan to ensure you can manage, contain and respond to breaches quickly, and notify the relevant supervisory authority within 72 hours. Set out the key personnel responsible for dealing with the breach and informing the supervisory authority. Data processing agreements should be reviewed to ensure they include a requirement for the processor to immediately inform the controller of any data breaches.
10. Consider whether you must appoint a data protection officer. Data protection officers will be required in certain organisations including public authorities, or where regular and systematic monitoring of data subjects on a large scale occurs, or those processing sensitive personal data on a large scale.
11. Review and if necessary renegotiate agreements which involve the processing of personal data. Liability provisions and responsibilities of respective parties will need to be clearly set out in light of the altered risk profiles of controllers and processors under the GDPR.

[1]The Irish Government may introduce further limitations with regard to the processing of genetic data, biometric data or health data.

[2]HCPs and HCOs may be obliged to notify another supervisory authority in other circumstances e.g. where its main establishment is not in Ireland.

KEY CONTACTS

Cliona Christle
Partner
+353 1 649 2442
cchristle@algoodbody.com

Róise Nic Ghráinne
Associate
+353 1 649 2350
rnicghrainne@algoodbody.com