MASON HAYES & CURRAN

Genera Data Protection Regulation for the Healthcare Sector

Tuesday 13 June 2017

@mhclawyers

MASON HAYES & CURRAN

Welcome

Niamh Callaghan
Partner
Mason Hayes & Curran

MASON HAYES & CURRAN

GDPR for the Healthcare sector

Robert McDonagh
Partner
Mason Hayes & Curran

MASON HAYES & CURRAN

Data protection reform

- GDPR
  - **applies from 25 May 2018**
  - **DPC expect move towards compliance now**
  - **implementing Bill published (with provision for SIs)**
  - **increase in health sector specific provisions**
- ePrivacy Regulations remain applicable, but Directive is to be replaced by a new EU Regulation (25 May 2018)

MASON HAYES & CURRAN

Increased exposure

- Shift in burden of proof – must be able to demonstrate compliance
- Significant fines
  - **up to €20 million or 4% of annual worldwide turnover**
  - **must be effective and dissuasive as well as proportionate**
  - **likely to apply to public hospitals where competing**
- Data subject claims:
  - **explicit right to compensation for damage, both material and non-material (pecuniary loss?)**
  - **possible joint and several liability**
- Data mapping and GDPR gap analysis

MASON HAYES & CURRAN

Data protection principles

- Same basic concepts and principles but generally tighter controls and greater emphasis on data subject rights
- Privacy by design
  - **implement appropriate technical / organisational measures**
  - **e.g. pseudonymisation / data minimisation**
- Privacy by default - only process data necessary for specific purpose:
  - **amount of data**
  - **extent of processing**
  - **period of storage**
  - **accessibility**

MASON HAYES & CURRAN

Profiling / big data / scientific research

- Can still undertake profiling and big data analysis
- Can object to profiling based upon public interest test
- Can object to automated decision making if has legal effect or significantly affects individuals unless (with some exceptions):
  - **necessary for contract;**
  - **data subject has explicitly consented; or**
  - **is authorised by law**
- Absolute right to object to profiling for direct marketing
- Specific provisions facilitating scientific research but can object

MASON HAYES & CURRAN

Data protection assessments

- Must do a documented DPA if high risk processing, e.g.
  - systematic and extensive automated evaluation with legal effect / similarly significant affects DS
  - large scale processing of sensitive data
  - systematic monitoring of public areas
- Where appropriate, seek views of data subjects representatives
- Exclusion if based upon law that specifically regulates processing operations and DPA already carried out for that law

MASON HAYES & CURRAN

Consulting DPC

- Must consult DPC if:
  - **DPA shows high risks not mitigated**
  - **proposed legislative / regulatory measure relates to processing**
- State may also require consultation for public interest tasks, e.g. social protection and public health – depends on Bill

MASON HAYES & CURRAN

Security

- Similar test but should specifically consider:
  - **pseudonymisation**
  - **encryption**
  - **ability to ensure confidentiality, integrity, availability and resilience**
  - **ability to restore availability and access**
  - **a process for regular testing**

MASON HAYES & CURRAN

Security breach

- Notify DPC without undue delay and, where feasible, within 72 hours, unless unlikely to result in a risk
- Processor must notify controller without undue delay
- Must notify data subjects if likely to result in a high risk to privacy / rights (with some exceptions)
- Must document breaches
- Should have security breach response plan in place

MASON HAYES & CURRAN

Using data processors

- More extensive requirements for data processor contracts
- Data transfer rules broadly the same
  - **Safe Harbour invalid – replaced by Privacy Shield**
  - **model clauses and adequacy decisions still valid**
  - **ongoing legal challenges**
  - **transparency requirements in privacy policy**
- Need to audit supplier contracts and transfers

MASON HAYES & CURRAN

Joint data controllers

- Need specific agreement between joint controllers
- Must set out:
  - respective responsibilities and duties; and
  - respective roles and responsibilities vis-à-vis data subjects
- Must inform data subjects of:
  - essence of arrangement
  - how to exercise rights
- Can still exercise rights against either controller

MASON HAYES & CURRAN

Greater accountability

- Must be able to demonstrate compliance

Notable shift in burden of proof, particularly in light of increased fines and higher risk of data subject claims

MASON HAYES & CURRAN

Accountability measures

- Must implement appropriate technical and organisational measures to ensure and demonstrate compliance
- Where proportionate, this should include implementation of appropriate data protection policies

MASON HAYES & CURRAN

Documenting compliance

- DC / DP must document all processing activities, e.g.:
  - categories of data subjects, recipients and data
  - data transfers (including details of safeguards)
  - retention / erasure period
  - general description of security measures (if possible)
- DC also must document purposes and (indirectly) legal bases
- Should be consistent with privacy policy
- Need to undertaking a data mapping exercise

MASON HAYES & CURRAN

Key points

1. Core principles broadly the same, but tighter controls
2. Greater accountability and shift in burden of proof
3. Increased records and compliance burden
4. Increased financial exposure

1 year to get it right, but time to start preparing is now

MASON HAYES & CURRAN

What to do now – step 1 (what are we doing)?

1. Data mapping exercise
    - data flows and disclosures
    - purpose and legitimisation mapping
2. Audit of data transfers (remember Brexit)
3. Audit of data related contracts
4. GDPR gap analysis and prioritisation

MASON HAYES & CURRAN

What to do now – step 2 (moving forward)?

1. Use gap analysis to decide on key action points
2. Create internal accountability records
3. Update internal and external policies
4. Create any necessary new policies and templates, e.g.
    1. privacy by design / default playbook
    2. DPA protocol and templates
    3. security breach response plan
5. Update contracts

MASON HAYES & CURRAN

Thank you

Robert McDonagh
Partner
Mason Hayes & Curran
e: rmcdonagh@mhc.ie
t: +353 1 614 5077

MASON HAYES & CURRAN

GDPR for the Healthcare Sector

Catherine Allen
Partner
Mason Hayes & Curran

MASON HAYES & CURRAN

Special Categories of Personal Data

- Article 9 GDPR defines special categories of personal data
  - Definitions of health data, genetic data, biometric data
- Prohibition on processing special categories of personal data

MASON HAYES & CURRAN

Special Categories of Personal Data

- Exceptions to the prohibition relevant to the healthcare sector
  - Explicit consent (but…)
  - Vital interests
  - Substantial public interest
  - Medical diagnosis and treatment
  - Public health

MASON HAYES & CURRAN

Special Categories of Personal Data

- Consent is more tightly defined.
- Consent must be:
  - Freely given
  - Fully informed (i.e. a proper explanation)
  - Separate consents for separate purposes
- Consent can be refused
- Consent can be withdrawn at any time
- Burden of proof lies with data controller

MASON HAYES & CURRAN

What is the impact?

- Impact for the healthcare sector?
  - Existing consents may become invalid and new consents may therefore need to be obtained
  - May be preferable to base processing on grounds other than consent

MASON HAYES & CURRAN

Data protection officer

- Must appoint a DPO where processing sensitive personal data on a large scale (WP view – includes hospitals)
- Must be expert in data protection law and practices
- Can perform other tasks provided no conflict of interest
- Can be employee or outsourced
- Can be appointed to a group of undertakings

MASON HAYES & CURRAN

Data protection officer

- Must be properly involved in all issues which relate to protection of personal data
  - inform and advise on compliance
  - monitor compliance
  - advise re DPAs
  - act as contact point

MASON HAYES & CURRAN

Data protection officer

- Must report directly to highest management level
- Must be independent – no instructions regarding exercise of function
- Must provide DPO with sufficient resources
- Protected role – cannot be removed or penalised for performing tasks

MASON HAYES & CURRAN

What is the impact?

- Impact for healthcare sector?
  - Possibly an onerous new obligation
  - Need to understand the rules relating to the appointment and role of DPOs

MASON HAYES & CURRAN

Data subject rights

- Subject access requests – more information
- Generally no fees
- Right to charge or refuse request if “manifestly unfounded or excessive” or “repetitive”
- One month time frame but can be extended to maximum of two further months
- Likely that an SI similar to SI No. 82 of 1989 (access to health data) will be enacted

MASON HAYES & CURRAN

What is the impact?

- Impact for the healthcare sector?
  - Risk that many more subject access requests will be received
  - Need to ensure compliance with the detailed rules in Articles 12 and 15

MASON HAYES & CURRAN

Other Data subject rights

- Right of erasure (right to be forgotten)
  - Can be refused for public health reasons
- Right to object to and stop processing
- New data portability right (where rely on consent or contract)

MASON HAYES & CURRAN

What is the impact?

- Impact for the healthcare sector?
  - Staff need to be trained on the new rights
  - New internal policies and procedures to aid compliance
  - Can your data processing systems cope with the new rights (e.g. be able to isolate and permanently erase data?)

MASON HAYES & CURRAN

Privacy Notices

- Must have transparent, clear, concise and easily accessible privacy policy
- Intelligible language adapted to data subject
- More information must be provided, e.g.
  - contact details of DPO
  - how long you will keep data
  - legal basis you are relying upon to legitimise processing

MASON HAYES & CURRAN

What is the impact?

- Impact for the healthcare sector?
  - Privacy notices will need to be revamped to comply with the new requirements

MASON HAYES & CURRAN

Takeaways

1. Review grounds for processing
2. Appoint a DPO
3. Get staff and systems ready to deal with new data subject rights
4. Review privacy notices

1 year to get it right, but the time to start preparing is now

MASON HAYES & CURRAN

Thank you

Catherine Allen
Partner
Mason Hayes & Curran
e: callen@mhc.ie
t: +353 1 614 5254