Anthony Collins
solicitors

The General Data Protection Regulation

Overview and key steps for compliance

The Care Provider Alliance

Meena Lekhi / Lauro Fava
Data Protection and Information Law
Anthony Collins Solicitors LLP
December 2017

What will be covered?

1. **Background**
2. **What you need to know**
3. **Key changes - impact and actions for health and social care providers**
4. **Steps to take now**
5. **Questions and answers**

Where are we now?

- New EU data protection framework
- Regulation
- Harmonisation
- Replaces current law
- "Directly applicable" from May 2018
- Data Protection Bill
- Brexit

What you need to know

- Countdown is on…
- Not quite out with the 'old'
- Broad provisions much the same
    - Enhanced rights
    - More perspective obligations
    - Increased penalties
- Mindset and approach

Why compliance matters?

- Data is an 'information asset'
- Regulatory enforcement action
- Litigation for damage and distress
- Loss of public confidence, negative media coverage and reputational damage
- Good information governance reduces the risks of non-compliance and 'mishaps'
- Safe and effective systems, documented processes and procedures and well trained staff
- Data protection laws as well as professional standards and guidance for health and social care

Key changes: new accountability principle

❑ *Impact:*

- Need to know law is changing
- No longer need to register with ICO (new fee structure)
- Demonstrate compliance under 'accountability principle'
- Detailed records of processing activity (incl. legal grounds), DP policies and procedures and training

➢ *Actions:*

- Raise awareness
- Risk register, comms strategy, action plan & timeline
- Organise information audit / information asset register
- Review and update your information governance framework (including breach management)

Key changes: document legal grounds for processing

❑ *Impact:*

- Need to identify lawful basis before you process data (see, ICO: Lawful bases for processing)
- Must be documented (accountability and transparency)
- Some rights may be modified e.g. consent
- New health and social care ground (Art. 9(2)(h))

➢ *Actions:*

- Determine and document legal grounds
- Differentiate between grounds for non-sensitive and sensitive personal data (special categories of personal data)
- Consider alternative grounds where appropriate

Key changes: more detailed privacy notices

❑ *Impact:*

- New information to be included e.g. contact details of DPO, legal basis for processing, retention periods and data subjects rights (see ICO: Privacy notices under the EU General Data Protection Regulation)
- Must be concise, easily accessible, written in plain language

➢ *Actions:*

- Review and update existing privacy notices
- How will you include additional information?
- Layered approach or 'just in time'
- Variety of media e.g. face to face (document), writing, signage or electronically (same medium as collection)

Key changes: enhanced subject access rights

- *Impact:*

- Some new rights e.g. right to be forgotten (erasure) and right to have data transferred to another data controller in a commonly used electronic format (portability)

- *Actions:*

- Review and update your procedures
- Ensure staff trained on how to respond
- Consider data deletion and portability when procuring new systems
- Do current IT requirements need to be updated incl. third party contracts
- Think about one-organisational approach

Key changes: subject access regime

- *Impact:*
  - Respond without undue delay and within 1 month
  - Extend by further 2 months (complex or number of requests)
  - Free of charge
  - Scope to charge reasonable fee if manifestly unfounded or excessive or refuse (evidence)
  - Entitled to other supplementary information (similar to PNs)
- *Actions:*
  - Review and update your SAR procedures
  - Plan how you will deal with requests more quickly
  - Explore the use of GDPR compliant templates
  - Consider secure self-service portals (if appropriate)
  - Ensure staff are trained on how to respond

Key changes: stricter requirements for consent

- *Impact:*

- Must be freely given, specific, informed and unambiguous (see ICO: draft GDPR consent guidance)
- Clear affirmative action that signifies agreement
- Presented in an intelligible and easily accessible form
- Must be verifiable and capable of withdrawal
- Not appropriate where necessary for the performance of a contract (e.g. service user or employee)

- *Actions:*

- Identify where consent relied upon, why and how it is obtained
- Ensure it is prominent, unbundled and granular
- Be prepared to alter consent mechanisms or consider alternative legal grounds
- Review systems/processes for recording consent (audit trail)

Key changes: new Data Protection Role

❑ *Impact:*

- Most health and care organisations will need to have DPO i.e. core business requires large scale processing of sensitive personal data
- Professional qualities and expert knowledge in data protection
- Must be able to act autonomously
- Report to highest level of management
- DPO 'tasks' (see ICO: Data protection officers)

➢ *Actions:*

- Assess where role should sit in organisational structure
- Consider practical implications surrounding appointment (e.g. independence, budget, direct reports)
- Review job description of current DPO and consider if appropriate
- Explore options e.g. can be an employee or a contractor or a group of undertakings may appoint a single DPO (no conflict and accessible)

Key changes: data protection by design and default

❑ *Impact:*

- Data protection controls must be considered at outset of design phase (not an afterthought or ignored)
- Must conduct a data privacy impact assessment (DPIA) if high risk processing involved e.g. new social care system (see ICO: Privacy by design)
- May need to consult ICO in cases of unmitigated risk

➢ *Actions:*

- Introduce/update internal processes for DPIAs
- Ensure staff and IT aware of requirements (i.e. when and how to implement DPIA)
- All new systems and initiatives need to be built using data protection by design and default

Key changes: direct obligations for data processors

- *Impact:*

- Mandatory written contract (as at present)
- New statutory obligations to be included (many currently imposed by contract negotiation)
- Select processor based on sufficient guarantees as to GDPR compliance (onus on controller to undertake due diligence)

- *Actions:*

- Assess level of awareness in procurement arrangements
- Review existing contracts and consider GDPR clauses
- Update precedents
- Prioritise contract review (volume and sensitivity)

Key changes: mandatory data breach notification

- *Impact:*

- Notify data security breaches to ICO without delay and where feasible within 72 hours
- Specific information to be provided (in stages if necessary)
- Notify data subjects without undue delay where 'high risk'
- Data processor to notify controller without undue delay
- In line with reporting requirements under NHS Digital (formerly HSCIC) IG Toolkit for SIRI

- *Actions:*

- Review technical and organisational measures
- Ensure mechanisms in place to detect and investigate data breaches e.g. incident management procedure
- Staff must be aware of reporting requirements

Steps to take now

- Preparation
- GDPR 'gap' analysis
- ICO "12 Steps"
- Project plan & timeline
- Establish framework of accountability
- Review and update data protection measures
- Staff training
- Share the load!

Questions

E-briefings:

www.anthonycollins.com/news-and-events/briefings.aspx

Contacts:

meena.lekhi@anthonycollins.com

lauro.fava@anthonycollins.com

Anthony Collins solicitors

What we do

Data Protection Services: Anthony Collins Solicitors

- DPA training for staff and managers – including GDPR
- Advice on information sharing and disclosures
- Practical compliance
- Privacy notices and consents
- Standard contracts and terms
- Policy, process and internal documents/templates
- Audits and Privacy Impact Assessments
- Requests from data subjects
- Dealing with breaches
- Advice on direct marketing and the Privacy and Electronic Communications Regulations 2003
- Advice on CCTV, surveillance and monitoring

Data Protection Workshops

- ✓ full day Training
- ✓ At our premises or yours
- ✓ Half day sessions