Anthony Collins
solicitors

The new General Data Protection Regulation and implications for care managers

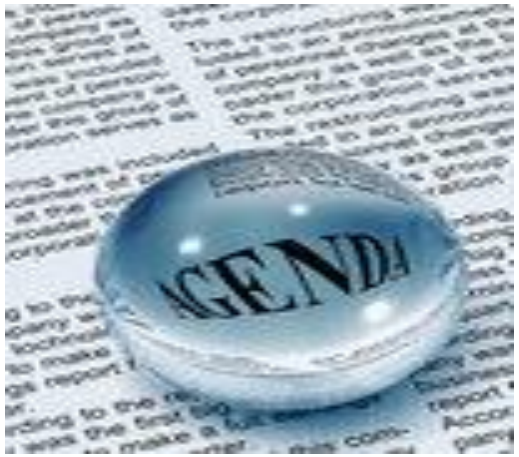
A workshop for the National Care Forum Managers' Conference

7th November 2017

Jane Burns
Head of Data Protection and Privacy Law
Anthony Collins Solicitors LLP

What will be covered?

1. **The existing law – starting points and existing risks**
2. **The new law – and key implications for providers of health and social care**
3. **What steps need to be taken now?**
4. **Questions and answers**



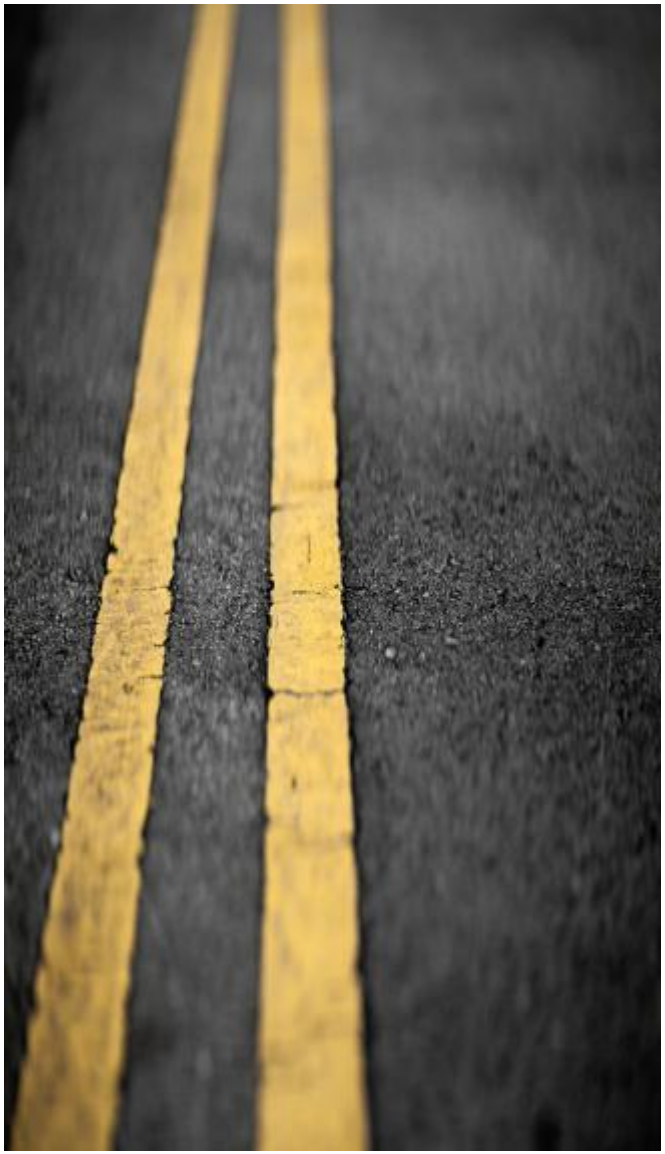
Why compliance matters

- **Regulator**: Office of Information Commissioner (ICO) publicises official enforcement action on its website: https://ico.org.uk/
- Since 6 April 2010: **penalty** up to £500,000
- **Media** reports, and **social media**: reputational damage
- Complaints and management **time**
- Enforcement: warnings, undertakings, enforcement notices, monetary penalty notices
- Powers of entry and investigation
- Offences of obtaining or disclosing data without controller's consent (s.55 of DPA) and under The Computer Misuse Act 1990: see those on ICO website

What is the GDPR?

New General Data Protection Regulation 2016

- Replaces UK's Data Protection Act 1998 (DPA) – aim is to harmonise DP law throughout Europe
- To come into force in UK on 25th May 2018
- Introduces significant changes to UK (and EU) Data Protection regime – including significantly higher fines



Sanctions and compensation – under the new law

Administrative fines

2 tiers – up to €20m/4% annual global turnover or up to €10m/2% annual GT – aggravating factors listed which can affect level of fine

Compensation for financial loss and/or distress

- available against data controllers and data processors under the new law

Personal data – new definition

'Personal data' means any information relating to an identified or identifiable natural person ('data subject'): an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Is Sensitive Personal Data being processed?

- Racial or ethnic origin
- Political opinions
- Religious belief or similar (philosophical belief*)
- Trade union membership
- Physical/mental health or condition
- Sexual life (or sexual orientation*)
- Commission or allegation of an offence*
- Proceedings for any offence, disposal of proceedings, sentence*
- Genetic data*
- Biometric data*

*Changes in GDPR

Key Definitions

Processing

This is very widely defined indeed and includes just about anything that could be done with personal data e.g. co sharing/disclosing, viewing, listening to, archiving, erasing/destroying.

Data Controller

A person (i.e. an individual or organisation) who decides the manner and purpose of how personal data is processed e.g. NCF member organisation in relation to the personal data of its data subjects (see next slide).

Data Processor

A person (as above) who processes on behalf of the Data Controller (DC) and under instruction from DC e.g. external individual or organisation which contracts with NCF member organisation to provide services – must act on controller's instructions to fall within the definition.

https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf

Key Definitions

Data Subject

A living individual who is the subject of personal data e.g. service users and their families, employees, trustees, volunteers, contractors etc.

Third Party

Any person other than data subject, data controller/staff of DC and data processor/staff of DP e.g. separate data controller – Police, safeguarding authorities.

Definitions and DPA Relationships

Data Subject:
e.g. service users, volunteers, employees, and anyone else whose PD processed

Data controller
(includes its staff)

NCF member organisation Responsibility/ Liability

Data processor
(includes its staff)
e.g. contractor

Contract

Legal ground for processing under DPA (e.g. consent)

Third Party

external organisation (e.g. Police, safeguarding officer) - might request disclosure

Trust and accountability

The 8 Data Protection Principles (paraphrased) – retained in GDPR

1. Personal Data must be processed fairly and lawfully (and in accordance with legal grounds set out in the DPA).

2. Personal Information must be used for limited purposes

3. Personal Data must be adequate, relevant and not excessive

4. Personal Data must be accurate and up to date

5. Personal Data must not be kept longer than is necessary

6. Personal information must be processed in line with data subjects' rights*

7. Personal Data must be secure

8. Personal Data must not be transferred to other countries without an adequate level of protection*

* These are dealt with by way of separate sections in the GDPR

GDPR: Accountability Principle - Obligations of Data Controllers

No longer need to register with ICO and new fee structure

but

Requirement to keep records of processing activities

Privacy Notices – **mandatory** under both DPA and GDPR **and:**

- Much more detailed and need to mention individuals' rights, including right to complain to ICO
- the rise to prominence of the 'legal grounds' for processing – review use of consent – see later.

Principle 1 of the DPA and equivalent under GDPR

Personal Data must be processed fairly and lawfully and in accordance with legal grounds (paraphrased)

i.e. requirement for:

- **Privacy/fair processing notice; and**

- **Legal 'ground(s)' for processing e.g.**
  - One for non-sensitive personal data e.g. consent? Legitimate interests? (not available to public authorities under GDPR); Necessary for a contract? Statutory gateway? Legal obligation?
  - Additional one required where data is sensitive personal data e.g. explicit consent? Or another 'ground' may be more appropriate– see later
  - Information Commissioner warns that consent is not a 'silver bullet' https://iconewsblog.org.uk/2017/08/16/consent-is-not-the-silver-bullet-for-gdpr-compliance/

Consent – new definition

> *'Consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.*

- **Not the appropriate ground where personal data necessary for performance of a contract e.g. with service user or employee**
- **Must be capable of withdrawal at any time without detriment – less likely to be relied upon to legitimise processing?**
- **Consent now much more granular**

- **Draft GDPR Consent guidance**

Example of alternatives to consent under GDPR

- ***'processing is necessary for the purposes of preventative 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 social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3:'***

- ***<u>Paragraph 3</u>: 'Personal data referred to [above] may be processed for the purposes referred to [above] when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.'***
- ***NB: privacy notice/statement still required***

Existing and new rights of the data subject

s.7 the right of subject access – changes in GDPR.

s.10 Right to object to processing causing or likely to cause substantial unwarranted damage or substantial unwarranted distress.

s.11 right to object to processing for direct marketing purpose; direct marketing not just limited to commercial purpose, can include promotional material of any organisation inc. charity.

s.12 right in relation to decisions made solely by automatic means – in certain circumstances; see GDPR - profiling

s.13 right for any person who has suffered damage or distress as a result of a breach of the DPA to seek compensation against the data controller.

s.14 right to rectification, blocking, erasure, destruction of personal data – new right to erasure under GDPR.

New right to data portability under GDPR

NOTE ALSO – s.42 assessment requests

New theme of increased transparency

- Data Minimisation, Privacy by Design and by Default
- Codes of Conduct, Certification Schemes and 'Privacy Seals'
- Data Protection Impact Assessments (PIAs rebranded) – mandatory for high risk processing
- Data Protection Officer – mandatory for high risk processing (see next slide)

The Statutory Data Protection Officer

DPO required where:

The processing is carried out by a public authority or body, except for courts acting in their judicial capacity

The core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purpose require regular and systematic monitoring of data subjects on a large scale or

The core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Art 9 and personal data relating to criminal convictions and offences referred to in Art 10.

The Data Protection Officer cont..

- Requires professional qualities and expert knowledge of data protection
- A group of undertakings may appoint a single DPO provided that he or she is easily accessible to each establishment.
- Must be able to act independently
- He or she shall not be dismissed or penalised by the DC or the processor for performing his tasks.
- To report to highest management level of the controller or the processor
- Can fulfil other tasks and duties but these must not conflict with DPO role

Appointment of Data Processors

High duty of care imposed on controllers in selecting service providers

Data Processors – direct obligations for first time

Mandatory requirement for contract in writing (as at present) – but:

- Greater information required
- Greater contractual obligations imposed on contractors

Data Security: Article 5.1(f)

"Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."*

- *Includes regular and ongoing staff training*

- *https://iconewsblog.org.uk/2017/03/29/garages-new-homes-and-old-offices-the-records-management-mistakes-that-put-health-records-at-risk/*

What else is to change?
Breach Notification

Data controller to report all breaches to ICO

- which are likely to result in risk to individuals - within 72 hours
- Specific information to be provided to ICO - in stages if necessary

Data subjects to be notified 'without undue delay' where breach would result in a high risk to them

Processor to notify controller 'without undue delay'

Read the NHS Digital (formerly HSCIC) checklist and guidance on reporting incidents

Data Protection: key documentation

1. The Data Protection Policy; and
2. The Privacy Notice/Privacy Statement/Fair Processing Notice/Data Protection Statement; and
3. The website Privacy Policy?
4. Should we have any other policies? Data/IT Security? Data Retention? Data Sharing?
5. When is a data sharing protocol needed?

What should organisations do in preparation?

- **Review personal data held -** conduct an audit if necessary and document retention periods.
- **Establish a framework for accountability –** policy documentation and record keeping, review capacity to comply with individuals exercising their rights, PIAs, privacy by design, Data Protection Officer?
- **Update Privacy Notices**
- **Breaches** – update policy and procedure
- **Review contracts with third party data processors**
- **STAFF TRAINING**

Sources of information/guidance?

A national GDPR working group is developing guidance on compliance for health and social care organisations:

https://digital.nhs.uk/information-governance-alliance/General-Data-Protection-Regulation-guidance.

ICO Health sector guidance:

https://ico.org.uk/for-organisations/health/

Questions

e-briefings:

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

Article: UKHCA Homecarer magazine May 2017

Advice:

Jane.Burns@anthonycollins.com
0121 212 7488

Anthony Collins solicitors

What we do

Data Protection Services from Anthony Collins Solicitors

- DPA training for staff and managers – including new GDPR
- Advice on Information sharing and disclosures
- How to comply
- Privacy notices and consents
- Standard contracts and terms
- Policy, process and internal governance advice
- Audit 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