The General Data Protection Regulation in health & social care

6 October 2016
Leeds
Session outline

09.05am: Roadmap of the GDPR
10.15am: Coffee break
10.30: GDPR impact: Streetview
  - Employment
  - Rights of data subjects
  - Integration & data sharing
11.15: Practicalities
11.25: Discussion on impact of the GDPR and next steps
GDPR Roadmap

Eleanor Tunnicliffe
Associate
etunnicliffe@dacbeachcroft.com
0113 251 4732
Themes of the GDPR

- Refining/tightening up existing concepts
- New concepts in regulation: accountability, demonstrating compliance, designing compliance
- Increased regulation/enforcement: by ICO and data subjects
- Enhanced rights for data subjects
- Expectations of uniformity and portability
What does Brexit mean for GDPR?

- GDPR comes into force automatically 25 May 2018 [cf October 2018 as earliest likely Brexit date]

- After Brexit:
  - GDPR will apply to UK firms processing EU PD or delivering goods & services in the EU
  - If outside EU, UK will need “adequate” data protection regime to receive EU PD

- Substantial differences in data protection regimes between UK & EU or within UK seem unlikely
Processing under GDPR

How will it compare to DPA framework?
Recap on DPA basics

Key concepts:

- National/MS legislation interpreting Directive
- Applies to all processing of “personal data”
- Additional requirements for “sensitive personal data”
- Core obligations rest with Data Controllers:
  - Process all PD in accordance with the data protection principles
  - Comply with subject access rights
- Data processors follow instructions of Data Controllers
- Regulation & enforcement by Information Commissioner
Overview of GDPR

- Directly-effective in MSs: no national variations
- Widened territorial scope

- Retains core concepts/definitions:
  - Data protection principles: Art 5
  - Identify conditions which justify processing

- Some additions to definitions and changes to conditions for processing
Key: where do I find....?

- Definitions: Art 4
- Data protection principles: Art 5
- Schedule 2 conditions: Art 6.1
- Schedule 3 conditions: Art 9
- Fair processing requirements: Arts 12-14
- Subject access rights: Art 15
- Rights of rectification, erasure, restriction: Arts 16-19
- Data controller obligations (data security, DP by design & default): Arts 24-25
- Data processing: Arts 28-30
Processing under the GDPR

Still require a Schedule 2 (Article 6.1) condition for processing personal data and a Schedule 3 (Article 9) condition for processing sensitive personal data.

The wording is similar to the DPA but not the same

Sensitive personal data:

- now “special categories of personal data”
- includes genetic or biometric data for the purposes of uniquely identifying an individual
Processing conditions: consent

Consent is Art 6 & 9 condition, but Article 7 makes reliance on consent more onerous:

- Must be able to “demonstrate” consent
- Requests for consent must be “clearly distinguishable from other matters”, “clear & plain language”
- Right to withdraw consent at any time: must be “as easy to withdraw as to give” consent
- Examination of whether consent is freely given or linked to contractual relationship
Processing conditions: Sch 2/Art 6

- Public authorities can’t rely on old 6\textsuperscript{th} condition of legitimate purposes (Article 6.1(f))
- Harder to rely on consent (Article 6.1(a))
- BUT there is a separate public/statutory function condition instead (Article 6.1(e))
  - \textit{processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller}
- Also “processing necessary for performance of contract” (Art 6(1)(c))
Processing conditions: Sch 3/Art 9

- Processing of SPD/special categories of PD is “prohibited” unless relevant condition identified [Art 9.1]

List of conditions similar but not identical to Schedule 3 DPA including:

- Explicit consent [Art. 9.2(a)]
- Vital interests of DS or another, where the DS is physically or legally incapable of giving consent [Art 9.2(c)]
- Legal proceedings [Art 9.2(f)]
Processing conditions: Sch 3/Art 9

- Processing necessary for… obligations and specific rights in the field of employment and social security and social protection law [if auth’d by EU or MS law or collective agreement providing for appropriate safeguards for fundamental rights & interests of the DS] (Art. 9.2(b));

- Processing necessary for reasons of substantial public interest, on the basis of EU or MS law…which are proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject (Art 9(2)(g));
Processing conditions: Sch 3/Art 9

Conditions specific to health & social care:

- **Art 9(2)(h):** Processing necessary for purposes of preventive or occupational medicine, for assessment of 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 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 [obligations of secrecy]
Processing conditions: Sch 3/Art 9

Conditions specific to health & social care:

Art 9(2)(i): Processing 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, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
Processing conditions: Sch 3/Art 9

Conditions specific to health & social care:

Art 9(2)(j): Processing necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.
Processing conditions: Sch 3/Art 9

- Article 9(4): MS can introduce further conditions (including limitations) for genetic or biometric data or data relating to health

- Specific provision on data relating to criminal convictions & offences
Particular categories of data subject

- Employees

- Children
  - Fair processing info must be suitable/particularly clear [Art 12]
  - If relying on consent under Art 6 for “offer of information society services directly to a child”, need verifiable consent of person with parental responsibility for person under 16/13 [Art 8]
Data processors

- More prescription of DC/DP relationship:
  - Detailed list of contents for data processing agreements (Art28)
  - Specific requirement on data processor to obtain data controller authorisation before sub-contracting
Data processors

- Re-balancing of relationship between data processors and both data controllers & data subjects
  - More direct obligations on data processors:
    - Keeping records of processing (Art 30)
    - Co-operating with ICO (Art 31)
    - Appropriate technical security measures (Art 32)
    - Notifying data controller of data breaches (Art 33)
  - Claims by DSs directly against DPs
  - DP becomes DC if breaches Art 28 requirements
The new approach to regulation: accountability
The new regime

- Principle of accountability: demonstrating compliance
- Records of data processing
- Self-assessment
- Risk-based regulation
- For you, all about systematic, evidenced approach
Accountability

- A new principle – with far reaching consequences.

  Art 5: “The controller shall be responsible for and be able to demonstrate compliance with [the data protection principles]”

- A catch all, but there are prescribed obligations.
  - Article 24 – security policies
  - Article 30 – records of processing activities
Accountability

Privacy Impact Assessments

Article 35 of the GDPR introduces a new obligation that PIAs have to be performed where the processing activities present a "high risk" to the rights and freedoms of individuals:

- Systematic processing to analyse behaviour;
- Large scale processing of sensitive personal data;
- Monitoring of public spaces

The ICO will produce a list.
Accountability

Privacy Impact Assessments

A PIA should contain:

- An assessment of the necessity and proportionality of the processing;
- a description of the processing, including the legitimate interest pursued by the data controller;
- an assessment of the risks to the rights and freedoms of data subjects; and
- the safeguards and measures to protect against those risks.
Accountability

**Privacy by design**
Appropriate technical and organisational measures having regard to:
- costs
- nature and scope of processing
- purpose of the processing
- risks posed to the data subject of the processing activities.

**Privacy by default**
Appropriate technical and organisational measures to ensure that only personal data that is necessary for a specific purpose of processing is processed. To comply, data controllers should take into account:
- the amount of data collected
- the extent of the processing
- the period of storage
- the accessibility to that data.
Accountability

Steps to be taken now:

- Ensure **systems are built** using data protection by design and by default and that privacy impact assessments are conducted when required.
- **Audit systems** processing personal data and the purposes for which the personal data is processed. These audit records should be updated regularly.
- **Employee training** provided on data protection by design and by default.
- If not already done, prepare a **template PIA** and train relevant employees in its use.
- **Begin to carry out a PIA in relation to each new data processing project** and ensure that such outcomes and compliance steps following the PIA are documented.
Records of processing

Article 30: Each controller "shall maintain a record of processing activities under its responsibility" which contains all of:

- name and contact details of controller, representatives, DPO
- purposes of the processing
- categories of data subjects and personal data;
- categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
Records of processing

Article 30 records (cont):

- any transfers of personal data to a third country or an international organisation (identification of country or organisation and documentation of suitable safeguards)
- where possible, envisaged time limits for erasure of the different categories of data;
- where possible, a general description of technical and organisational security measures
Security

- Appropriate technical and organisational security measures – flexible standard
  - DPA – security obligations only fell to data controllers
  - GDPR – similar security requirements but now extends to processors too
- Balance of cost, technology, and risk of breach and harm to data subjects
- Comply with data protection by design and by default
- Regular review
Notification of data breaches

- DPA: no mandatory notification but ICO recommends reporting “serious breaches”
- GDPR: mandatory notification, subject to certain exceptions
Notification of data breaches

GDPR

- **Supervisory authority:**
  - without undue delay and, where feasible, within 72 hours of first awareness.
  - If not feasible, a “reasoned justification” must be provided.
  - **No need to notify** if unlikely to result in risk to data subjects’ rights
Notification of data breaches

GDPR

- **Data subjects**: must be notified if the breach is “*likely to result in a high risk*” to rights and freedoms.
- **No need to notify if**:
  - The data is unintelligible to third parties (e.g. encrypted)
  - Measures are taken to ensure risk does not materialise (e.g. total recovery)
  - It involves disproportionate effort – can use public communication instead of individual notification
Compensation for data breaches

- **DPA:**
  - Liability for data controllers only
  - Material damage only – but expanded to include distress in *Vidal-Hall v Google*

- **GDPR:**
  - Liability for data controllers and data processors
  - Data processor’s liability limited to specific obligations/breach of instructions of the data controller
  - Includes distress
Data protection officers

All public authorities must have a data protection officer – can share with other public authorities

Must be independent

Need to have “expert knowledge of data protection law and practices”

Can be staff member or contractor
Data protection officers

- Point of contact for the public and ICO
- Inform the organisation and its employees of their obligations under the GDPR
- Monitor compliance with the GDPR, including audits
- Advise on data protection impact assessments
- Must have “due regard” to the risks associated with the processing operations
Data protection officers

- Involved “properly and in a timely manner” with all issues that relate to the protection of personal data
- Public authority to provide the “resources necessary” to carry out role, maintain expert knowledge
- Public authority to give access to all personal data and processing operations
Impact of the GDPR: Streetview
GDPR impact: Employment

Rebecca Pallot, Associate
rpallott@dacbeachcroft.com
0113 251 4786
Mandatory appointment of DPO

- **Scope**
  - Public bodies; and
  - Organisations who control large data sets for their core business i.e. large organisations

- **Duties**
  - Self-regulating role – report to highest level of management / maintain significant independence
  - Ensure regulatory compliance, staff training, co-ordinating with regulators

- **Protected employment status** – no dismissal / detriment for performing tasks
Data subject access requests

- Changes
  - Abolition of £10 fee
    - Anticipated increase in SARs of 25-40%
    - Exception for “manifestly excessive” requests, particularly if repetitive
    - Reasonable fee / no fee
  - Reduction in time period for response to 1 month
    - Extendable by 2 months where particularly complex/numerous
  - ICO still planning to operate a pragmatic approach
Conditions for processing

- DPA & ICO Guidance
  - Consent is problematic in the employment context
  - Employers should rely upon other conditions

- GDPR
  - Higher burden for consent
    - Freely given, specific, informed and unambiguous
    - Where consent given in broader document, must be clearly distinguishable
  - Move away from standard consent provisions in employment contracts
  - Consider other conditions for processing and update privacy notices
GDPR impact: Rights of data subjects

Sophie Devlin, Solicitor
sdevlin@dacbeachcroft.com
0113 251 4985
Enhanced rights

- Fair processing notices
- Profiling
- Right of portability
- Right of erasure
- Right of rectification
- Subject access requests
- Right to object and restrict processing
- Requests to exercise rights
Fair processing notices (Art 13 + 14)

Notices must be:
- concise
- transparent
- intelligible
- in an easily accessible form
Fair processing notices (Art 13 + 14)

They must include the following information:

- Who will receive the data
- Any international transfers and protection arrangements
- Retention period
- Right to rectification/erasure
- If relying on consent right to withdraw it
- Right to complain to ICO
- Whether personal data is legally required, what happens if it is not supplied
Fair processing notices (Art 13 + 14)

- Still going… remember to keep it concise!

- Details of any automated decision-making

- If data obtained from a third party, the source of the data

- Fair processing requirement is dis-applied if the data subject already has the relevant information
Subject access requests (Art 15)

- Recipients
- Retention period
- Right to rectification/ erasure
- Right to complain to ICO
- Source of data
- Profiling
- Out of EU arrangements
- No fee payable
Right to rectification (Art 16 + 19)

- Right to rectify inaccurate personal data maintained
- Right to have incomplete personal data completed
- Data controller must notify recipients of rectification unless impossible or disproportionate effort
- Data controller must inform data subjects of recipients if required
Right to erasure (right to be forgotten) (Art 17 + 19)

- Right to obtain erasure of personal data where:
  - PD no longer necessary
  - Data subject withdraws consent
  - Data subject makes valid objection to processing
  - Unlawfully processed
- If DC has made information public, it must take reasonable steps to inform other DC’s of the erasure
- Number of exceptions
Right to restriction of processing (Art 18 + 19)

- Mark personal data to restrict future processing:
  - Accuracy contested and to allow DC to verify accuracy
  - Unlawful processing and DS opposed to erasure
  - DC no longer needs PD but DS wants it for legal claims
  - DS objected to processing and DC needs to consider if legitimate grounds to continue
Right to data portability (Art 20)

- No equivalent right under DPA
- Right to receive copy of PD provided to DC in structured, commonly used and machine readable format
- Right to transmit that PD to another DC ‘without hindrance’
- Where possible, original DC must transfer directly to the other DC
- Only applies where:
  - PD processed by automated means
  - Processing based on consent or a contract
…and the best of the rest

- Right to object (Art 21)
- Right to object to automated decision-making (Art 22)
Other rights for data subjects

New general rules about upholding all of these rights:

- New obligation on data controllers to facilitate the exercise of DP rights (similar to FOIA duty to advise and assist)
- For all rights, action “without undue delay”, 1 month long stop, possible 2 month further extension
- If no action, a refusal notice within one month akin to FOIA refusal notice
- No charge
- If data subject requests/complaints are “manifestly unfounded or excessive” may charge a fee or refuse to act
GDPR impact: Integration & data sharing

Eleanor Tunnicliffe, Associate
etunnicliffe@dacbeachcroft.com
0113 251 4732
Topics in this section

- Processing conditions
- Fair processing notices
- Onward notifications
- Claims and liability
- Data portability
Processing conditions – personal data

Article 6(1)(e)

“Processing is necessary for the performance of a task carried out in the public interest”
Processing conditions – sensitive personal data

Article 9(2)(h)

“Processing is necessary for.... The provision of health or social care or treatment or the management of health or social care systems”
Article 9(2)(h)

- To rely on 9(2)(h) data must be processed:
  - by “a professional subject to the obligation of professional secrecy” or
  - by another person subject to an obligation of secrecy”
Article 9(2)(i)

- Covers processing “necessary for reasons of public interest in the area of public health such as... ensuring high standards of quality and safety of health care and of medicinal products or medical devices...”
Article 9(2)(i)

“….which provides for suitable and specific measures to safeguard the rights and freedoms…..in particular professional secrecy”
Data subject rights

Fair processing notices
- Content
- Provision

Joint data controller arrangements

Onward notifications
Claims

- New duty to notify individuals
- No need for material damage
- Can claim in full against any organisation involved in the processing
- Defence if “not in any way responsible”
- Can clawback from others
Data portability

- Applies if rely on consent or contract conditions
- Most likely to apply to private sector services
- A shift in demand
Practicalities

Sophie Devlin, Solicitor
sdevlin@dacbeachcroft.com
0113 251 4985
DON’T PANIC
What to do next?

- Identify dataflows
- Review the data processing you do and identify legal basis. In particular, review:
  - where you are relying on consent
  - contracts (lead in times)
  - data processing & sharing arrangements
- Raise awareness at senior level, in procurement/IT teams
- Consider specific areas of impact e.g. children’s services
What to do next?

Also:

- Review data breach notification processes
- Get into the way of DP by Design and PIAs (start doing PIAs for big/sensitive projects)
- Start thinking about the data protection officer role
- Review implementation of data retention/destruction policy
ICO guidance

- Three phases of guidance promised – but pre-Brexit
- Start subscribing to ICO newsfeeds etc!
Discussion on Impact & Next Steps