

EU Data Protection Reform

Interpretations at GP level



EU Data Protection Reform

Why GDPR

BREXIT
implications

EU GDPR
Reform key
aspects

GPs getting
ready

Further
resources, help
and advice

Why the DP reform?

- Strengthens citizen's rights (where is my data, when is shared, consent, right to be “forgotten, children data)
- Adapts better to new technological challenges (e.g. switching service providers – how does data portability work?)
- Dealing with Big Data and Social Networks
- Strengthens the internal market
- Making easier international cooperation
- Simplifying some existing rules

GDPR & BREXIT

- Uncertainty about the implementation in the UK
- GDPR still relevant for a large number of data controllers
- GDPR comes into force in the UK on 25 May 2018
- ICO and SG preparing guidance & overview of the law
- GDPR allows some manoeuvre margin for National derogations and exceptions in certain matters
 - e.g. national security, defence, prevention/investigation of criminal offences, other important public interests, enforcement of civil law matters etc.
 - Access to official documents, National ID numbers, archiving/scientific/historical research, secrecy obligations, churches & religious associations.

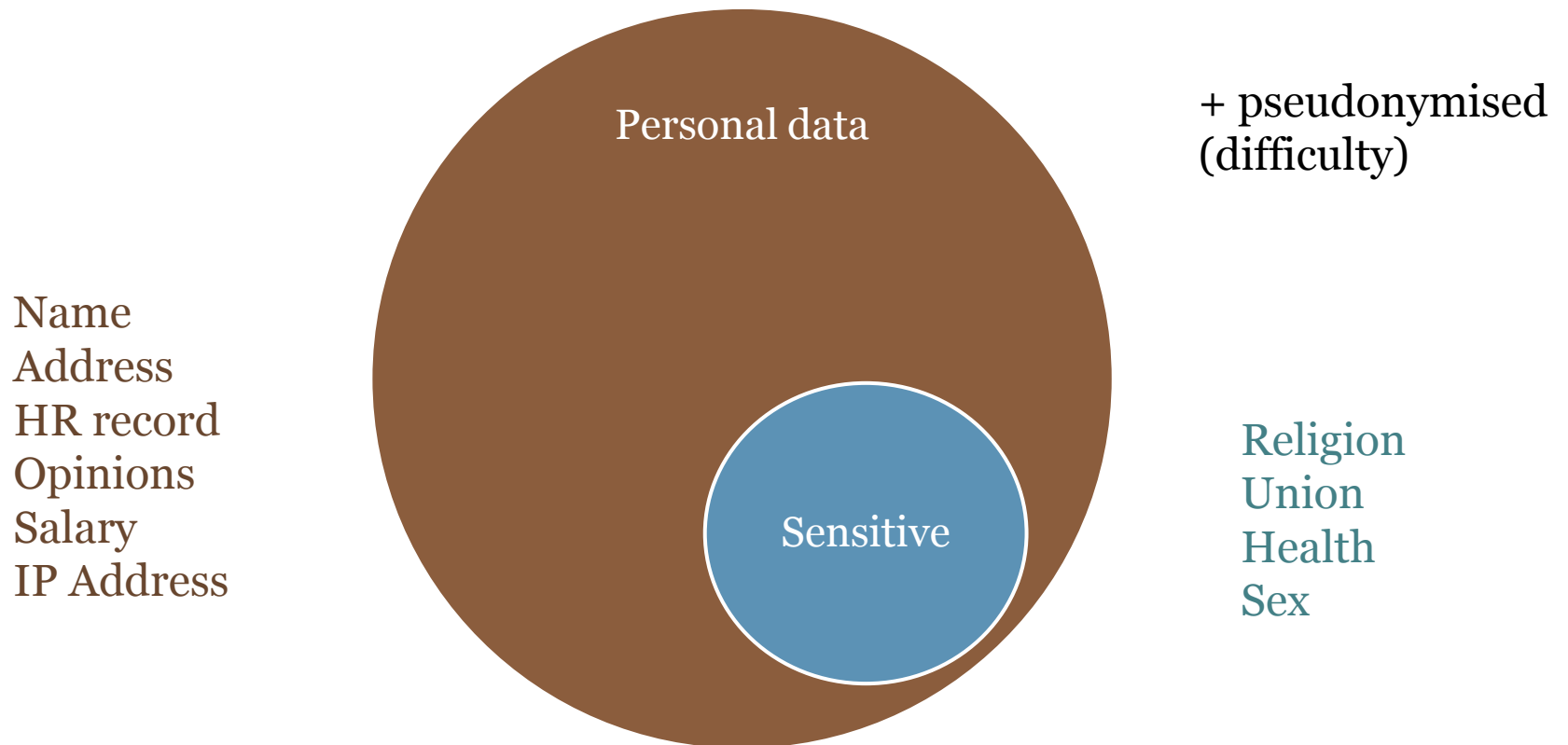
Does the GDPR apply to GPs?

- applies to
 - ‘controllers’ **and** ‘processors’ (same as DPA 1998)
 - processing carried out by organisations operating within the EU
 - organisations outside the EU that offer or receive goods or services from/to the EU.

The GDPR does not apply to certain activities (e.g. [Law Enforcement Directive](#), processing for national security purposes and processing carried out by individuals purely for personal/household activities.

What information does the GDPR apply to?

automated personal data and manual filing systems where personal data are accessible



EGDPR does NOT change current legal basis for GPs to process sensitive data

- The main reason for GP's processing is necessity for **medical purposes** but there are others, e.g. legitimate interest, vital interest, legal obligation, consent
- **Medical purposes**
 - Processed by a health professional (or equivalent duty of confidentiality)
 - Includes preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.


GDPR Principles

- Similar to those in the DPA
 - Lawful & fair processing, specified purposes, adequate & relevant, minimum necessary, accurate & up to date, technical & organisational security ...
- The most significant addition is the **accountability** principle.
- The GDPR requires you to show **how you comply with the principles**
 - e.g. by documenting the decisions you take about a processing activity

GDPR
elevates
their
significance



Rights for individuals

- The right to be informed
 - The right of access
 - The right to rectification
 - The right to erasure
 - The right to restrict processing
 - The right to data portability
 - The right to object
 - Rights in relation to automated decision making and profiling.
- 
- Right to be forgotten

What all this means for GPs?

- Demonstrate compliance
- Report data breaches
- Don't send data out with the EU unless the country has equivalent protection (or there is a mandate)
- *Keep an eye on ICO and SG updates on GDPR and new UK legislation on data protection*
- *Appoint a DPO (if you like – not mandatory for most GP as not considered public authorities and under 250 employees).*

How can GPs demonstrate compliance?

- Have a continual security improvement plan
- Keep internal records of your data processing activities
- Think of data protection by design and data protection by default. For example:
 - Data minimisation, Pseudonymisation, Transparency and continually improving security (continual improvement cycles)
- Use data protection impact assessments where appropriate.
- You can also
 - adhere to approved codes of conduct and/or certification schemes.
 - arrange expert data protection advice at hand (even if you are not required to appoint a DPO)



What should GPs record(*)?

- Name and details of your organisation, your representative and data protection officer (+partners & data processors)
- Purposes of the processing.
- Description of the categories of individuals and personal data.
- Categories of recipients of personal data.
- Details of transfers to third countries including documentation of the transfer mechanism safeguards in place.
- Retention schedules.
- Description of technical and organisational security measures.
- Contracts with data processors, information sharing activities and any relevant agreements
- Records of controversial decisions (e.g. prejudice tests, privacy assessments, etc.)
- You may be required to make these records available to the relevant supervisory authority for purposes of an investigation.

(*) similar to 'registrable particulars' under the DPA which currently must be notified to the ICO.

Obligation to report data breaches

- report certain types of data breach to the relevant supervisory authority, and in some cases to the individuals affected.

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

- Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you must notify those concerned directly.

The Scottish Information Sharing Toolkit

For organisations involved in the protection, safety, health, education and social welfare of the people in Scotland, including statutory, private and voluntary sector organisation

Improving Information Governance in Scotland - a package of measures



The IS Toolkit approach

Helping practitioners in public bodies in Scotland navigate their way through all the steps that need to be completed for sharing information in a safe and intelligent way.



From the more strategic decisions to the more operational arrangements

<http://www.informationgovernance.scot.nhs.uk/>

The screenshot shows a web browser displaying the 'IS Toolkit' page on the 'Information Governance' website. The browser's address bar shows the URL www.informationgovernance.scot.nhs.uk/is-toolkit/. The page header features the 'Information Governance' title and the 'The Scottish Government' logo. A navigation menu includes 'Home Page', 'News', 'Blog', 'Key Groups & Topics', 'IS Toolkit', 'PBPP', 'IG Publications', 'FAQ', and 'Contact us'. A search bar is located in the top right corner. The main content area is titled 'IS Toolkit' and contains text about the 'Scottish Information Sharing or Personal Information 2013' and the 'Information Commissioner's Office'. A dropdown menu is open over the 'Key Groups & Topics' navigation item, listing 'Caldicott', 'GIRFEC', 'H&SCI', 'SPIRE (GPs)', 'Information Security', and 'Police'. Below the main text, there are three columns of content: 'IS Toolkit Standard', 'Approach', and 'Resources', each with an icon and a 'More Info' link. The 'Recent Posts' section on the right shows a post titled 'Where and what are the boundaries of the 'safe haven' which are being accredited...'.

Additional resources and advice

- **Information Commissioner Office** www.ico.gov.uk (guide to Data Protection and EU GDPR)
 - or ask for advice from your **NHS Board Data Protection Officer**
 - **National templates, guidelines and policies**
 - www.informationgovernance.nhs.scot.uk
 - **NHS Policies & Privacy Notices**
 - **ISO 27001 ISMS** – Information Security set of policies
 - Confidentiality & Data Protection Policy
 - **National leaflets & Privacy Notices**
 - <http://www.nhsinform.co.uk/>
 - **Scottish Primary Care Information Resource**
 - <http://www.spire.scot.nhs.uk/>
- **The Scottish Government Information Assurance & Governance Team (NHS Scotland, Health and Social Care), eHealth Division** - 0131 244 2373