brownrudnick

Data Protection
Top Tips for Digital Health Companies

Mark Lubbock, Partner
Ruth Arkley, Associate

24 March 2021

Today's Agenda

1. Key elements of the legislation
2. Notable post-Brexit issues
3. Health data landscape
4. Case studies
5. Top tips

Why is Data Protection Important?

- Covid – access to data critical to making decisions on how to manage public health.
- Data innovation in UK healthcare driven by:
  - Better data leads to better outcomes and better use of resources e.g. improving availability of national collections of clinical and treatment outcome datasets.
  - Leads to growing investment and support for AI and machine learning in the healthcare sector.
- Fines.
- Health is a special category of data – more difficult.

Data Protection Legislation

- **General Data Protection Regulation (EU) 2016/679 (GDPR):**

  - **retained** by s.3 of the European Union (Withdrawal) Act 2018
  - **amended** by the 'Data Protection Brexit Regulations'
  - **supplemented** by the UK's pre-existing **Data Protection Act 2018**

- Fines of up to **€**20 million (£17.5 million) or 4% of annual turnover (whichever is the higher)
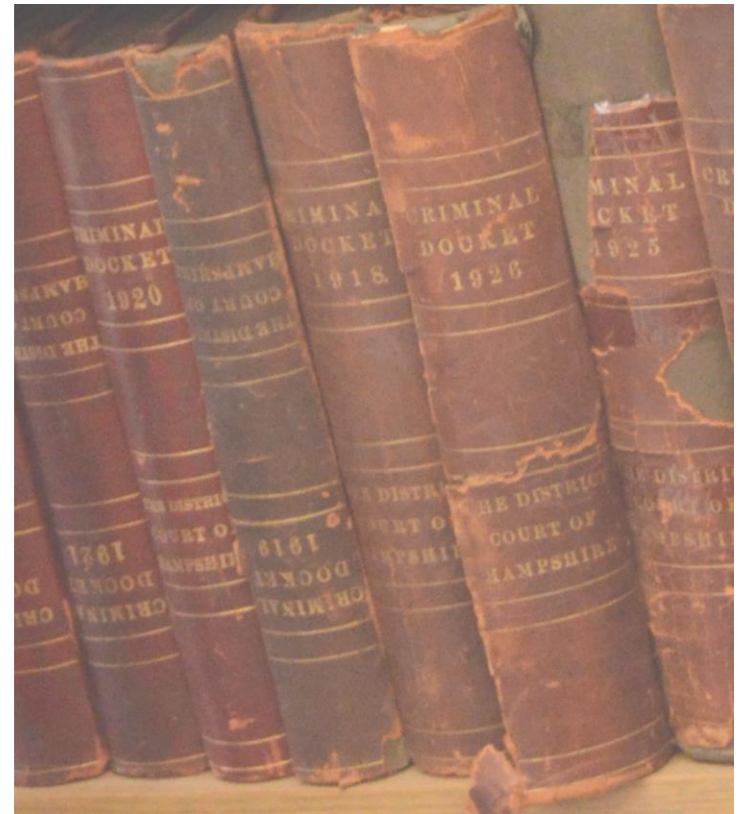
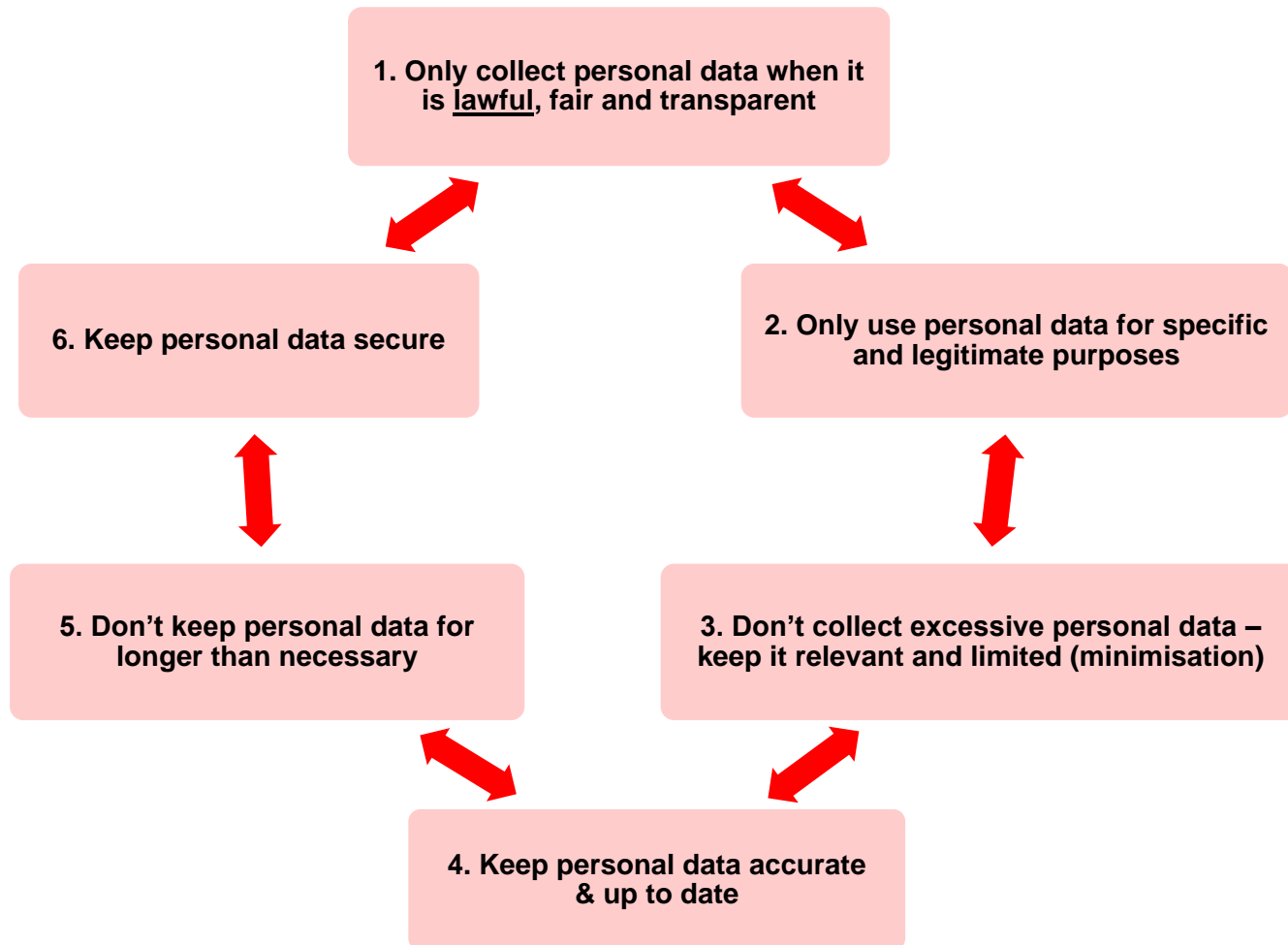# What *is* 'Personal Data'?

- Defined in the GDPR as:

  "**any information** relating to an **identified or identifiable natural person**; 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"

- Not just names and contact details
- No confidentiality requirement
- Could <u>anybody</u> use this data – alone or in combination with other data - to identify somebody?

Some Other Definitions

- **Controller** = makes decisions about how data is collected and used.

- **Processor** = acts on the instructions of a data controller (e.g. AWS).

- **Processing** = any action performed on data (collecting, storing, analysing, checking, referencing – anything you can think of!).

- **Data subject** = the individual to whom the personal data relates.

- Also definitions concerning biometric data, data concerning health and genetic data.

Your GDPR obligations

1. Only collect personal data when it is <u>lawful</u>, fair and transparent

6. Keep personal data secure

2. Only use personal data for specific and legitimate purposes

5. Don't keep personal data for longer than necessary

3. Don't collect excessive personal data – keep it relevant and limited (minimisation)

4. Keep personal data accurate & up to date

Must **demonstrate compliance** with these principles.

Territorial Scope

- **Specific gateways:**

1. Processing 'in the context of' an establishment
2. The controller/processor is <u>not</u> 'established' in the territory, but it:
   a) Offers goods or services to individuals in that territory, or
   b) Monitors individuals' behaviour in that territory

- **Case law:** *Weltimmo, Soriano*

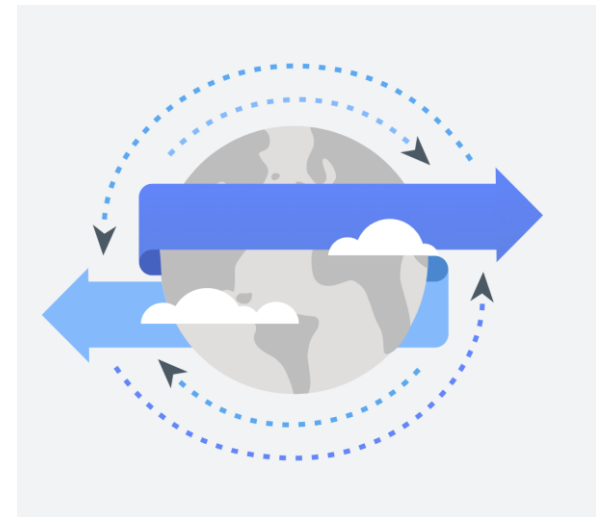# Post-Brexit Changes: Transfers

- **From the UK**
  - UK will be able to make its own adequacy decisions
  - "Disappointed" by *Schrems II* decision – expect pragmatism?
  - ICO may make its own 'Model Clauses'

- **From the EU to the UK**
  - Draft adequacy decision
  - Revising Model Clauses

Other Post-Brexit Changes

- Representatives
- Lead supervisory authority
- Reform?

MP Oliver Dowden:

"a slightly less European approach as set out in GDPR by focusing more on the outcomes that we want to have and less on the burdens of the rules imposed on individual businesses".

Broad Considerations – How GDPR deals with Health Data

- To process - need to satisfy both Article 6 and Article 9.
- Article 6 – consent, legal obligation, public interest* and legitimate interest.
- Article 9 – explicit consent, substantial public interest*, medicine and healthcare*, contract with health professional, public health interest* and archiving.
- Member states can enact further conditions on processing of genetic data, biometric date and data concerning health.
- Article 23 – member states can restrict some rights for public health reasons (article 9(4)).
- Article 89 – derogations permitted for scientific research provided suitably protected and minimised.

*based on EU or member state law.

Health Data Landscape – EDPB Guidance on Health Research

Key Issues:

- CTR consent different to GDPR consent.

- Consent may not legitimise processing in a trial context.

- Public interest/scientific research legal bases – rely on specific Member State/EU Law.

- Subsequent processing with different purpose/changed legal basis, controller must give subject information.

- Data retention depends on purpose.

- Anonymous and pseudonymous data.

Issue: DeepMind/the Royal Free

- In 2015, the Royal Free shared the personal data of 1.6 million patients with DeepMind.

- In July 2017, the ICO ruled that the Royal Free was in breach of the DPA.

- The ICO found that:

  1. Patients had not been properly informed about the processing of their data.

  2. Processing was not transparent or proportionate.

- The importance of the NDG's view on the sharing of confidential personal information.

- Deepmind were not part of the direct care team and the NDG's view is the confidentiality must be judged from the patient's perspective.

Novartis ICO/Sandbox

- Sandbox beta phase launched 2019 – 2020
- Novartis report released February 2021
- 'Digital Solution' to:
  - reduce face-to-face appointments
  - help triaging and decision-making
- Consideration of controller/processor role
- Can speech/voice data be considered 'biometric' or 'special category biometric' data?

Top Tips!

1. Take an active approach to compliance.
2. Important to collect the data in the right way.
3. The law is evolving quickly – keep tracking.
4. Map applicable laws and transfers – be wary of sharing data.
5. Privacy by design - talk to the experts!

Boston
One Financial Center
Boston, MA 02111
+1.617.856.8200
+1.617.856.8201

London
8 Clifford Street
London W1S 2LQ
+44.20.7851.6000
+44.20.7851.6100

Orange County
2211 Michelson Drive, 7th Floor
Irvine, CA 92612
+1.949.752.7100
+1.949.252.1514

Providence
10 Memorial Boulevard
Providence, RI 02903
+1.401.276.2600
+1.401.276.2601

Hartford
185 Asylum Street
Hartford, CT 06103
+1.860.509.6500
+1.860.509.6501

New York
7 Times Square
New York, NY 10036
+1.212.209.4800
+1.212.209.4801

Paris
1, rue François 1er
75008 Paris
+33(0)1.85.56.82.20
+33(0)1.85.56.82.21

Washington, DC
601 Thirteenth Street NW, Suite 600
Washington, DC 20005
+1.202.536.1700
+1.202.536.1701