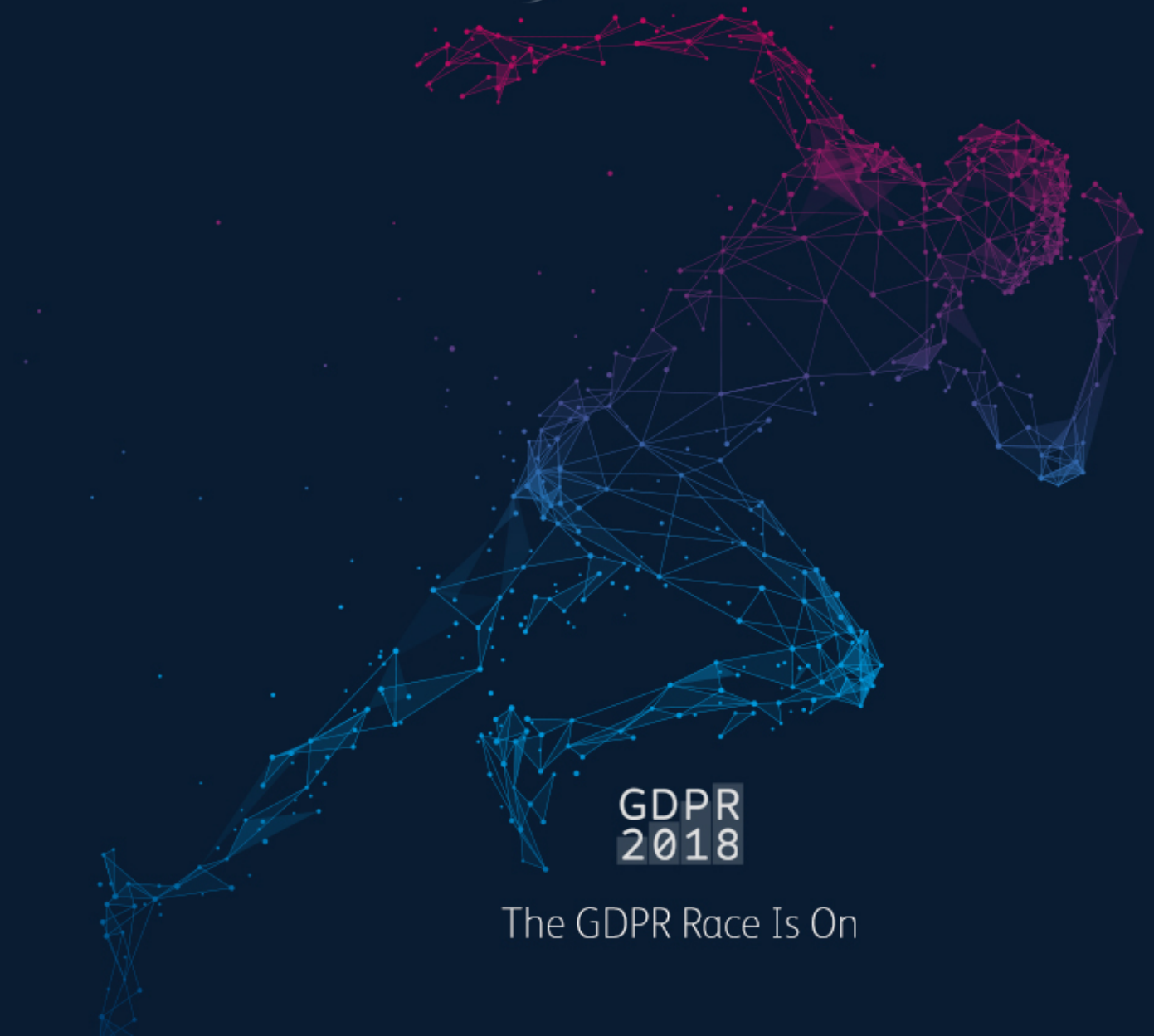
irwinmitchell



GDPR 2018

The GDPR Race Is On

GDPR – what is it?

- Replaces the Data Protection Act 1998
- European legislation – will not be gold plated
- Comes into force **25 May 2018**
- BREXIT
- Data Protection Bill

Why is GDPR relevant to me?

- Healthcare has been an area of particular interest to the ICO.
- Fines/ investigations have been common.
- For example, HCA International fined £200k in February.
- See health care resources on ICO website.
- Low awareness of GDPR in the sector.

What is captured?

- What is personal data?
- Data Controllers and Data Processors
- The Regulation applies to:
  - the processing of “Personal Data”
  - by automated means
  - **AND** by non-automated means
- Ordinary personal data
- Sensitive personal data

First steps to becoming compliant

- Understand the data you hold
- Analyse the personal data and determine lawful purposes
- Just because it was permitted under DPA does not mean that it will be permitted under the GDPR

Basis for processing

GDPR lawful purposes for **ordinary personal data:**

- Consent
- Legitimate interests of the data controller
- Necessity for the performance of a contract

GDPR lawful purposes for **special category personal data**:

- Explicit consent
- Vital interests
- Necessary for establishment or defence of legal claims

Transparency and consent

- Review your fair processing notices and privacy policies
- Consent must be:
  - unambiguous
  - freely given
- Requires clear affirmative action
- For sensitive data, must be explicit
- Can be withdrawn at any time
- Not available where there is a clear imbalance in the relationship
- Multiple purposes need multiple consents

Administrative steps

- Audit your contracts
- Train your staff
- Consider appointing a DPO
- Undertake Privacy Impact Assessments
- Prepare to deal with enhanced rights of individuals/ ICO

Possible consequences

- 2 tier system:
  - Up to €10 million or in the case of an undertaking, up to 2% of global annual turnover, whichever is higher.
  - Up to €20 million or in the case of an undertaking 4% of total worldwide annual turnover
- Position under DPA - financial loss required
- Position under GDPR - any damage suffered should be compensated

Dr Natalie Blakely
Consentz
Co-Founder & Chief Medical Officer

Consentz
The Medical Practice Software Company

GDPR – Individual's Rights

Right to be Informed:

- Understand how data is stored and used
- The language explaining this should be clear & concise

Right of Access:

- Individuals have the right to obtain access to their personal data.
- Provide requested data free of charge within 1 month

Right to Rectification:

- Individuals have right to correct their personal information

GDPR – Individual's Rights

Right to Erasure:

- Data can be held only for as long as is necessary
- Deletion of personal data when requested (unless needed)
- No requirement to delete if held for a defence claim

Right to Portability:

- Shouldn't apply to clinics as little processing would be by automated means, most would be by human intervention.

Right to Object:

- Stop receiving direct marketing – this should be clear at the point of 1st communication and subsequent communications

GDPR – Accountability & Governance

Clinics process *special category* data and need to have documentation on processing activities, data protection policies, staff training and HR policies.

Implement measures such as:

- Data minimisation & transparency
- Access levels, erasure & correcting
- Improving security features on an on-going basis

Data Breach - such as loss of a health record due to lack of appropriate controls.

Reporting time scales are short and therefore require robust detection, investigation and reporting procedures to be in place

GDPR: Big Burden or Glorious Opportunity?

Embrace the challenge!

A high quality digital platform will:

- Address fully the issues arising from GDPR regulation, as well as
- Transforming practice management and patient care

Consentz
The Medical Practice Software Company

Consentz – Built for GDPR

Consentz Terms and Conditions address the above points (prepared by Stuart, Irwin Mitchell)

GDPR features include:

- Time period for retention & report for files to be erased
- Patient access to their information
- Patient can change personal information remotely

Consentz – How Else Are You Protected?

Your records are secure with Consentz:

- Encryption
- Cyber security insurance
- Information Recovery Plans
- Data security monitoring
- Regular penetration testing by global data security company
- Hourly data back-ups
- Instantly revoke staff access

Any Questions?

Thank you for listening.

We’re on Stand D111

We’re here to help!

Consentz
The Medical Practice Software Company