

Digitalisation and Big Data: implications for the health sector.

Legal and Regulatory Aspects

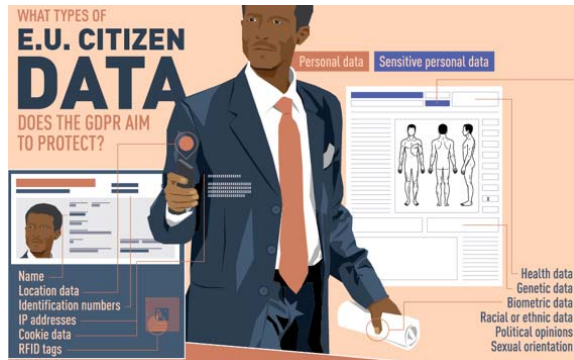
David Supple, Zissou Projects Ltd



Overview

- On 25 May 2018 new European Union (EU) data privacy legislation, the General Data Protection Regulation (GDPR) came into effect. It replaced the existing national Data Protection laws in EU countries and created (*in theory*) a uniform data protection framework.
- The GDPR hasn't brought manifestly significant approaches to data protection and privacy – organisations in the health sector have always needed to take this subject very seriously – however from an individual's perspective, it enhances their rights around their personal data and places a responsibility on them to understand the reason why their data is being collected, how it's used, shared and secured.
- GDPR (and the many other privacy regulations across the world) requires time, resources and an on-going commitment to ensure you stay on the right side of the regulations – the outcome if you don't, can be severe!

Who does GDPR apply to?



GDPR brings increased accountability

- The GDPR does not prohibit the use of personal data for legitimate purposes, but it does place increased accountability on the organisations using it.
- In today's modern economy, data has become a valuable commodity, and if you are collecting such data you need to instill a culture of being **honest and transparent** about it.
- GDPR brings with it new mandatory breach reporting rules and heavy fines of up to €20m or 4% of a Group's annual worldwide turnover, whichever is higher, for non-compliance and breaches of the regulation.

Key health specific challenges

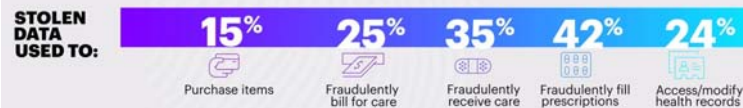
- Are patients interested in a healthier nation?
- Are patients interested in a healthier nation more than they are interested in their own health?
- How do we demonstrate the responsible sharing of their data can lead to better patient outcomes?
- How do we explain the relationship between the three?

- Where is the balance to be struck between leveraging data for research and clinical purposes to protecting patients rights to privacy?
- Fast moving challenges against the trend – '*Attitudes towards the impact of digitalisation and automation on daily life*' was pre Cambridge Analytica
- **Equitability** of engagement – upper middle class vs working class, impact of age and poverty on access to services

- How do we secure data, when patently we have failed so many times to do so previously
- How do we keep the strategy moving when the risk of failure (in fines, reputation and compensation) is now so great?

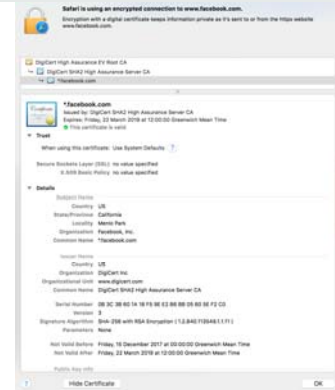
Trust and Harm

Healthcare Data Breaches Among England Consumers



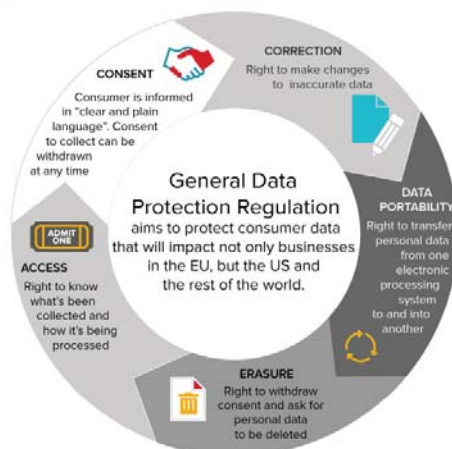
Source: Accenture Survey, 2017

NUMBER OF RECORDS BREACHED BY INDUSTRY IN FIRST HALF OF 2017



Rights and Obligations

CONSUMERS RIGHTS



DATA OBLIGATIONS FOR COMPANIES



Consent

The consent request should:

- ✓ Be easy to understand, prominent and concise,
- ✓ Include the name of your organisation and any third parties,
- ✓ Explain why you want the data,
- ✓ Explain what you will do with it,
- ✓ Remind Data Subject that he can withdraw consent at any time,
- ✓ Be specific wherever possible,
- ✓ Be kept under periodic reviews,
- ✓ Explain how long will you keep the data,
- ✓ Explain what data are you collecting.

And the consent request should NOT:

- ✗ Use pre-ticked boxes, opt-out boxes or default settings.



Trans-Territoriality

TERRITORIAL SCOPE



Article 3

If you don't have a formal presence in the EU zone, but process the personal data or monitor the web behavior of EU citizens, the long arm of the GDPR can reach out to you.



How will the EU enforce Article 3?

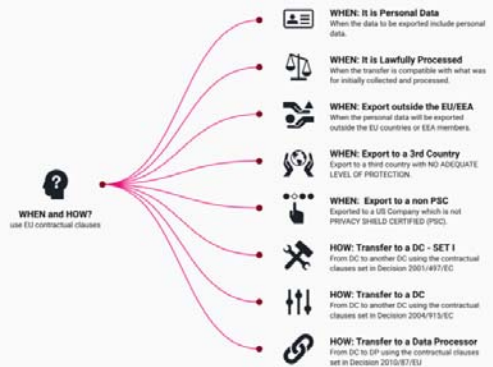


Will other countries then respond with their own border-less data laws?



When and How to use the EU Contractual Clauses

INTERNATIONAL TRANSFER OF PERSONAL DATA



by www.privacyshield.com

View from the Regulators

- Unlike planning for the Y2K deadline, GDPR preparation didn't end on 25th May 2018 – it requires ongoing effort.
- It's an evolutionary process for any organisation – 25 May was the date the legislation took effect, but no organisation stands still. You'll be expected to continue to identify and address **emerging** privacy and security risks in the weeks, months, and years beyond May 2018.
- Key building blocks should be identified:
 - Organizational commitment
 - Understand the information you have
 - Implement accountability measures
 - Ensure appropriate security
 - Train staff