Sarpal Consultancy

Solutions to Business Problems

GDPR Nostalgia?

Baljit Sarpal

BCS Business Change SG

15th December 2020

GDPR enforced

- Between 2018 and 2019, the average number of fines issued per month increased by 260%
- Over 220 fines have been handed out for GDPR violations in the first ten months of 2020
- Still only 20% of US, UK, and EU companies are *fully* GDPR compliant

(source Tessian)

- Different supervisory authorities approach enforcement with varying degree of vigour
- The fines imposed have also differed by SA.

May 2018

GDPR enforced

Sarpal Consultancy

- **Ticketmaster: £1.25m** fine for failing to protect customer payment information
- **Cathay Pacific: £500k** fine for not securing personal data
- **Google (France): €50m fine** for not being transparent of data gathering and targeted advertisements
- **H&M (Germany): €35m fine** for unlawful monitoring of staff
- **Telecom Italia (Italy): €28m fine** for multiple unlawful actions relating to aggressive marketing
- **Wind (Italy): €17m fine** for unlawful marketing activity by the telecom company
- **Google (Sweden): €7m fine** for failure to implement right to be forgotten
- **AOK Health Insurance (Germany): €1.2m fine** for unlawful direct marketing and processing
- **Marriott International Inc.: £18.4m fine** for failing to secure millions of customers' personal data – original intent was to fine **£99m.**
- **BA : £20m** fine for failing to protect personal and financial information of 400,000 customers. Original intention was to issue fine of **£183m**

GDPR Change Initiatives

Sarpal Consultancy

- **Assessment of Business Processes**
  - What personal data is processed?
  - Who processes the data?
  - Where the data is processed?
  - How is the data stored?
  - How is the data secured?
- **Assessment of risk**
  - Risk for the individual
  - Risk to the organisation
- **Remediation Plan & Business Case**
  - Risk Appetite
  - Sector specifics
- **Implement Change**
  - Organisation
  - Training
  - SAR & Data Breach
  - Technology
- **Continuous Monitoring**
  - Incident Management
  - Risk Management
  - Change Management – new initiatives

Change is not singular!

We live in interesting times…….

Sarpal Consultancy

UK GDPR
Adequacy Status

International Transfers

EU GDPR

UK Data Protection Act 2018

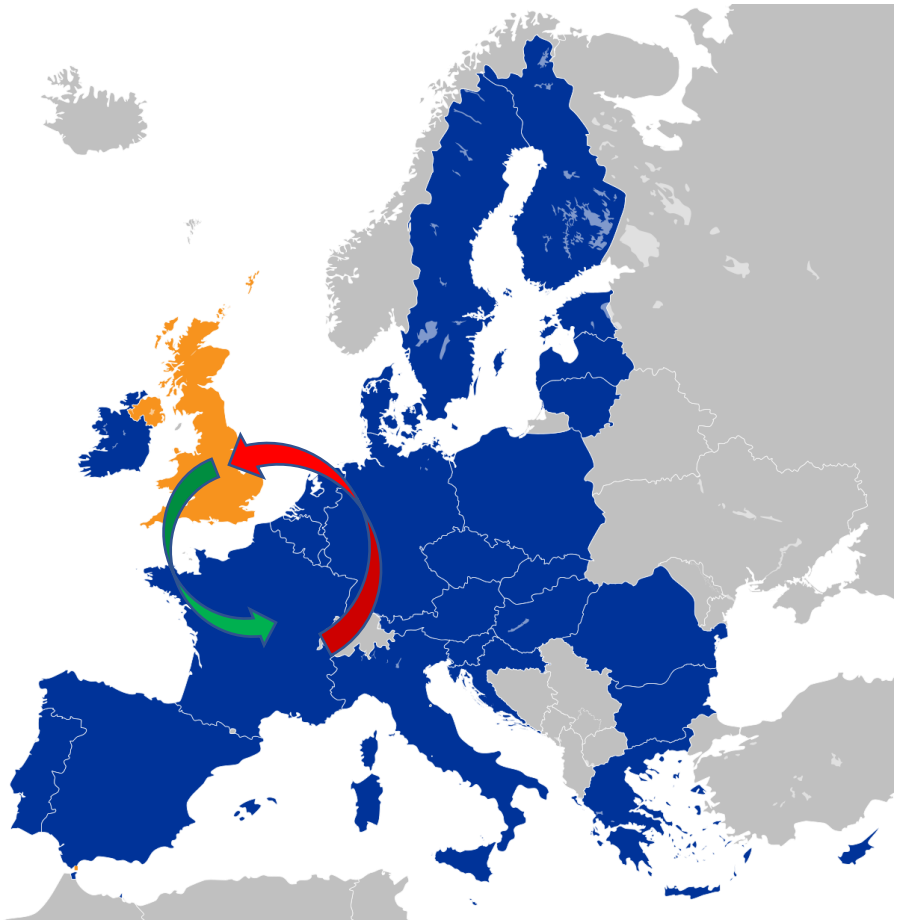
Sensitive Personal Data
Monitoring
Test & Trace
Working from Home

Brexit

Sarpal Consultancy

- UK will transpose GDPR as the UK GDPR on exit
- UK & EU will become "3rd countries" in the respective GDPR
- UK has already agreed to consider EU as being "adequate"
- EU has NOT yet designated UK as having an adequacy status
- Exports of personal data from an EU country to UK will no longer be unrestricted
- Exports of data only permitted with specific controls (BCR, SCC) or exceptions for occasional transfers.

- This will have impact on organisations using Cloud Services – e.g. AWS & Azure typically hosted in Ireland.



Schrems II

Sarpal Consultancy

- In July 2020 ECJ struck out Privacy Shield as not being a sufficient control on the export of personal data from the EU to US
- It ruled that other mechanisms such as BCRs and SCCs could be used
- **BUT** each transfer of data must be risk assessed based on the data being exported and laws of the 3rd country regarding the protection of the personal data within the jurisdiction.
- This effectively requires the organisation to undertake a Transfer Impact Assessment based on the types of data and the likelihood of government agencies seeking access to the data in the 3rd country.

- Will impact organisation who utilise Cloud Service Providers

- **Assess the risks**
- **Minimise the data exported**
- **Put in place technical and organisational and legal controls with the importer.**

Covid-19

Sarpal Consultancy

Workplace Monitoring

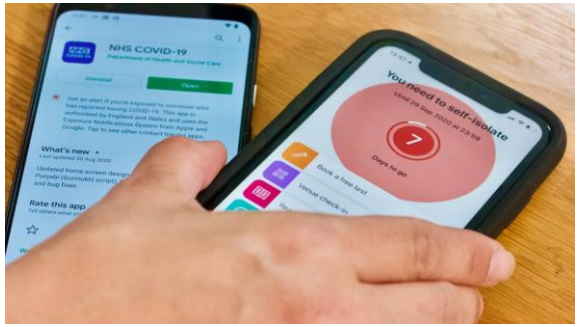
Prevent employees getting infected by others at work.

- What do you need to achieve?
  - What's the legal requirement to monitor individuals?
  - Do you actually need to record personal information for that purpose? Can it be done in an alternative way?

- **Minimisation Principle**

Test & Trace App

Control the spread of infection in the population.



Need high take-up to be effective

- Centralised vs Decentralised
  - **Centralised** – data is stored on central servers and matching done centrally manged by government/health bodies.
  - **Decentralised** – data is stored on individual's device, only the anonymised key of the other contacts is stored on the device. Matching done by individual's mobile device.

- **Minimisation Principle**

Summary

Sarpal Consultancy

- Data Privacy is not a one off activity - it has to be embedded into organisation's Change Management activities
- Need to be clear about what is the business objective - **Purpose Assessment & Purpose Limitation**
- What are the risks to the individual's rights and freedoms- **Risk Assessment**
- How can we achieve the business outcomes in the least impactful way - **Data Minimisation**
- How can we monitor - **Effective Controls**
- How do we achieve this cost effectively - **Privacy by Design**

Thank You!

Sarpal Consultancy

Solutions to Business Problems

Questions?

baljit.sarpal@outlook.com

Tel: 07740098784

https://www.linkedin.com/in/baljit-sarpal-4b2b335/

Dr Baljit Sarpal

CIPP/E, CIPM

PRINCE2 Practitioner