

Life after divorce: UK data protection policy, law and regulation

Professor Ian Walden

7th March 2024

Introductory remarks

- Thus spoke Ian Walden.....
 - Pro-remain
 - No fan of the Conservative government!
 - Data protection academic and practitioner since 1987
 - Member of Commission Multistakeholder Expert Group to support the application of Regulation (EU) 2016/679
- Implications of reform for the UK?
 - Commission Adequacy Decision (2021/1772)
 - Sunset clause: Art. 4, 27 June 2025
 - Court of Justice views on UK intelligence gathering
- Implications of reform for the EU?
 - EDPS: “We need genuine debate on whether current data protection legislation.... is actually serving people in the way it was designed to.”

...and issues that map those addressed through the rest of the programme

UK data protection laws

- Data Protection Act 1984
 - Council of Europe Convention 108
- Data Protection Act 1998
 - Directive 95/46/EC
 - Commission threatens action against the UK (June and September 2010)
- Freedom of Information Act 2000
 - Section 40 *Personal Information*
- Privacy and Electronic Communications Regulations 2003
 - Directive 02/58/EC, as amended
- Data Protection Act 2018
 - General Data Protection Regulation 2016/679 has become the ‘UK GDPR’
 - *King (on behalf of the 3Million & ORG) v Secretary of State for the Home Department* (2023)
 - Part 3: Law Enforcement Processing (Directive 2016/680)
 - Part 4: Intelligence Services Processing

GDPR: Not without criticism....

- Commission Two-year review (June 2020)
 - Problems with ‘one-stop-shop’ mechanism
 - Too much variation
 - Compliance burden for SMEs
- “EU must overhaul flagship data protection laws, says a ‘father’ of policy” *Financial Times* (3 March 2021)
 - Alex Voss:
 - “We cannot stick with principles established in the 80s that do not reflect the new situation we are living in.”
 - Sophie in’t Veld: “The idea that we have overlooked something is not plausible.”
- Wojciech Wiewiórowski (EDPS): “acknowledging there may be structural issues behind the malfunctioning of the GDPR” (2022)

Policy objectives

- ‘Data: A new direction’ (September 2021)
 - Data as the fuel..... in a hyper-connected world
 - Unleashes data’s power across the economy and society for the benefit of British citizens and British businesses
 - Unnecessarily complex or vague, and which continue to cause persistent uncertainty over three years after its introduction
 - Data sharing, especially for research
 - Delivering better public services
 - Joined-up data: COVID-19 experience
 - UK’s status as a global hub for the free and responsible flow of personal data
 - Interoperability
 - Competence and pragmatism of its regulatory institutions
 - more risk-focused regulator
 - UK's worldwide reputation for high data protection standards

Data Protection and Digital Information Bill

- Consultation process
 - Government responded to feedback: proceed, not proceed, further consideration
- Amendments to the UK GDPR and the Data Protection Act 2018
 - Part 1: Data protection
 - Part 4: Privacy and electronic communications
 - Part 5: Information Commission
- Committee Stage in the House of Lords
- Net direct monetised benefit of £1.04 billion over 10 years
 - More research and innovation, while easing cost of compliance
 - Commissioner Reding (January 2012): “This will reduce the administrative burden on companies and save an estimated €2.3bn a year.”
 - Further benefits difficult to quantify in economic terms
 - e.g. better data-sharing between public authorities leading to more effective delivery of public services

Compliance issues

- Principle of accountability
 - Compliance as ‘box-ticking’
 - ‘Privacy management programmes’
 - Modelled on Singapore & Canada
- Controller obligations
 - Remove requirement for DPIAs (Art. 35)
 - Bill: retained but name change: ‘Assessment of high risk processing’
 - No requirement for prior consultation with the ICO (Art. 36)
 - Bill: but ‘may’
 - Record of processing activities (Art. 30)
 - Bill: only for ‘high risk processing’
 - Breach notification (Art. 33): ‘non material risk’ **X**

Compliance issues

- Over-reliance on seeking consent from individuals
 - Unnecessary burden for consumers ('consent-fatigue') and controllers
 - Uncertainty over 'legitimate interests' (Art. 6(1)(f)), especially documenting the balancing exercise
 - C-621/22, *Koninklijke Nederlandse Lawn Tennisbond v Autoriteit Persoonsgegevens*
 - Bill: 'recognised legitimate interest' detailed in Annex 1, e.g. 'democratic engagement'
 - E.g. Singapore: Personal Data Protection Act 2012, First Schedule, Part 3
- Anonymisation
 - Recital 26 & Convention 108+ Explanatory Memorandum: as statutory tests
 - Relative to the means available to the controller to re-identify
 - C-582/14 *Breyer v Bundesrepublik Deutschland* 19 October 2016)
 - T-557/20 *Single Resolution Board v EDPS* (26 April 2023): on appeal
 - Bill: 'Information relating to an identifiable living individual'

Compliance issues

- Data sharing & re-use
 - ‘Open Banking’
 - PSD2 (Directive 2015/2366)
 - Broad consent for research purposes
 - Further processing
 - Art. 5(1)(b) and 6(4): incompatible and compatible purposes
 - Recital 50: public interest tasks specified in law
 - Reasonable expectations
 - Bill: omit Art. 6(4) and replace with 8A + Annex 2
- Subject access
 - Scope of provision and time period for responding
 - Bill: ‘a reasonable and proportionate search’ + ‘applicable time period’
 - Raise threshold from ‘manifestly unfounded’ (Art. 12(5))
 - Bill: ‘vexatious or excessive requests’

Compliance issues

- Cookie banners!
 - Analytics as ‘strictly necessary’ (e.g. France)
 - Bill: for statistical purposes ‘with a view to making improvement to the service/website’ *or* ‘to adapt to the preferences of the subscriber or user’ *or* to enhance appearance or functionality *or* enable software & security updates *or* in emergencies
 - Transparency + opt-out possibility
 - Regulations to permit consent to be given automatically
- Unsolicited emails
 - Charitable, political or non-commercial purposes
 - Further to an expression of interest
 - ‘Democratic engagement’
 - ‘..an electoral system or other democratic process in the United Kingdom..’
 - Service provider duty to notify of any reasonable grounds for suspected contraventions
 - Fine for non-compliance

Data protection & AI

- Policy responses to AI
 - EU AI Act
- Separating the research and development (training and testing) phase from the deployment phase
 - Processing, especially sensitive personal data, to monitor outcomes and identify and mitigate bias
 - Data protection laws as a barrier to processing demographic data
 - Processing to monitor, detect and correct bias as a ‘legitimate interest’
- ‘Fair’ processing
 - Unjust (outcomes), unexpected (transparency) and procedural (decision-making) fairness
 - Bill: Compulsory transparency reporting on the use of algorithms in public sector decision-making
- Article 22 & profiling
 - Uncertainties around ‘solely’ + ‘significant effects’
 - Bill: insert Arts. 22A, B, C & D - ‘no meaningful human involvement’

As a regulatory regime

- Risk-based & outcomes-led
 - “The UK was successful in negotiating a more risk-based approach to the GDPR, allowing for greater flexibility in relation to the regulation’s mandatory requirements” *Matt Hancock, Dec. 2016*
- Internal governance
 - Bill: omit Art. 27 - ‘representatives of controllers & processors outside the UK
 - From DPOs to ‘senior responsible individual’ (Art. 37-39)
 - Voluntary undertakings **X**
- External governance
 - Art. 57: ‘a long list of tasks and functions....without a strategic framework..’
 - Principal objective: “to secure an appropriate level of protection for personal data, having regard to the interests of data subjects, controllers and others and matters of public interest”
 - From Information Commissioner to Information Commission (‘ICO’)
 - Independence, accountability and transparency concerns

Transborder data flows

- Trade agreements
 - JSI negotiations on data flows, data localization & data sovereignty
- Adequacy assessments
 - Risk & outcomes based: The likelihood and severity of actual risks to data subjects
 - Bill: ‘the data protection test’ - ‘not materially lower’
 - ‘only personal data likely to be subject of such transfers’
 - Review on an ongoing basis, not every 4 years
- Alternative transfer mechanisms
 - Proportionate, flexible and more interoperable
 - Bolster use of certification schemes **X**; Create-your-own (e.g. New Zealand) **X**
- Derogations
 - ‘Reverse transfer’ exemption **X**
- Redress mechanisms
 - Both judicial and/or administrative

Concluding remarks

- Radical or incremental
 - Room for manoeuvre
- Differential compliance
 - Parsing DP policies & procedures in a European market
- Risk-based regulation
 - Reconciling legal certainty
- Bridge between US and EU
 - Onward transfers & the ‘closed ecosystem’
- The politics and the optics.....