The lawyer’s perspective: A year in review and a look to the future

10 July 2019

charlesrussellspeechlys.com

Part 1: The year in review

The regulator's 'school report'

- 14,000 personal data breach reports (25 May 2018 – 1 May 2019) vs 3,300 personal data breach reports in the year from April 2017.
- 41,000 data protection concerns from the public (25 May 2018 – 1 May 2019) vs 21,000 for 2017/18.
- Data subject access requests are still the most frequent complaint category.
- ICO workforce growing rapidly (anticipated 825 employees in 2020/21)
- The ICO has primarily dealt with marketing and data breaches but now wants to focus on transparency, accountability and consent.

Enforcement action and case law

Facebook/Cambridge Analytica *(a statement of intent?)*

- Allowed application developers access to users personal data without sufficiently clear and informed consent.
- Maximum fine of £500,000 under DPA 1998 vs up to 4% of global turnover or 20m Euro (whichever is greater)

Various Claimants v Morrison Supermarkets Plc

- Group litigation on the back of a data breach – Morrisons vicariously liable for the rogue employee's actions

Big fine 1: British Airways

- Cyber incident due to poor security arrangements at the company
- £183.39m

Big fine 2: Marriott

- Cyber incident affecting 339 million guests
- £99m

How about the question of insurance coverage?

- **Right to compensation and liability**
  - *"The fact of a defendant being insured is not a reason for imposing liability, but the availability of insurance is a valid answer to the Doomsday or Armageddon arguments…"*

    Various Claimants v Morrison Supermarkets Plc, CA judgment, [2018] EWCA Civ 2339
  - Morrisons should have been insured!

- **Are GDPR monetary penalty notices (i.e. ICO administrative fines) insurable?**
  - Nothing in the GDPR expressly permits or excludes.
  - Q for local law and not entirely clear: public policy likely excludes fines for criminal, intentional or reckless wrong-doing.

"A focus on insurance rather misses the point, and organisations should be looking to recognise the benefits of good information rights practices to their efficiency, reputation, and competitive edge."

ICO

Part 2: Future gazing – what next?

Take your pick – we're moving quickly!

- Brexit
- Certification Schemes
- E-Privacy Regulation
- ICO's new focus on accountability
- International developments
- Legal challenges to Model Clauses and Privacy Shield
- Rise of compensation claims (Conditional Fee Agreement, anyone?)
- Technological developments: AI / IoT
- UK Government 'Online harm' white paper

Data protection by design and by default

- Integrate safeguards into your processing to meet the requirements of the GDPR (*GDPR, Art 25).*

  =

- Putting in place practical measures in a organised, structured way.

- What does that mean for your organisation: Resources, roles, records, training and awareness, monitoring etc.

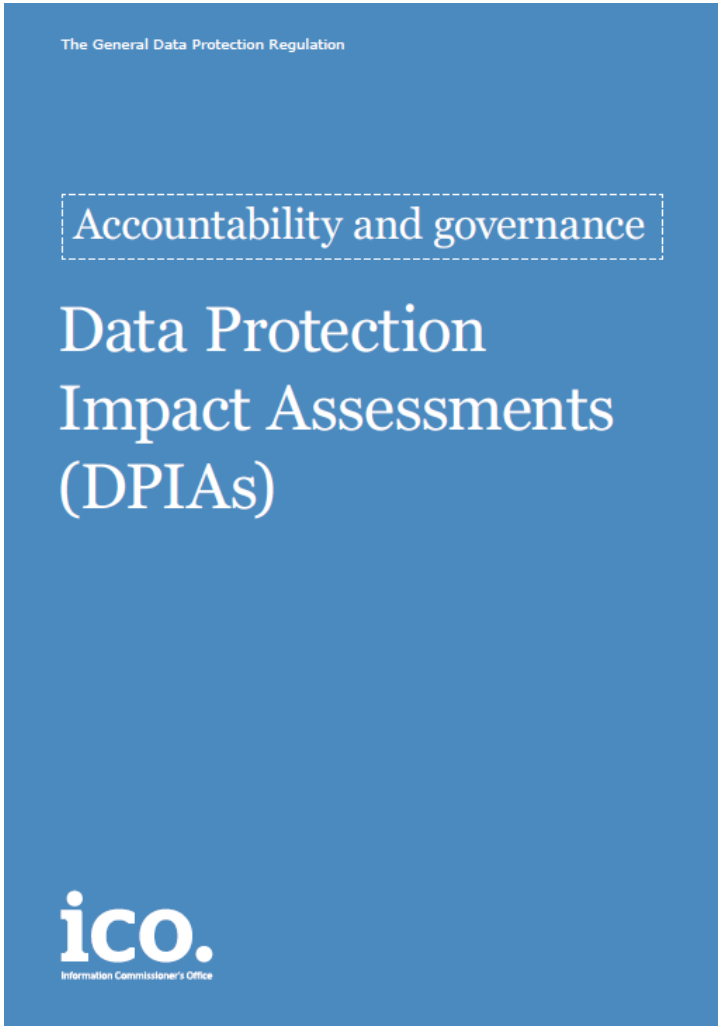
- Should be seen as not just a ‘compliance headache’: competitive advantage, investment to mitigate the risk of problems (including data breaches and an inability to respond to individuals exercising their rights).

Data Protection Impact Assessments

- Process to help identify the and minimise the DP risks of a project

- Should comprise the following:

  - a systematic description of the envisaged processing operations
  - an assessment of the necessity and proportionality
  - an assessment of the risks to the rights and freedoms of data subjects
  - the measures envisaged to address the risks.



Part 3: A commercial case study: Employee processing

Shiny Computers Inc. – an introduction

- Shiny Computers Inc. is a US headquartered multi-national with a UK subsidiary that provides an IT software platform for its customers.
- It has a privacy compliance programme. However, its UK data protection officer left the business two months ago.
- A recent efficiency drive is prompting a review of its employment practices and it is considering adopting the following in its UK offices:
  - Acme Corp. Employee Monitor. A software product that monitors employee internet and email usage; computer activities; telephone use; and GPS tracking of their mobile phones.
  - Acme Corp. Energy Monitor. A hardware and software product that monitors the use of energy in the office environment.

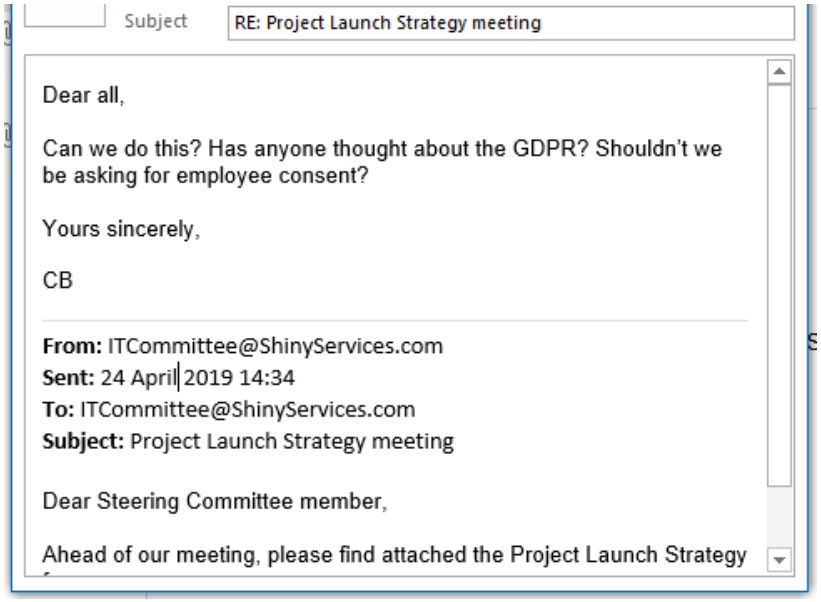
Initial considerations

Acme Corp. Employee Monitor

and

Acme Corp. Energy Monitor

Project Launch Strategy



POINTS TO CONSIDER

- Can individuals 'issue spot'?
  - Is design/default at that level?
  - Is general/specific training and awareness provided?
- Is CB right?
  - Is the GDPR relevant?
  - Is employee consent relevant?
- 'Would a DPIA be useful and/or is it mandatory?

Undertaking the DPIA

Shiny Computers

Data Protection Impact Assessment (DPIA) ~~Template Policy~~ undertaken for Acme Corp. Employee Monitor

Last revised: ~~24 May 2018~~ 28 April 2019

Section 1: Screening Questions – Likely to result in a high risk

…

[x] Tracking an individual's geolocation or behaviour

[x] Data concerning vulnerable data subjects

…

We [will / will not] undertake a DPIA because…

POINTS TO CONSIDER

- What is the procedure?
- Who will do the DPIA?
  - Should the processor assist?
  - Internal v. external support?
  - Has one been completed already?
- What is the timeframe?

Undertaking the DPIA

Section 2: Describe the processing

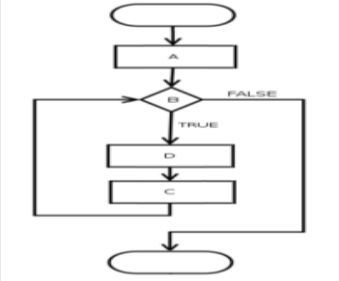
Nature of the processing:

Acme. Employee Monitor will allow Shiny to monitor employee desktop application usage. The collected data will detail which applications were used during which periods and can be presented as a daily, weekly or monthly report. Employees may be profiled as productive, non-productive, absent…

Scope of the processing:

[…]

Data flow diagram:



Section 3: Necessity & proportionality

[…]

POINTS TO CONSIDER

- Providing an accurate description of the processing is core to the DPIA process
- Describe:
  - Nature of the processing
  - Scope of the processing
  - Context of the processing
  - Purposes of the processing
- Consider:
  - Types of personal data
  - Categories of data subject
  - Source of the data
  - Length and frequency of processing
  - Volumes

Undertaking the DPIA

POINTS TO CONSIDER

- Identify risk scenarios:
  - Brain-storm / past experience
  - Precedents / templates
  - Group discussions
  - Consultations
- Analyse and assess the risks
  - Likelihood x severity

Undertaking the DPIA

Section 5: Measures to address the risk

No	Risk description	Likelihood	Severity	Rating	Solutions / mitigations	Notes / next steps
1.	Location data may be used incorrectly and/or maliciously by staff who have access to the data.	3	3		Policy document outlining access controls and expectations of those receiving the data. Appropriate training given to line managers.	FL responsible for drafting policy document….
2.	Legitimate challenge to lawful basis for processing by a disgruntled employee.	2	4		Robust assessment of legitimate interests; publish as part of policy document.	JM responsible

Section 6: Sign-off and record outcomes

Item	Name/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		

POINTS TO CONSIDER

- Determine the measures to address the risks
  - Manage / mitigate?
  - Eliminate?
- Reduce the severity or reduce the impact?
- Sign-off
  - Advice of the DPO
  - Consultation with the Supervisory Authority?
- Report and publish
- Review