Compass Chambers

GDPR in PI Practice

Craig Murray

Advocate

Compass Chambers

GDPR on a Friday afternoon?

Compass Chambers

Some of this …

Compass Chambers

A mention of this …

Compass Chambers

To be swiftly followed by …

Compass Chambers

A hot topic?

Various Claimants v. Wm Morrison Supermarkets plc [2019] 2 WLR 99

- Breach of statutory duty under the DPA 1988 (direct liability)
- Breach of confidence (vicarious liability)
- Misuse of private information (vicarious liability)

Compass Chambers

Wm Morrison

D asked by external auditors to provide payroll data

Copy of data prepared and given to internal auditor, Mr Skelton

Skelton had previously been disciplined and bore a grudge against D

Skelton copied the data onto a personal USB

12.1.14 Skelton posted data on a file sharing website of 99,998 employees

Compass Chambers

Wm Morrison

Name

Address

Gender

DOB

Phone numbers

National Insurance

Bank Account numbers

Salary

Compass Chambers

Wm Morrison

- Before instructed, investigated TOR network
- When knew of instruction, obtained a burner
- Brought a USB stick to work
- Laid low
- Used a colleague's name and DOB for TOR acc
- After posting on internet, sent anonymous letters to 3 newspapers

Compass Chambers

Wm Morrison

5,518 employees sued D:

- Asserted D was directly liable as the 'data controller' at the time when the data was misused.

- Vicarious liability at common law (breach of confidence and misuse of private information).

Compass Chambers

Wm Morrison

- Judge dismissed claims of primary liability under DPA, holding that Skelton, not D, was the data controller.

- Judge allowed the claims based on vicarious liability.

Compass Chambers

Wm Morrison

D argued on appeal:

- Vicarious liability could not apply to breaches of DPA 1988
- DPA 1988 excluded the application of vicarious liability
- The wrongful acts of Skelton had not occurred in the course of his employment

Compass Chambers

Wm Morrison

Court of Appeal, on the D's appeal

Held: The DPA 1988 did not exclude, either expressly or by necessary implication, the bringing of a claim for breach of confidence or misuse of personal information that was based on the vicarious liability of an employer for breaches of the Act by an employee.

Compass Chambers

Wm Morrison

D had been successful on DPA points:

- Not foreseeable that Skelton not to be trusted
- Technological and organization measures could not fully protect against a rogue employee
- No practical way to detect search for TOR
- Any failure to monitor internet usage not causative
- D did not carelessly permit misuse of data by Skelton

Compass Chambers

Wm Morrison – vicarious liability

"[186] … he chose to disclose [the data] to others [who were] not authorized, but it was none the less closely related to what he was tasked to do."

"[184] … These actions were in my view all part of a plan, as the research and careful attempts to hide his tracks indicate. This was no sequence of random events, but an unbroken chain beginning even before, but including the first unlawful act of downloading data."

Compass Chambers

Wm Morrison – vicarious liability

D submitted that to impose vicarious liability would render the court an accessory in furthering Skelton's criminal aims.

- Motive is generally irrelevant (to vicarious liability)
- If correct, the victims of the data breach would only have a remedy against Skelton personally

Compass Chambers

Wm Morrison

- A case of statutory interpretation and vicarious liability.

- No challenge to dismissal of claims for breach of DPA 1988.

- Neither side challenged the finding that Skelton, not D, was the data controller when the data was wrongfully copied onto USB.

Compass Chambers

Wm Morrison – vicarious liability

"[78] There have been may instances reported in the media in recent years of data breaches on a massive scale caused either by corporate systems failures or negligence by individuals acting in the course of their employment. These might, depending on the facts, lead to a large number of claims against the relevant company for potentially ruinous amounts. The solution is to insure …"

Compass Chambers

Insurance for cyber breach

Perhaps not so straightforward?

- "One of the most significant issues with cyber insurance pricing and underwriting is the lack of robust data on cyber risk … Progress in delivering this access with the ICO has not been as swift as we would have liked."

James Dalton, DG Insurance Policy at ABI

13.5.19

Compass Chambers

GDPR

"Everyone has the right to the protection of personal data concerning him or her.

Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law"

Charter of Fundamental Rights of the EU, Art. 8

Compass Chambers

What does the GDPR apply to?

- Automated and partly automated processing of personal data
- Does not apply to ‘unstructured files’
- Files containing multiple categories of information
- Could a temp be able to extract specific information without having to manually trawl through all the records?

Compass Chambers

Definitions

- ‘Personal data’ includes name, location data and online identifiers by which a person may be identified.
- ‘Profiling’ is the automated collection of personal data to evaluate a natural person, including:
  a) Behaviour
  b) Location
  c) Movement

Compass Chambers

Examples

Surveillance footage is personal data:

- Must be selective (public accessible areas/ 3rd parties/ children)
- Transmitted securely
- Obtained by reputable surveillance agent

Compass Chambers

ABI Guidance on surveillance

- "A PI should only be employed where there is reasonable suspicion that the claim might be fraudulent or there are reasonable grounds for requiring validation of a claim and the information they can obtain using surveillance is deemed appropriate and necessary under the circumstances. When an insurer is considering whether or not to instruct a PI to investigate an individual, it should consider all other options first, such as using other sources of information available to the insurer and assess whether information gathering by the PI is strictly necessary."

2014

Compass Chambers

Social media

- Low cost, not intrusive, publicly available information.
- In line with ABI Guidance.
- Now very common.

Compass Chambers

Emerging issues: Trackers

Compass Chambers

Emerging issues: Drones

Compass Chambers

Definitions

- "Personal data breach": a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure or, or access to, personal data.
- "Data concerning health": broadly construed special category – past and future health, examination and test results, diagnoses of diseases, disabilities and medical history (recital 35)

Compass Chambers

GDPR: Core principles

- Personal data processed fairly and lawfully
- Collected for specified, explicit and legitimate purposes
- Not excessive data for the purposes
- Accurate and kept up to date
- Kept in a form which allows identification for no longer than necessary

Compass Chambers

Fair processing

- No definition of "fairness" in GDPR
- Legitimate interests of data controller is lawful justification where within the expectations of the data subject.
- Does not apply where data subject is a child.
- Processing is unfair if it is "sneaky, creepy or dishonest".
- Where strictly necessary for the prevention of fraud.

Compass Chambers

“Blagging calls”

June 2017, Joseph Walker, a former claims company manager, pleaded guilty to 12 offences of obtaining personal data.

- Unlawfully obtained data from car hire companies, used as leads
- Called insurance companies to illegally obtain information about policyholders and RTAs
- Similar tactics used for car repair centres

Compass Chambers

How long is necessary?

- Case-by-case basis: depending on the legal or business reasons for retention of data.
- Will rarely be justifiable to hold personal data in a form that permits identification of individual for an unlimited period.
- LawScot recommend a Data retention policy.
- Anonymisation of house styles.

Compass Chambers

Integrity and confidentiality

IT measures:

Encryption; password protection; firewalls; and antivirus software

Organisational measures:

Pass/ key control to office; clear desk policy; 'need to know' access to data; employee vetting; training and monitoring.

Compass Chambers

Special categories

- General prohibition on processing data concerning health, sex life or sexual orientation.
- Does not apply where necessary “for establishing, exercising or defending legal claims”.
- Transfer of personal data permissible on same grounds.
- Criminal convictions not a special category, but some protections.

Compass Chambers

Medical records

Compass Chambers

Objecting to processing

- Data subject can object to types of processing
- On receipt of objection, must cease processing unless it is necessary for establishing, exercising or defending legal claims (Art 21(1))
- Court has a "wide and untrammeled" discretion in whether to grant a subject access request (*R v. SSHD ex p Lord* [2003] EWHC 2073 (Admin), per Mumby J)

Compass Chambers

Durant v. Financial Services Authority [2003] EWCA Civ 1747

- Long-running dispute with Barclays Bank
- Request for data recovered large volume of material
- The purpose was to enable the subject to check whether the processing of data unlawfully infringed his privacy and, if so, to take such steps as the Act provided to protect it. It was not an automatic key to any information, readily accessible or not, of matters in which he might be named or involved. (para.[27])

Compass Chambers

Access request and privilege

Legal professional privilege/ litigation privilege means that in certain circumstances:

- There is no requirement to provide fair processing information to other individuals involved in the matter.

- In each case, you should consider whether the provision of such information would prejudice your advice or your client's interests.

LawScot advice

Compass Chambers

Mandatory breach notification

- Major innovation.
- Includes: lost laptop or mobile phone; hacking attack; sensitive letter to wrong address; “cc all” instead of “bcc”
- Must inform ICO without undue delay (in any event within 72 hours) and if a high risk breach, the data subject.

Compass Chambers

Remedies

- Data controller may refuse to erase data in response to a request, in respect of future legal claims.

- Broad right to damages for breach.

- Damages in respect of material damage or non-material damage (including distress or embarrassment).

Compass Chambers

The new PPI?

- On 24 October 2018, Cathay Pacific announced a data breach of personal data of 9.4m customers.
- Names, DOB, addresses, credit card numbers, passport details, historical travel data.
- SPG Law set up a website to attract clients to a group action.