


Liability Insurance Discussion Group





Shaping the future of insurance law

GDPR - privacy breach notification in practice

11 June 2019

PRESENTED BY

Mark Anderson, Partner

wotton
kearney+


A founding member of **LEGALIGN™**
GLOBAL

GDPR: jurisdiction and application

Also applies to controllers or processors not established in the EU where processing relates to:

(a) Offering of goods or services to data subjects in the EU

(b) Monitoring the behaviours of data subjects in the EU



Applies to controllers or processors established in the EU

GDPR breach notification

Personal Data Breach

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

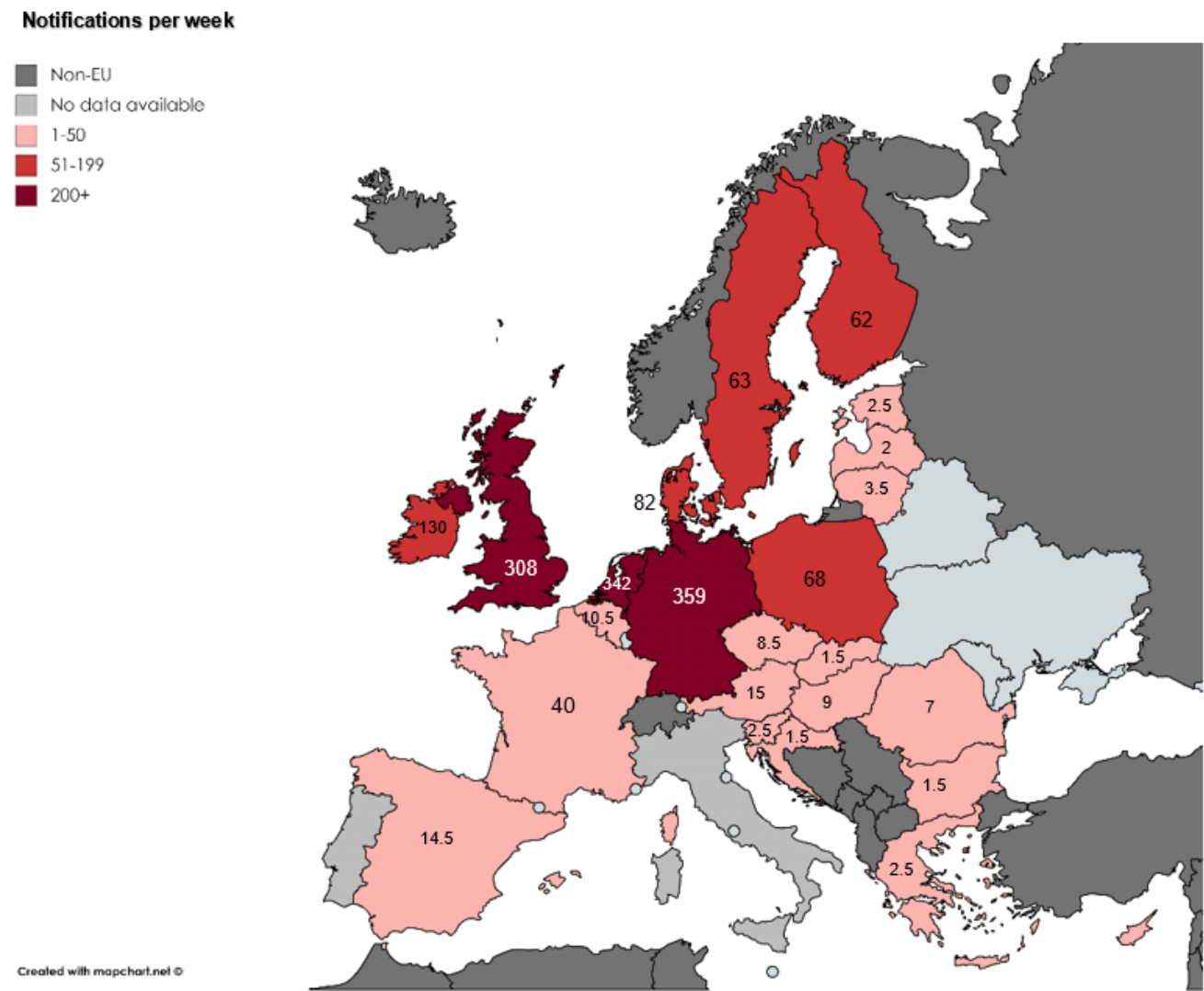
Notify ICO/DPA

- Unless the personal data breach is **unlikely** to result in **a risk** to the rights and freedoms of natural persons.
- Notification must be made within **72 hours** of the organisation becoming aware of it.

Notify Data Subjects

- All organisations must notify data subjects of breaches that are likely to result in **a high risk** to the rights and freedoms of individuals.
- Notification to individuals must be made **without undue delay**.

GDPR: breach notifications – by jurisdiction



GDPR fines

- Portugal: Barreiro hospital was fined EUR400,000 for three GDPR violations.
- Austria: EUR4,800 was issued by the Austrian regulator in relation to the use of CCTV
- France: CNIL fined Google EUR50m
- Germany (over 60 fines)

GDPR - liability beyond fines – civil litigation

https://www.badatabreach.com

☆

☰


SPG

LAW

BA DATA BREACH
COMPENSATION


— SPG —

SEE IF YOU CAN CLAIM



DATA SECURITY

Tackle a large company for inadequately ensuring data security.



FINANCIAL GAIN

If eligible, you could receive up to £1500.

Hayes

Connor

SOLICITORS

DATA BREACH CLAIMS, TICKETMASTER DATA BREACH

HOW MUCH
COMPENSATION COULD
YOU RECEIVE
FOLLOWING THE
TICKETMASTER DATA
HACK?

TICKETMASTER
COMPENSATION

How much you might win if you had your financial details stolen and they were used fraudulently	£5,000
How much you might win if you had your financial details stolen	£3,000
How much you might win if you had your email address stolen	£1,500
How much you might win if you had other personal information stolen	£500-1,000

Emma's Diary Data Breach

Earlier this month, parenting website Emma's Diary was fined £140,000 for selling data collected from its app to the Labour Party.

Using a database created by Experian, Labour used this personal information to target new mothers with direct marketing. The data gathered included parent names, addresses and the dates of birth of the mother and children.

By now those who have been affected should have been emailed. If you have received this email then you may be able to claim compensation once the matter has been fully investigated.

To ensure that you are fully informed on this matter complete your details and we will notify you about the investigation and your legal rights when making a claim.

Litigation: UK cases - the broadening application of privacy law

Causes of action

- Duty of Confidentiality
- Art 8 ECHR
- Tort of Misuse of Private Information
- Material (financial) and non material damage (distress) for DPA '18 / GDPR breach

Campbell v MGN Ltd [2004]: (£2,500 general, £1,000 aggravated)

Halliday v Creation Consumer Finance [2013]: £750 (compensation)

AB v MoJ [2014]: £1 (nominal) £2,250 (distress).

Vidal-Hall v Google [2015]: Claimants entitle to sue for compensation for misuse of private information despite no direct financial loss.

Litigation: UK cases cont'd

Gulati v MGN [2015]: individual privacy awards up to £260,000. Claimants entitled to sue for mere “loss of autonomy” over personal information plus aggravated damages.

TLT v Home Office [2016]: Six awards between £2,500 to £12,500, including those not named on the spreadsheet. Quantum based on psychological injury awards. Subsequent appeal confirmed unnamed parties entitled to claim.

Cliff Richard v (i) BBC (ii) South Yorks Police [2018]. £190k general, £40k aggravated damages. Privacy and DPA claims are essentially the same. Damage to reputation allowed.

WM Morrisons v Various Claimants v [2018]: Vicarious liability for employee’s malicious data breach. Costs award penalised claimants pursuing unmeritorious causes of action.

Litigation: what do claims look like?

Individual claims

- Determining which jurisdiction
- The alleged unlawful act
- Cause of action: Confidence, Misuse of Private information, GDPR, ECHR
- Distress
- Psychological injury (medical evidence)
- Quantum (difficult to determine)
- Costs, CFA

Group claims

- All of the above but harder settlement

What is keeping the GDPR regulator busy?

- 93% increase in enquiries made via the ICO helpline
- 94% increase in complaints overall
 - Complaints relating specifically to DSARs have increased by 98%
 - Complaints relating specifically to retention of personal data have increased by 81%
 - Of all complaints made, 31% have been upheld
- 8,000 breach notifications made in UK
- 1,000 one-stop shop referrals between supervisory authorities via an EU level portal
- By far, the most common complaint is in relation to DSARs, followed by wrongful disclosure; security issues; retention; and data inaccuracy.
- The ICO are starting to see a levelling off of complaint levels, but not a drop.
- First Enforcement Notice issued under GDPR was on an extra-territorial basis against Aggregate IQ (Canadian)

What is keeping the Wotton + Kearney team busy?

- Office 365 and Mimecast breaches
- Ransomware (Ryuk + Emotet/Trickbot, Seedlocker, Bit Paymer)
- Misdirected emails and post
- Litigation (individual nuisance claims and also group claims)
- Providing comfort that breaches do not need to be notified
- Determining jurisdiction, Controller/Processor status before breaches can be advised on.....

GDPR notification examples

MISDIRECTED EMAIL

- Email with medical records for one individual sent to the wrong doctor in an South East Asian country.
- ICO responded that it was not a notifiable breach

UNAUTHORISED ACCESS

- Questionnaire URL for 150,000 sent to the wrong people. First name and some personal but not sensitive information.
- Number of people expected to access data in questionnaire that was not meant for them anticipated to be low if not zero.
- ICO responded that it was not a notifiable breach.

GDPR notification examples – cont'd

UNENCRYPTED HARD DRIVES

- <100 hard drives stolen from a server room. Drives were unencrypted.
- Initial notification during 72-hour period due to lack of understanding as to access.
- IT expert later opined that access was less than 5%.
- ICO took no further action.

RANSOMWARE

- Design and engineering company suffered ransomware attack. No access to computers for 4 weeks.
- Employee data encrypted during this period but no impact (e.g payroll not interrupted).
- ICO not notified.

GDPR notification examples – cont'd

EMAIL COMPROMISE

- Hacker obtained access to email account, IMAP access meant external synchronisation of all email.
- 300 employees data exfiltrated. Name, IR information, driving licenses, health insurance information.
- ICO informed that data subjects to be notified. ICO took no further action.
- Data subjects notified.
- Compensation claim.

EMAIL COMPROMISE (2)

- Hacker gained access to 6 email accounts.
- Personal and financial details (employee bank accounts) potentially accessed.
- No evidence uncovered that personal data targeted. Intention was to target corporate invoice fraud.
- ICO asked 10 questions relating to security measures and policies.
- ICO later decided no further action required.

Contact us



Mark Anderson

Partner

T: +64 9 280 0524

E: mark.anderson@wottonkearney.com



Andrew Moore

Senior Associate

T: +64 9 280 1490

E: andrewr.moore@wottonkearney.com



New Zealand Offices

Auckland

Level 18, Crombie Lockwood Tower
191 Queen Street, Auckland 1010

T: +64 9 377 1854

Wellington

Level 13, Harbour Tower
2 Hunter Street, Wellington 6011

T: +64 4 499 5589

Australian Offices

Sydney

Level 26, 85 Castlereagh Street
Sydney NSW 2000

T: + 61 2 8273 9900

Melbourne

Level 15, 600 Bourke Street
Melbourne VIC 3000

T: +61 3 9604 7900

Brisbane

Level 23, 111 Eagle Street
Brisbane QLD 4000

T: +61 7 3236 8700

Perth

L1/Suite 1, Brookfield Place Tower 2 123
St Georges Tce Perth WA 6000

T: +61 8 9222 6900

Contact us



Sierra Ryland

Senior Associate

T: +64 4 974 9280

E: sierra.ryland@wottonkearney.com



Amelia Goodall

Solicitor

T: +64 4 909 7158

E: amelia.goodall@wottonkearney.com



Kieran Doyle

Special Counsel

T: +61 2 8273 9828

E: Kieran.doyle@wottonkearney.com.au



The background is an abstract composition. The left side features a solid blue area with a subtle, overlapping pattern of lighter blue, curved, leaf-like shapes. A large, curved white shape separates this from the right side. The right side is a black area with a prominent, three-dimensional, wavy pattern of overlapping, curved, leaf-like shapes that create a strong sense of depth and movement.

Q&A

Privacy Bill – update

LIDG June Session

11 June 2019

Jane Foster

General Counsel

Privacy Bill – key changes

- New information privacy principle (IPP12):
Disclosure of information outside of New Zealand
- Access directions
- Mandatory data breach notifications
- Compliance notices

IPP12



Principle 12 – requirements for disclosure to foreign person or entity:

- The individual authorises, after being expressly informed, that the foreign person or entity may not have comparable safeguards
- The foreign person or entity is carrying business in NZ and subject to the Act
- The agency believes the foreign person or entity is subject to law with comparable safeguards
- **Binding scheme** participant
- Subject to laws of a **prescribed country**
- Other belief, reasonably held that foreign person or entity is required to protect the information in a way that, overall, provides comparable safeguards (for example, pursuant to an agreement)

Access directions

- Commissioner can direct agency to provide access in any matter including:
 - confirming what is held
 - permits individual access
 - make available in a particular way
- Human Rights Review Tribunal can make enforcement order if don't comply with direction (and no appeal)
- Commissioner can at any time amend or cancel a direction.

Mandatory data breach notifications

- Notifiable privacy breach – a breach that “it is reasonable to believe has caused serious harm....or is likely to do so”
- Privacy breach in this context is broadly defined:
 - “unauthorised or accidental access to, or disclosure, alteration, loss, or destruction of” **OR**
 - “an action that prevents the agency from accessing the information on either a temporary or permanent basis”
- Whether or not was caused by person inside or outside the agency, or is attributable by the agency’s action or is ongoing.

If “notifiable privacy breach”

- Must notify as soon as practicable after becoming aware:
 - Commissioner, otherwise liable for offence (principals liable for agents)
 - affected individuals personally unless impractical then public notice
 - some exceptions apply to notification of individuals and timeframe for notification
- Failure to notify individuals can be interference with privacy
- Commissioner may publish identify of agencies that have notified of a privacy breach



Factors:

Any action taken by the agency to reduce the risk of harm following the breach;

Whether the personal information is sensitive in nature;

The nature of the harm that may be caused to affected individuals;

The person or body that has obtained or may obtain person information as a result of the breach (if known);

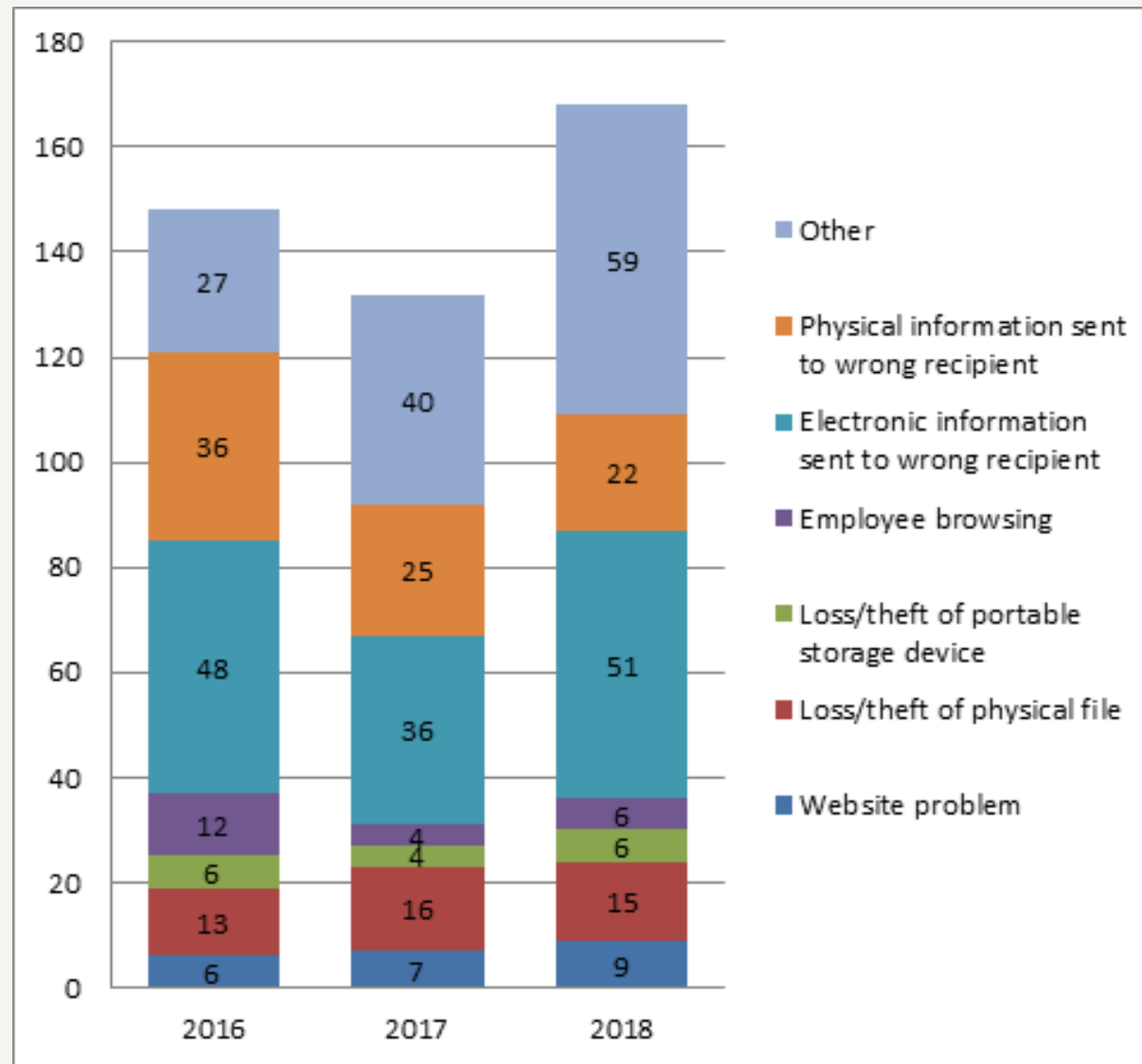
Whether the personal information is protected by a security measure;

Any other relevant matters.

Before the breach

1. **Assume you will have a breach** (despite everything you can do).
2. **Take steps to mitigate the risk** (e.g. - comply with NZISM etc, do the CERT Top Ten and check for the OWASP Top Ten, automatically get rid of information you do not have to keep.)
3. **Encrypt** (laptops, any data going out)
4. **Plan your response** (similar to your planning for a Computer Emergency Incident Response)
5. **Test your Plan!**

Common types of breaches



Not yet published

Who you gonna call?

Must:

- Internal governance reporting!
- Legal obligations to notify?
- Contractual obligations to notify?
- Professional obligations to notify?

Should:

- If personal information? – OPC if notifiable breach
- If cyber ? – CERT
- If personal information and too many affected people for you to handle ? – IDCare

Compliance notices

- Flexible enforcement tool
- Commissioner can issue for any potential interference with privacy, at any time, including concurrently with use of other means under the Act.
- Notice must describe the breach and require agency to remedy the breach, and agency must take steps to comply with the notice.
- Notice can be varied or cancel. Appeal right to Tribunal

OPC resources and tools

- Enquiries Line 0800 803 909
- Data breach guidance – Data Safety Toolkit
- Ask Us Knowledge base
- Privacy Trust Mark
- E-learning privacy modules
- OPC reports, case notes, media statements and blogs www.privacy.org.nz

