PHILIPLEE

RSM

WELCOME TO GDPR IN REVIEW

@PHILIPLEELAW @RSM_IRELAND

#GDPRINREVIEW

Agenda

- **8.00:** Eoghan Doyle, Partner, Philip Lee
- **8.05**: Sophie O' Connor – Associate, Philip Lee
- **8.15:** Terry McAdam – Management Consulting Partner, RSM Ireland
- **8.25**: Nicola Coogan – Head of International Transfers, DPC
- **8.40**: Panel discussion and Q & A

PHILIPLEE

GDPR IN REVIEW

Presented by Sophie O'Connor

10 APRIL 2019

Outline

- Takeaways from GDPR compliance programmes
- Case study: Google's €50 million fine

Takeaways from GDPR compliance programmes

- Identifying personal data - mapping is extremely important
- Controller or processor? Joint controllers? Separate controllers?
- Ownership of data protection matters: DPO or other

Takeaways from GDPR compliance programmes

- Simple ways to improve a company's compliance:
  - Training
  - Privacy statements
  - Data processing agreements
  - Employee facing privacy documents
  - General data protection policy

Takeaways from GDPR compliance programmes (continued)

- Importance of policies and procedures for dealing with data subject requests and data breaches
- Advancement in technologies bring problems and solutions:
  - Use of personal devices in work and personal use on company devices
  - Dealing with breaches: ability to remotely wipe devices and/or cut off access
  - Cloud storage: issues with data transfers

Case study: Google's €50million fine

- Fined imposed by CNIL – French supervisory authority
- Infringements:
  - Lack of transparency and lack of information
  - Invalid consent
    - Not specific
    - Option to personalise ads is "pre-ticked"
- Choice of lead supervisory authority

PHILIPLEE

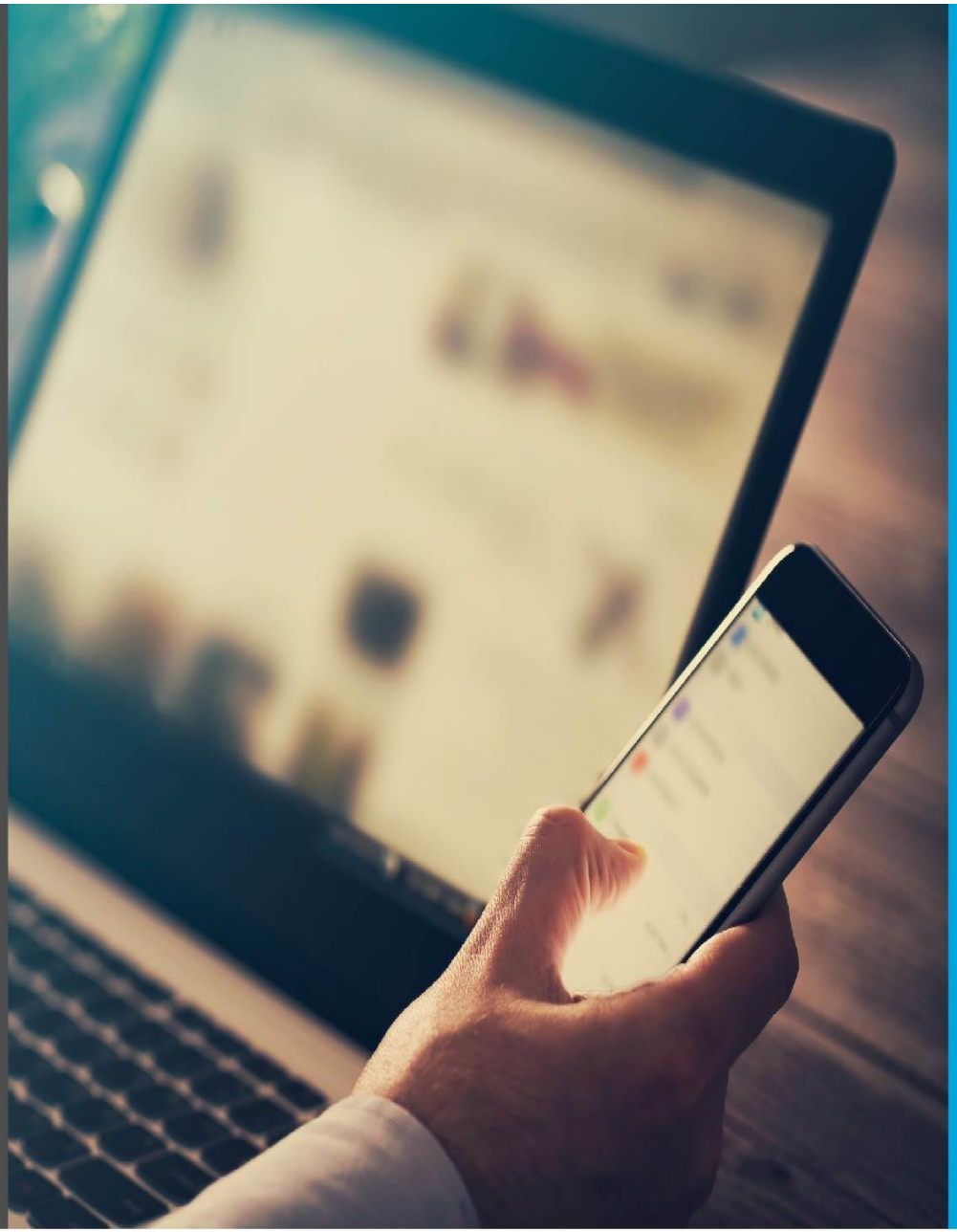
philiplee.ie
info@philiplee.ie

DUBLIN
7/8 Wilton Terrace
Dublin 2
Ireland
T: +353 (0)1 237 3700

BRUSSELS
EU Quarter, level 6 box 6,
Schuman Roundabout, 2-4,
1040 Brussels
T: +353 (0)1 237 3700

SAN FRANCISCO
388 Market Street, Suite
1300, San Francisco,
CA 94111
T: +1 415 839 6406

LONDON
2 Eastbourne Terrace,
London, W2 6LG
United Kingdom
T: +44 20 3934 7010



PHILIPLEE

GDPR
10 months on:
A view from the coalface

RSM

Your presenter

Terry McAdam

Management Consulting Partner, RSM Ireland

tmcadam@rsmireland.ie

Mobile: +353 (86) 0474002

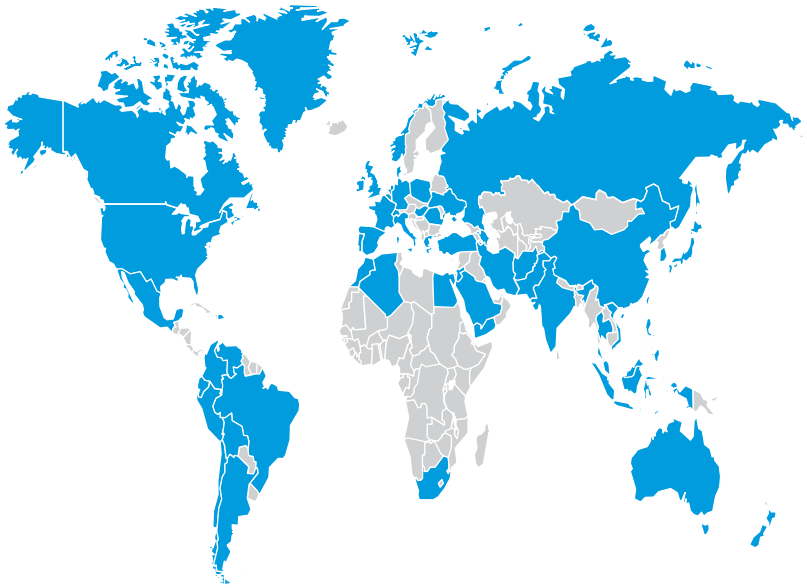
www.rsmireland.ie

RSM Ireland

Our firm's history goes back to **1987** and since then we have grown to become a top **8** professional services firms in Ireland specialising in providing advice to **mid-market businesses and government agencies.**

Our **150 people,** across all areas of the practice, provide clients with pragmatic, expert led, personalised advice and insight that helps them succeed, grow and prosper. Our firm is ideally placed to offer an unparalleled level of experience and expertise to our business partners in Ireland.

Network coverage map:



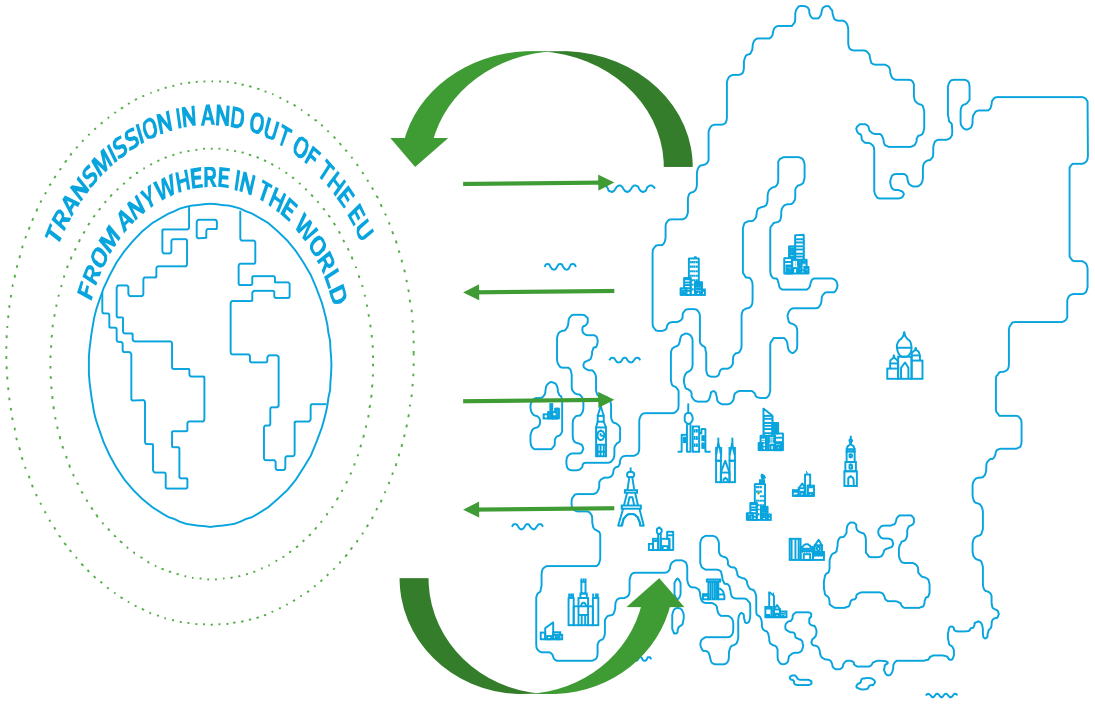
About RSM International:

RSM International is one of the fastest growing networks of audit, tax and consulting firms in the world –

- ✓ We are the **sixth largest** with combined revenues of **$5bn+;**
- ✓ Our member firms operate out of more than **800 offices**
- ✓ We are located in over **120 countries**; and
- ✓ We have over **43,000 staff worldwide**.

CLIENT CONCERNS POST GDPR

- Is our organisation compliant?
- What are our data compliance blind spots?
- Is our compliance approach robust? – breaches, data subject requests
- Is our DPO/data protection lead on top of their remit?
- Is our investment in compliance appropriate?
- Is the current regime adequately communicated to our team?



DATA PROTECTION HEALTH CHECK

- Developed in response to demand from clients for answers to questions on prior slide
- Re-assess client approach to data protection in light of the post GDPR experience
- Assignment, which can be tailored in scale based on client circumstances, focuses on:
    - the data compliance regime developed (policies, procedures and process) and how it aligns to data risk profile of the entity
    - how the organisation communicated its approach to its staff, customers and stakeholders
    - how the initial focus on data protection is embedded and sustained via audits of practice, ongoing training events for staff etc.

1. IMPORTANCE OF POLICIES

- Key bed rock of compliance is a quality set of policies which are communicated to staff. Four core policies are critical:
    - Data protection
    - Data retention
    - Data Subject requests
    - Data Breach Management
- Data retention policy and related Information Asset Register (IAR) are core elements of data protection regime
- Large numbers of queries re content of core policies and the operation of an IAR

2. MANAGEMENT OF DATA SUBJECT REQUESTS

- Recent annual report from DPC confirmed significant portion of complaints received revolve around management of Data Subject requests
- Beyond a strong policy, organisations need practical operational procedures which staff can follow to react to and address requests within the relevant timeline
- Training data champions across the your entity to lead the response to requests appears to bring the best results
- Champions need to work closely with the DPO/data protection lead and call for an extension of the timeline before deadline looms

3. COPING WITH POTENTIAL DATA BREACHES

- Second key source of Data Subject complaints to the DPC based on annual report
- organisations need clear and communicated procedures for how team members report a potential data breach and how it is investigated thereafter. An aggressive timeline needs to be complied with
- The DPO/data protection lead needs to be central to the process and communication to the DPC and Data Subjects, if required
- Must maintain a log of potential breaches and their outcome. Useful in terms of communicating risks and lessons learned to staff

4. GOVERNING YOUR DATA RELATIONSHIPS

- Whether you are a Data Controller, Data Processor or Joint Controllers, when you share personal data with another party you need an agreed document to govern the arrangement
- In practice, parties signing such Data Processing or Data Sharing Agreements in a timely fashion is proving challenging. Causes delays in their business activity
- Problem exacerbated when there is a mismatch in the scale of the entities – SME and large corporate
- Issues tend to centre on matters such as Data Controller insisting Data Processor accepts unlimited liability for costs which arise due to issues with the latter's data management

Thank you for your time and attention.

An Coimisiún um Chosaint Sonraí
Data Protection Commission

General Data Protection Regulation "10 months on"

Nicola Coogan
Head of International Transfers

Philip Lee and RSM Ireland Seminar

- First Post-GDPR Annual Report findings
- Statutory Inquiries - update
- Some 2019 Priorities
- Data Transfers to the UK after Brexit

Statistics

Statistic Type	Total since 25 May 2018
Complaints	**5,377**
GDPR applied	4,193
Old Acts	1,184
Breaches	**5,039**
GDPR Applied	4,548
Other Legislation	491
DPO Notifications	**1,110**
Cross-Border Statutory Inquiries	**16**
Non-Cross Border SI	**33**

Annual Report

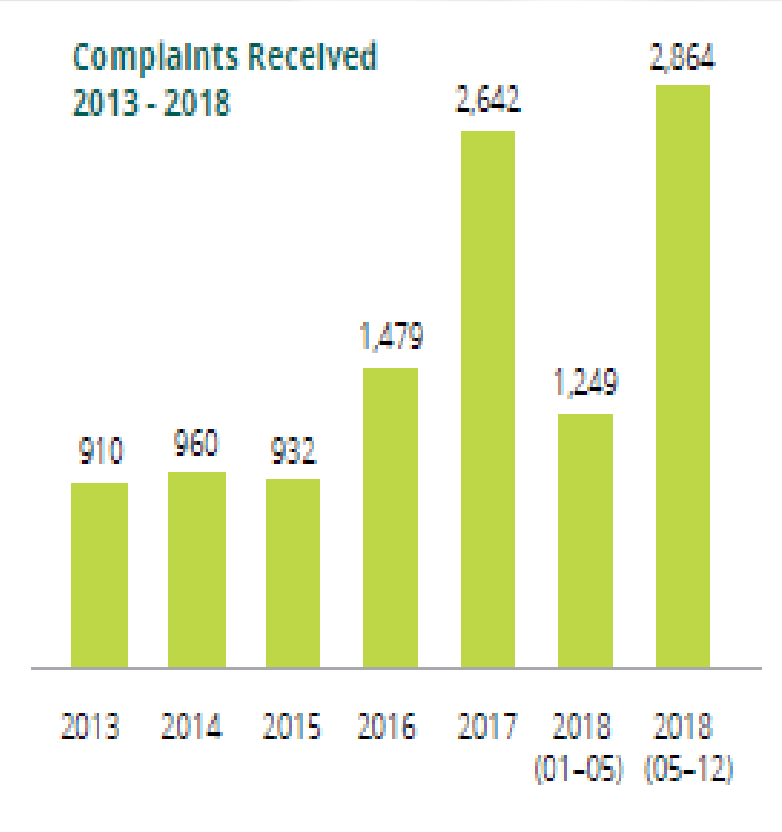
GDPR 2018 (25 May — 31 Dec 2018) — Breakdown by complaint type

	Percentages	Totals
Access Rights	30%	582
Multinational Complaints — Others	22%	396
Unfair Processing of Data	15%	285
Disclosure	11%	217
Electronic Direct Marketing	6%	111
Fair Obtaining	5%	100
Use of CCTV Footage	2%	35
Failure to secure data	2%	33
Internet Search Result Delisting	2%	31
Right of Rectification	2%	30
Retention	1%	28
Multinational Complaints — Access Rights	2%	25
Excessive Data	<1%	16
Accuracy	<1%	16
Unauthorised Access	<1%	9
Specified Purpose	<1%	6
Postal Direct Marketing	<1%	4
Biometrics	<1%	4
TOTALS	**100%**	**1,928**

Data Protection Acts 1988 and 2003 (25 May to 31 Dec 2018) — Breakdown by complaint type

	Percentages	Totals
Access Rights	39%	365
Unfair Processing of Data	19%	178
Disclosure	15%	138
Fair obtaining	8%	74
Electronic Direct Marketing	4%	36
Use of CCTV Footage	3%	29
Failure to secure data	2%	19
Retention	2%	15
Internet Search Result Delisting	2%	14
Excessive Data	2%	13
Specified Purpose	2%	12
Right of Rectification	1%	10
Accuracy	1%	9
Unauthorised Access	<1%	9
Multinational Complaints — Others	<1%	7
Multinational Complaints — Access Rights	<1%	5
Postal Direct Marketing	<1%	2
Biometrics	<1%	1
TOTALS	**100%**	**936**

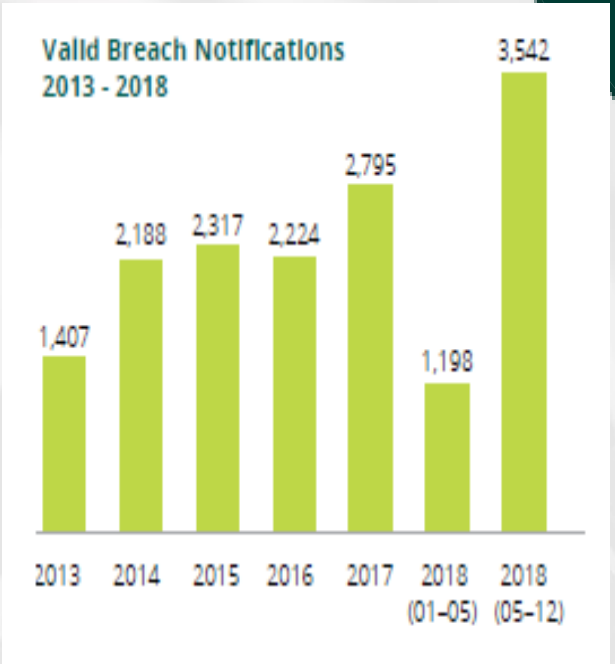
COMPLAINTS



Annual Report Summary

Data-breach notifications by category (2018)	Private	Public	Grand Total
Device lost or stolen (encrypted)	21	21	42
Device lost or stolen (unencrypted)	17	13	30
Disclosure (unauthorised)	2070	1064	3134
Hacking	102	14	116
Inappropriate disposal of paper	15	15	30
Malware	27	5	32
Paper lost or stolen	86	110	196
Phishing	91	16	107
Grand Total	**2429**	**1258**	**3687**

BREACHES



Unauthorised Disclosure: *Email/SMS to incorrect recipient; Letter/Correspondence to incorrect recipient; disclosure through customer online portal, processing error; verbal disclosure*

Cyber Incident: *Hacking; Phishing; Malware; Ransomware; Software Vulnerability*

Device Lost or Stolen: *Mobile Phone; Laptop, Portable Storage Devices*

Statutory Inquiries

DPC as the Lead Supervisory Authority

Cross-Border Statutory Inquiries
Facebook x 7
Whatsapp x 2
Instagram x 1
Twitter x 3
LinkedIn x 1
Apple x 2

Non Cross-Border Statutory Inquiries
Local Authorities/AGS x 31
Tusla x 1
DEASP x 1

Some 2019 Priorities

- Data transfers and Brexit
- Progressing Inquiries – first decisions Summer 2019
- Supervising and engaging with big-tech (multi-faceted)
- Children's Consultation
- DPC DPO Network

Data transfers and Brexit

- Under EU Law free movement of personal data is guaranteed between EU member states (GDPR rules apply).
- Transfers to recipients outside the EEA are considered to be a transfer to a “third country” and require additional safeguards to be put in place.
- In the event of a ‘no deal’ Brexit the UK will become a “third country” for the purposes of EU personal data transfers.

Data transfers and Brexit

- This will have repercussions for all organisations and bodies doing any kind of business with entities in the UK, including Northern Ireland, if the transfer of personal data is involved.

- This is because personal data transfers to the UK will require the implementation of legal safeguards by the Irish-based organisations and bodies that are transferring the personal data.

Data transfers and Brexit

- Example of safeguards are Standard Contractual Clauses, Ad-hoc Contractual Clauses, Binding Corporate Rules (BCR), Code of Conduct, Certification Mechanism

- Adequacy decision – where the commission decides that the UK ensures adequate levels of protection when data is transferred there and therefore separate safeguards will not be required- will not be forthcoming in the immediate term

Data transfers and Brexit

- **What should businesses be doing next?**

- Check your data flows to see if personal data is transferring to the UK (including Northern Ireland) and it if will continue post-withdrawal of the UK from the EU
- Put in place a safeguard to legally transfer the data
- Notify customers/employees/suppliers that their data is being transferred to a third country (Privacy policy/privacy statements should be updated)

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Thank You