MASON HAYES & CURRAN

# In-House Counsel Masterclass
# Data Protection & NIS Regulations

Thursday 10 January 2019

***@mhclawyers***

***#mhcgdpr***

MASON HAYES & CURRAN

# Welcome

Declan Black, Managing Partner

MASON HAYES & CURRAN

# Our Experts

- **Philip Nolan**
- **Oisín Tobin**
- **Áine Cadogan**
- **Melanie Crowley**
- **Robert McDonagh**

MASON HAYES & CURRAN

# GDPR: The story so far

Philip Nolan, Partner & Head of Privacy and Data Security
Oisín Tobin, Partner & Head of San Francisco Office

MASON HAYES & CURRAN

# Overview

- Legal sources
- Contracts
- Security breach notification
- Data Protection Impact Assessments
- Data Protection Officers
- Enforcement

MASON HAYES & CURRAN

## *How do I research a GDPR issue?*

MASON HAYES & CURRAN

# *What's happening with data protection contracts?*

MASON HAYES & CURRAN

***Must I notify all data breaches to the DPC?***

MASON HAYES & CURRAN

# *How should organisations approach Data Protection Impact Assessments?*

MASON HAYES & CURRAN

***How should my organisation deal with the requirement for a Data Protection Officer?***

MASON HAYES & CURRAN

## *What is the enforcement climate like at present?*

MASON HAYES & CURRAN

# Dealing with Subject Access Requests

Melanie Crowley, Partner & Head of Employment Law

Áine Cadogan, Senior Associate, Privacy & Data Security

MASON HAYES & CURRAN

# The Network and Information Systems Regulations

Robert McDonagh, Partner, Privacy & Data Security

MASON HAYES & CURRAN

# The context

- NIS Directive
  - boost EU cybersecurity
  - national strategy for each MS
  - sharing information across MS
- EU Implementing Regulation 2018/151
- EU (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018

MASON HAYES & CURRAN

# Relevant bodies

- Competent authority: DCCAE and CBI
- Computer Security Incident Response Team ('**CSIRT**')
- Single point of contact: DCCAE

MASON HAYES & CURRAN

# Who is subject to NIS?

- Operators of essential services ('**OES**')
- Relevant digital service providers ('**RDSP**')
- Light touch ex post reactive supervision for RDSPs

MASON HAYES & CURRAN

# What is an OES?

- Established in Ireland
- Service essential for maintenance of critical societal or economic activities
- Fall within scheduled sector and type
- Service depends on NIS
- Incident would have significant disruptive effects
- Can be OES in other Member States
- Businesses informed if classified as OES

MASON HAYES & CURRAN

# Relevant sectors covered

- Energy: electricity, oil and gas
- Transport: air, rail, water and road
- Banking
- Financial market infrastructures
- Health sector
- Drinking water supply and distribution
- Digital infrastructure: IXPs, DNS and TLDs

MASON HAYES & CURRAN

# What is a RDSP?

- 3 criteria:
  1. must be either:
     - online marketplace;
     - online search engine; or
     - cloud computing service
  2. main establishment (e.g. head office) or designated representative in Ireland
  3. not a micro or small enterprise
- Regulated in other MS if main establishment outside Ireland
- Designate representative if no EU establishment

MASON HAYES & CURRAN

# What is a RDSP?

- Self-determination (unlike with OES)
- Telecom and trust services out of scope

MASON HAYES & CURRAN

# What is an online marketplace?

- B2B and B2C online marketplaces for conclusion of contract
- Includes app stores
- Excluded:
  - intermediaries, e.g. comparison sites and ad sites
  - sites selling own products/services

MASON HAYES & CURRAN

# What is an online search engine?

- Performs searches of, in principle, all websites
- Excluded:
  - search functions limited to a specific website
  - comparison sites

MASON HAYES & CURRAN

# What is a cloud computing service?

- Service enabling *"access to a scalable and elastic pool of shareable computing resources"*

MASON HAYES & CURRAN

# What is a micro / small enterprise?

- Small enterprise: < 50 personnel and turnover and/or annual balance ≤ €10 million
- Micro enterprise: < 10 personnel and turnover and/or balance sheet total ≤ €2 million

MASON HAYES & CURRAN

# Security

- Risk:
  - appropriate and proportionate technical and organisational measures to manage risks, with regard to state of art
  - RDSP: regard to additional criteria (e.g. international standards, incident handling, continuity, auditing etc)
- Impact:
  - appropriate measures to prevent and minimise impact of incidents on service continuity
- Does not apply to banking / financial market infrastructure
- EU Implementing Regulation 2018/151 and guidance
- RDSP: documentation to enable verification

MASON HAYES & CURRAN

# What are notification requirements?

- Incident must:
  - have actual adverse effect on security of NIS
  - concern RDSP or concern OES or DSP relied upon by OES for essential service
  - have a “significant impact” on service continuity (OES) / “substantial impact” on service provision (RDSP)
- Voluntary notification

MASON HAYES & CURRAN

# Incident notification criteria

- "Significant impact" (OES):
  - number of users affected
  - duration
  - geographical spread
- "Substantial impact" (RDSP): 2 additional factors:
  - extent of disruption
  - extent of impact on economic and societal activities
- RDSP: must be in a position to estimate specific criteria

MASON HAYES & CURRAN

# Incident notification thresholds

- OES: thresholds currently being defined
- RDSP: notify if one of following applies:
  - service unavailable for more than 5m user hours
  - risk to public safety, security or loss of life
  - material damage to a user exceeding €1m
  - resulted in loss of integrity, authenticity or confidentiality of stored, transmitted or processed data or related services offered by, or accessible via, NIS affecting more than 100,000 EU users
- Non-exhaustive thresholds

MASON HAYES & CURRAN

# Timelines

- Notify CSIRT:
  - without delay and no later than 72 hours after aware
  - RDSP: n/a if don't have access to info
- Notify CSIRT when resolved:
  - as soon as practicable and no later than 72 hours after resolved
- Notification should not increase liability: NIS Directive
- Failure to notify is an offence

MASON HAYES & CURRAN

# Competent authority: DCCAE

- Can:
  - carry out compliance assessment (e.g., audit)
  - request information
  - issue information notice
  - appoint authorised officers (warrant)
  - co-operate and share information with DPC / Gardai
- Authorised officers broad powers including:
  - declaration of truth
  - compliance notice
- Does not apply to banking / financial market infrastructure sectors

MASON HAYES & CURRAN

# CSIRT

- Will, where possible, provide info to assist with incident
- Can inform the public about the incident if:
  - necessary to deal with it
  - necessary to prevent same or similar incident with other OES/RDSP
  - otherwise in the public interest (RDSPs only)
- Will forward notification, if appropriate, to SPOC in other Member State

MASON HAYES & CURRAN

# Action points

- Determine if subject to NIS
- Check security meets requirements
- Maintain documentation
- Update security incident response plan and processes

MASON HAYES & CURRAN

# Thank You

Questions?


**Philip Nolan**
pnolan@mhc.ie
+353 1 614 5078



**Oisín Tobin**
otobin@mhc.ie
+1 415 655 6841



**Melanie Crowley**
mcrowley@mhc.ie
+353 1 614 5230



**Áine Cadogan**
acadogan@mhc.ie
+353 1 614 7728



**Robert McDonagh**
rmcdonagh@mhc.ie
+353 1 614 5077