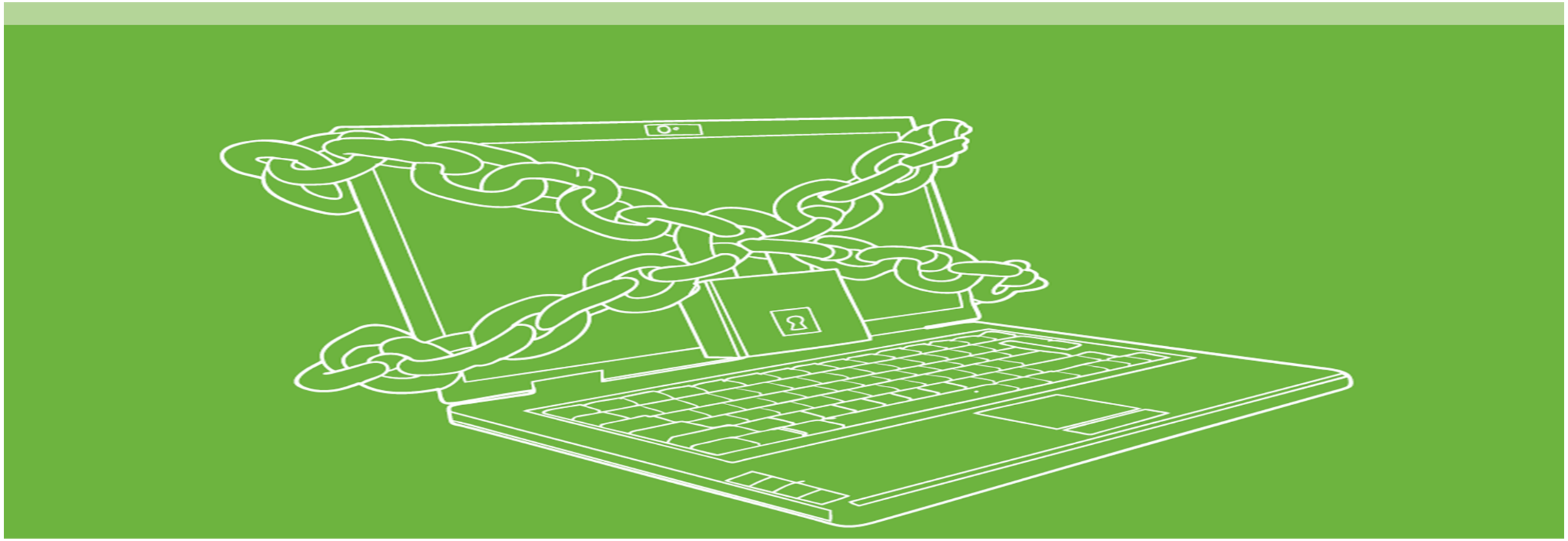
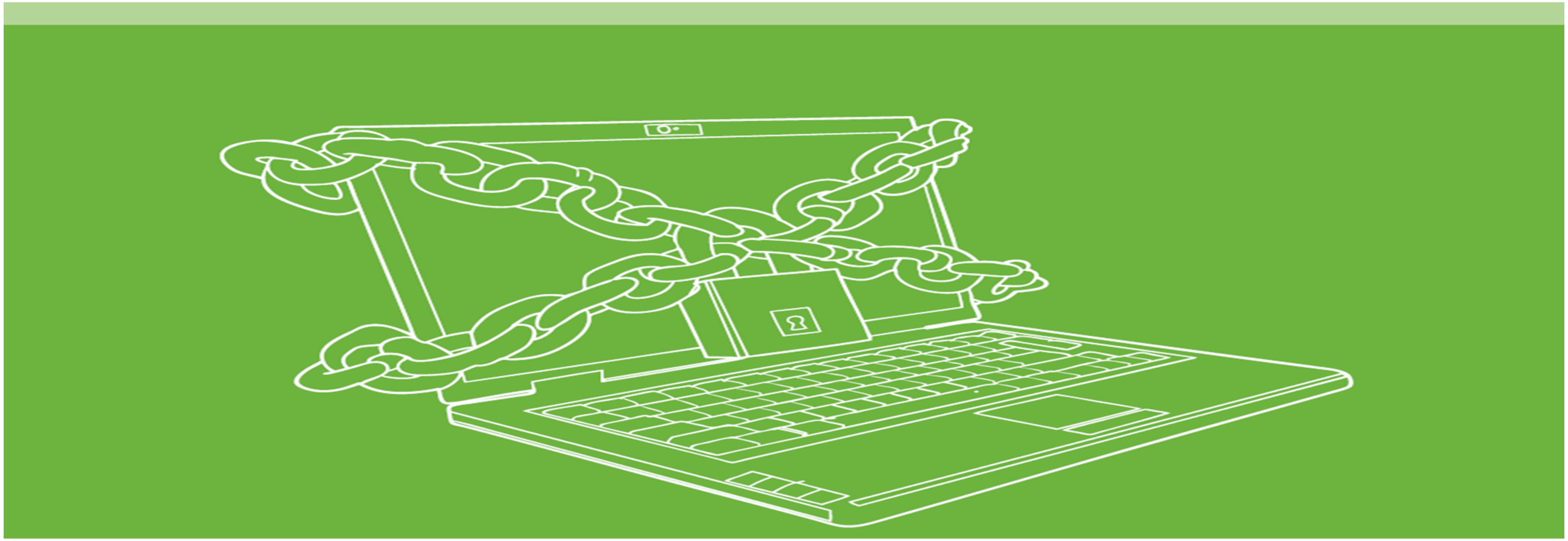
MASON
HAYES &
CURRAN

Cyber Security for Directors
Tuesday, 24 February 2015



Welcome

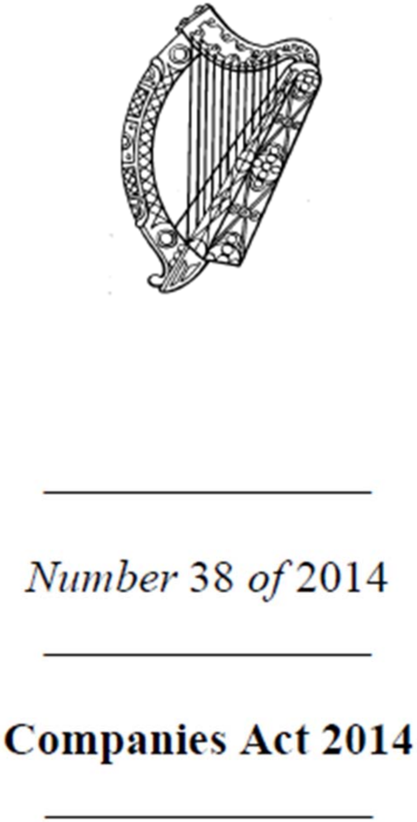
Paul Egan
Partner & Chairperson, Corporate
Mason Hayes & Curran
pegan@mhc.ie



MASON
HAYES &
CURRAN

Legal Background

Legal Background

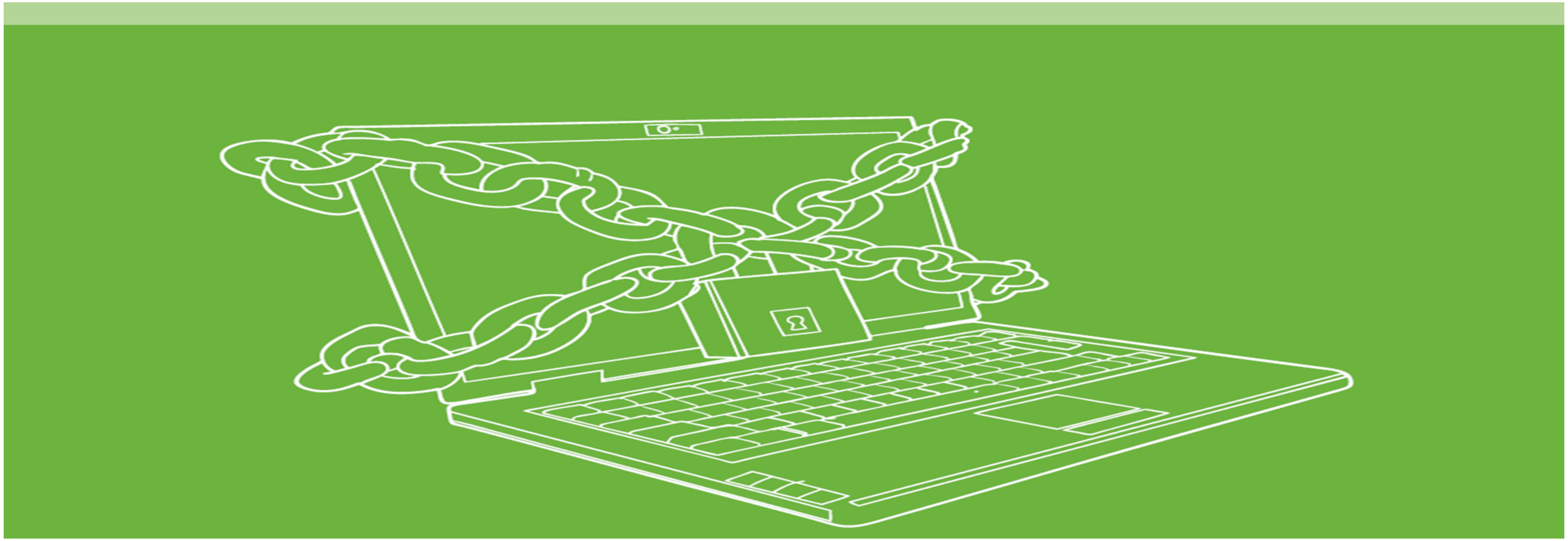


Number 38 *of* 2014

Companies Act 2014

A Framework for Managing Data Protection Risk

Oisin Tobin
Senior Associate, Technology, Media & Communications
Mason Hayes & Curran
otobin@mhc.ie



Data: A Key Asset

- **Core to business models**
  - → Customised services
  - → Advertising
- **Challenge:**
  - → how to think about data protection in a pragmatic way that limits legal risk

MASON
HAYES &
CURRAN

Agenda

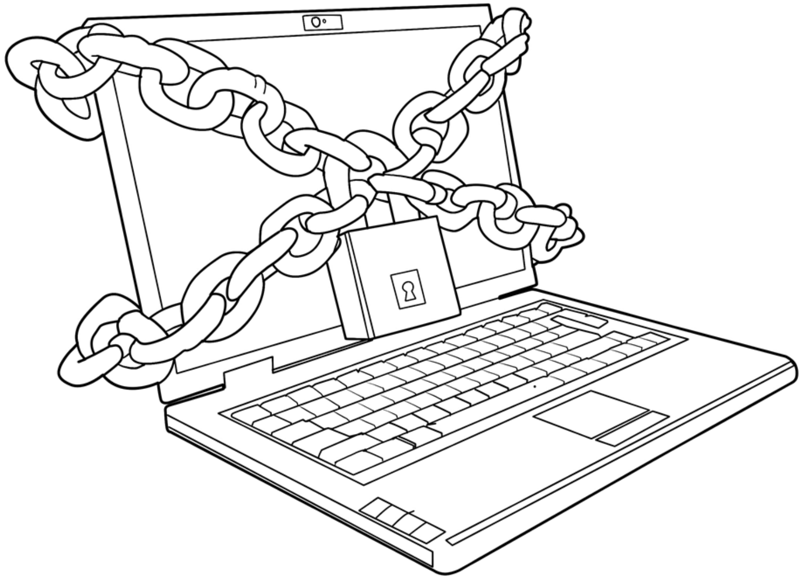
1. **Challenges**

   → What do I need to look out for?

2. **Management Strategies**

   → How do successful businesses proactively deal with the issues?

Part 1: Challenges
(or 7 Questions to Ask)



MASON HAYES & CURRAN

Q 1: Are we being transparent?

- **Must be obtained "fairly"**
  - → Must be transparent about reason the data is being collected and purpose for which the data will be used.
  - → Data must not then be put to a further "incompatible" use

- **Practical Lesson:**
  - → Work out in advance why the data is needed
  - → State this purpose in the Privacy Policy
  - → Remember that *permitted uses* are defined by *disclosures* made

Q 2: Do we have consent?

- **Usually (but not always) required**
  - → If non sensitive: can be implied consent
  - → If sensitive: explicit consent
- **Practical Lesson:**
  - → Have a privacy policy
  - → Build "consent event" into the new customer/ upgrade experience
  - → [If online] consider "in line"/ contextual explanations

MASON
HAYES &
CURRAN

Q 3: How long are we retaining data for?

- **Personal data can only be stored for as long as is necessary**

  → DPC takes an “evidenced based approach”

  → No retention “just in case”

- **Practical Lesson:**

  → Have clear retention/ deletion policies

  → Build into the code

Q 4: Are we collecting unnecessary data?

- **Data should only be collected if necessary**

  → PR risks

- **Practical Lesson:**

  → Identify necessary data/permissions

  → Only ask for that (apps)

  → Delete unnecessary data

MASON HAYES & CURRAN

Q 5: Are we keeping the data secure?

- **Must have ‘appropriate security measures’**
  - → State of technology
  - → Cost of implementation
  - → Nature of data and potential harm if a breach occurs
- **If subcontracting?**
  - → impose equivalent obligations via contract
- **Practical Lesson**
  - → Deploy appropriate resources to security
  - → Manage outsourcing carefully

MASON
HAYES &
CURRAN

Q 6: Are we giving the data to third parties?

- **Are they controllers or processors?**
  - i.e. on whose behalf will they use the data?
  - If controllers: likely need consent
  - If processors: special written contract terms required

- **Practical Lesson**
  - Carefully review disclosures of data
  - Make sure legal requirements (disclosures, contracts) are dealt with

Q 7: Is the data leaving Europe?

- **Within EEA – no issue**
- **If outside EEA:**

  → Ok if approved country, e.g. Canada

  → otherwise safeguards are required
- **Key safeguards**

  → Model Contractual Clauses

  → Safe Harbor (for US)
- **Practical Lesson:**

  → Know where your data is going!

  → Deploy the safeguards where required

MASON
HAYES &
CURRAN

Part 2: Management Strategies

MASON
HAYES &
CURRAN

Four Level Framework

- **A four-way approach to compliance and risk mitigation**
- **Not just about the “legals”. Requires input from product/process designers and IT**
- **Four Layers:**
  - → User facing disclosures
  - → Engineering choices (“Privacy by design”)
  - → Back-end contracts
  - → Response plans

MASON
HAYES &
CURRAN

1. User Facing Disclosures

- Addresses issues around “*transparency*” and “*consent*”
- Have clear public facing statements/ policies re. data usage
- Make sure they incorporated into the customer experience flow
- Also consider inline explanations, help centres etc…
- Fundamentally a customer experience issue

2. Engineering Choices

- Addresses issues around “retention”, “unnecessary processing” and “security”.
- “Privacy by Design”
- Make sure the product is designed and built lawfully
- Fundamentally involves back-end engineering considerations

MASON
HAYES &
CURRAN

2. Engineering Choices

- **Implementation strategies:**
  - → Centralised product management/ controls
  - → Data protection discussions during design/ development (questionnaires), internal review
  - → Software Development Life Cycle policies
  - → Penetration Testing

MASON
HAYES &
CURRAN

3. Back-end contracts

- **Addresses issues around “transfer” and data “leaving Europe”**

- **Primarily done through the use of the correct contractual language**

- **Implementation strategies:**
  - → Understand what sort of contracts are being entered into
  - → Know where the data is going
  - → Have standard language for inclusion in agreements
  - → Negotiate if necessary

4. Response Plans

- **Policies for dealing with major incidents (particularly security breaches)**

- **Often adopted by larger companies to prepare for crises situations and allow for more rapid reposes**

- **Implementation Strategy**
  - → Identify material data protection risks to the business (external attack, internal bad actor)
  - → Prepare response plans

MASON
HAYES &
CURRAN

Key Takeaways

- **Data protection rules impose restrictions on companies**

- **Dealing with these is not just a legal issue**

- **Sophisticated businesses adopt a <u>4 level framework</u> to tackle these challenges considering:**
  - → User disclosures
  - → Product design
  - → Legal agreements
  - → Response plans

MASON
HAYES &
CURRAN

Security risks and breach management

Robert McDonagh
Partner, Commercial
Mason Hayes & Curran
rmcdonagh@mhc.ie

Some Quick Facts

- Average cost is $3.5 million / $145 per record
- Biggest hit from loss of reputation and customers
- Incident response plan shown to reduce cost
- **= take security seriously**

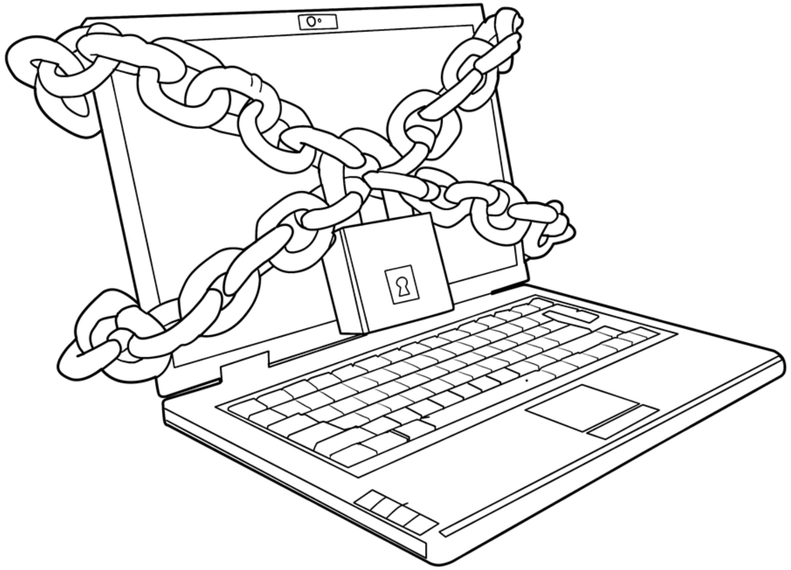
3 Important Points

- Controller often takes the hit, even if caused by processor
- Security breach:
  - not *necessarily* a breach of dp law
  - could still be a breach of contract
- You need to consider laws of other countries too

MASON
HAYES &
CURRAN

Managing a Security Incident

- You cannot be prepared for a security incident without having prepared for it!



Key Management Tools

- Security Breach Policy (and training)
- IT Security Policy
- Acceptable Usage Policy
- Firewalls
- Logs / red flags
- Supplier due diligence
- Contractual measures
- Insurance
- Starters, movers and leavers

Security Breach Policy

- Reporting lines
- Incident management team (and deputies)
  - compliance/audit/legal/IT/security/PR/business control etc
  - include senior officer so can make quick decisions
- Third party advisers
- Include contact details
- Identify key action points
- Training for incident management team

Key Action Points – Initial Steps

- Act quickly
- Assemble incident response team
- Internal escalation
- Stop or mitigate breach
- Information lockdown
- Preserve evidence

NB. remember litigation is possible

MASON
HAYES &
CURRAN

Key Action Points – Investigation

- Identify data controller
- Determine your status
- Investigate facts
    - data affected
    - individuals affected
    - cause
    - resulting harm / damage
    - use legal counsel – legal privilege?
- Remember things move and change quickly

Key Action Points – Implications

- Consider legal exposure
  - liability and fines
  - contract termination
  - audit / escalation
- Contractual obligations?
- Consider any wider business critical implications
- Tolling agreement

MASON
HAYES &
CURRAN

Key Action Points – Notifications

- Notify insurers if required under policy
- Consider regulatory notifications in Ireland and abroad, e.g. DPC, Gardai, foreign DPC etc
- Consider data subject / customer / dc notifications
- Check relevant contracts
  - confidentiality
  - preservation of rights

Key Action Points – Customer Relations

- Create customer relations’ strategy
  - press release
  - customer relationship management
  - mitigation measures: hotline, online helpdesk, monitoring service, discounts etc.

Key Action Points – Corrective Action

- Audit
- Disaster recovery / business continuity etc
- Implement corrective / disciplinary action

MASON
HAYES &
CURRAN

Should you notify DPC?

- No express obligation (except ECSPs / ECNPs)
- No fines in Ireland (except ECNPs / ECSPs)
  - different in other countries
- Negative PR resulting from failure to disclose – can incident be contained?
- Have you notified other regulators etc.?

Should you notify DPC?

- DPC has a statutory obligation of confidentiality
- General practice not to disclose except in response to inquiry by media or concerned person
- However, may issue press release or notify other DPCs if significant incident

Should you notify DPC?

- Before making disclosure, also consider:
  - is disclosure permitted by contract?
  - must you notify insurers first?
  - implications of DPC finding for third party litigation?
  - other implications?
  - similar issues apply to other notifications, e.g. to individuals
- Notification based on current information
- Remember DPC has statutory enforcement powers

Voluntary Code

- Applies if personal data put at risk
- Also earlier DoF public sector guidance
- Code only applicable if DC or DP subject to DPA
- Code is not legally binding
    - but what if incorporated into contract?
- Not applicable to ECNP / ECSP as separate legislation applies

MASON
HAYES &
CURRAN

Voluntary Code – DC and DPC Notifications

- DP must report to DC all incidents of loss of control of data
- DC must report to DPC incidents in which data put at risk within 2 working days unless:
  - individuals already informed;
  - no more than 100 data subjects; and
  - does not include sensitive personal data or financial data
- Keep summary record even if don't notify DPC
  - brief description
  - why chose not to notify

Voluntary code – notifying individuals

- DC must give immediate consideration to informing those affected
  - No obligation if no risk to data due to technological measures of high standard
  - Risk of over notification or more harm than good
  - Audit trail for reasons not to notify

MASON
HAYES &
CURRAN

Steps in a DPC Investigation

1. Initial call / email

2. Written submission

   - amount and nature of personal data

   - action to secure / recover personal data

   - action to inform those affected or reasons for the decision not to do so

   - action to limit damage or distress to those affected

   - chronology of events leading up to incident

   - measures to prevent repetition

MASON HAYES & CURRAN

Steps in a DPC Investigation

3. Additional Materials

   - contract
   - recruitment process
   - relevant policies
   - training documents
   - log of training for relevant staff
   - expressly state it is confidential and commercially sensitive

NB: remember your confidentiality obligations

Steps in a DPC Investigation

4. Enforcement notice?

5. Site visit

    - systems
    - procedures
    - live demonstrations
    - questions

6. Draft finding or report / recommendations

7. Right of reply

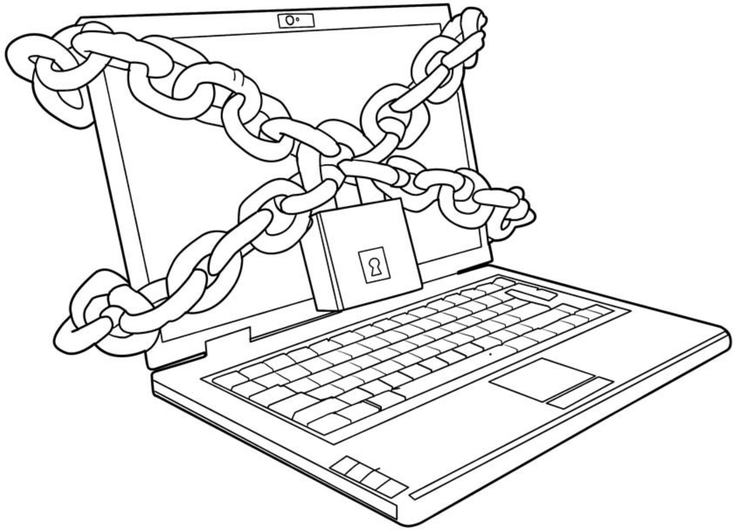
8. Final finding or report

Third Party Contracts

- Diligence
- Notification of incident
- Control of incident
- Co-operation / information / preservation obligations
- Right to interrogate devices / data
- Right to interview personnel

Third Party Contracts

- Notification of policies to others
- Restoration of data
- Confidentiality clause
- Indemnity / cap
- “subject to law” qualifications



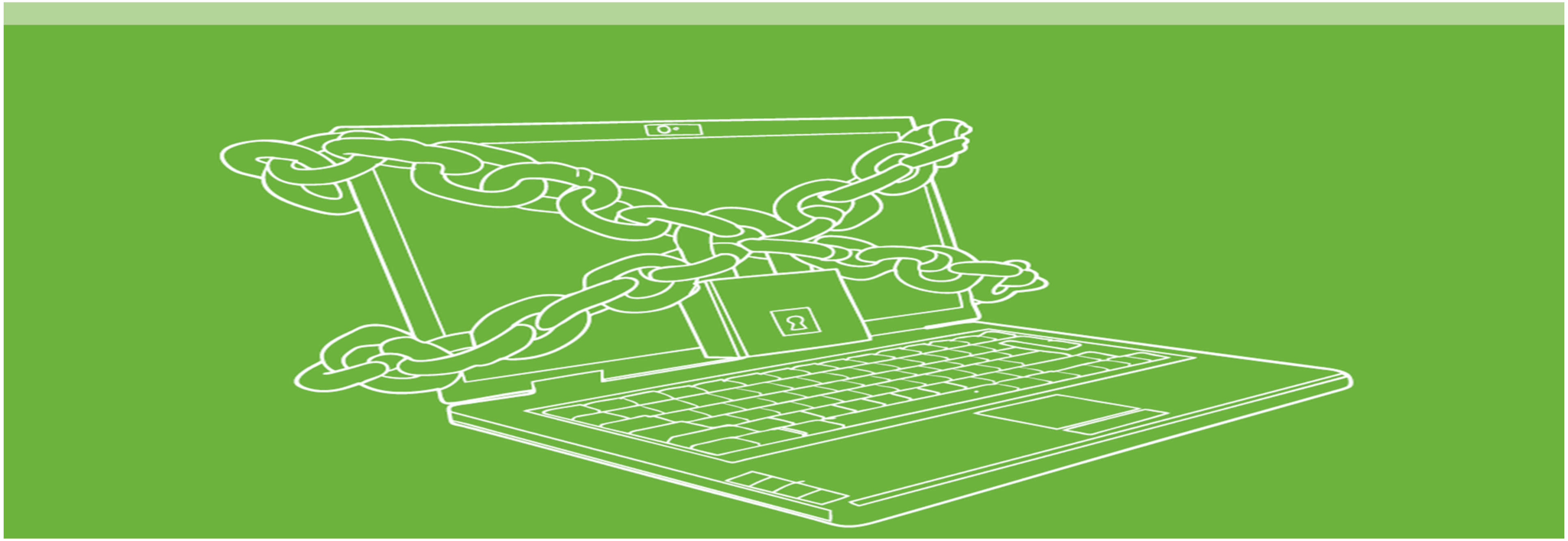
MASON
HAYES &
CURRAN

Things are changing

- Draft General Data Protection Regulation
  - significant fines and J&S liability
  - privacy by design and impact assessment
  - document processing activities
  - evaluate risk, verify effectiveness and demonstrate compliance
  - DP can become joint DC
  - specific notification obligations

MASON HAYES & CURRAN

Q&A



MASON
HAYES &
CURRAN

Thank you