The Inside Track: GDPR & Cyber Security

ALEX FLEMING

Country Head and President of Staffing & Solutions
The Adecco Group UK&I
AGENDA

09:15 - 09:35
GDPR – The Essential Guide
Pat Moran, Cyber Security & Data Privacy Leader, PwC Ireland

9:35 – 09:50
GDPR: An Adecco Group UK&I Perspective
Gavin Tagg, General Counsel and Head of Compliance, The Adecco Group UK&I

09:50 – 10:10
Cyber Security: Staying Safe from Cyber Crime
Pat Moran, Cyber Security & Data Privacy Leader, PwC Ireland

10:10 onwards
Q&A

#theinsidetrack
Our Aims:

• To give you an essential understanding of the key regulations, Cyber Security and its potential impact

• To give you high level pointers; but not to advise on your specific company policies or how to approach implementation according to the regulations

• To provide you with the insight and relevant agenda items to help you make informed decisions

• Chatham House rules apply
Pat Moran
Cyber Security & Data Privacy Leader
PwC Ireland
AGENDA

• Data protection – Why do we need it?
• Data breaches today
• GDPR pillars
• The essential guide
Data Protection – Why do we now need it?

• The increasing sophistication of IT.

• New developments in medical research and care, telecommunications, advanced transportation systems and financial transfers have dramatically increased the level of information generated by each individual.

• Key Questions for Privacy Concerns as a citizen / consumer:
  • What information of mine is being collected?
  • What are you using my information for?
  • Where is my information being stored?
  • Who has access to my information?
  • Who is my information being shared with?
Privacy Breach Examples

• Numerous cases have come to light recently of privacy rights violations, resulting in civil litigation consequences:

• Facebook : 87m users
• Tesco : 20,000 customers
• Equifax : 143M users
GDPR Pillars
The GDPR’s Biggest Pain Points

Businesses are seeing **FIVE GDPR** requirements in particular cause the biggest impact on their future business plans:

- Mandatory data inventorying and record keeping of all internal and third-party processing of European personal data
- Mandatory data-breach notification to regulators and individuals whose information is compromised following information-security failures
- Comprehensive individual rights to access, correct, port, erase, and object to the processing of their data
- Routine data-protection impact assessments for technology and business change
- Mandatory data protection officers and an overall rethinking of privacy strategy, governance, and risk management.

**GDPR Pillars**

- A new ‘Transparency framework’
- A new ‘Compliance Journey’
- A new ‘Punishment Regime’
Building a GDPR Compliance Roadmap
The GDPR Essentials

- Governance & Operating Model
- International Data Transfers
- Process Inventories
- Information Security
- Data Subject Rights
- Data Retention
- Privacy Notices & Consents
GDPR Compliance Roadmap

- Assess Current Capabilities
- Risk Analysis
- Data Discovery
- Gap Assessment
- Remediation Roadmap

Design Future

- Cross Functional Oversight
- Planning
- Implement Programme

Operate and Sustain

- Ongoing Programme Operation
- Maintenance

2018

2018 - 2019

2020 - Beyond
The Inside Track: GDPR & Cyber Security

GAVIN TAGG

General Counsel and Head of Compliance
The Adecco Group UK&I
GDPR
Adecco’s Journey
Data Protection Programme – why are we doing it?

- Comply with GDPR following a risk-based approach
- Be a caring and trusted partner

Data Protection and Privacy is a market differentiator. It is embedded in our business.

Maturity

Adecco is here

Comply with GDPR

Year

April 2017  May 2018  2019 on....
Privacy Programme: Compliance, Position and Operating Model

How compliant we want to be:

**Triaged approach**
(in 2018)
Cover the most material risks in line with industry practice, whilst seeking to address the remaining as soon as practicable, but not necessarily before May 2018, using a risk-based approach.

**95% compliance**
(in 2020/2021)
Positive affirmations of compliance, covering all areas of the new law for all categories of Adecco personal data.
Position reflects the most cautious guidance in the market.

What our position in privacy is:

**Privacy moving towards excellence in compliance**
(in 2018)
- Using privacy to "sell" Adecco to clients and candidates. Be and behave as a trusted partner – linked to OGSM.
- Senior management recognition and buy-in on the importance of privacy, and support through resources and finances.
- Proactive interaction with regulators and forums – connected with Thought Leadership.

**Achieving excellence in compliance globally**
(2020/2021)
- Significant candidate and client awareness activities and significant eminence activities, including sponsorship of events, articles and thought pieces.
- Development and input seals.
- Maximizing and utilizing Adecco's data giving candidates an "information dashboard" to control the types of companies that can see their information and update details in real-time.

Centralized Privacy Operating Model

One view of privacy compliance pushed to entire organization giving single direction of travel
**Introduction**

The *target operating model* is the implementation of our strategy and will define the target structure of our privacy functions.

The model will define what will be delivered in the future; how they will be delivered; who will be responsible and/or interact with what is delivered; and how this will be governed.

---

**Vision**

What is the risk appetite? What is the scope? What is the culture/philosophy?

**As-Is**

Deep dive of the current state: who does what?

**Organisational Principles**

Set the overarching remit and understand constraints for the TOM.

**To-Be: Service Catalogue, Key Processes, Governance Model**

- Define the teams, reporting lines and key roles -
  - Service catalogue: the detailed services and activities required;
  - Key processes: required to manage privacy within the business;
  - Governance: defining the forums/committees needed.

**Transition Plan**

Next steps: roadmap of implementation.
To-Be: Group Structure and Governance

**Privacy Steering Committee**
- Meet on a monthly basis
- Called as required: CIO, CFO, CHRO, Chief Audit Officer, and other functions as required, Regional Leads

**Data Breach Committee**
- Meet ad-hoc

---

*(i) The Group Privacy Office deals with IT and data protection matters; (ii) The Group Privacy Office provide a service for Group Functions (e.g., HR, Finance, Digital, etc.)

**(ii) Local Privacy Lead reports solid line to Group Statutory DPO.
To Be: Local Country Governance Structure

**Group Privacy Office**

**Local Privacy Working Groups**
- Local Privacy Lead
- Local Legal Head
- Privacy Champions (Interact into Local Privacy Working Group (local version of Group Privacy Office) as required)

**Local Business Lines**

**Country/Region/Business Executive**

Periodic invites to appropriate boards/committees to provide Data Privacy update, the local legl head and other local funcitons as required.

**Local Data Breach Committee or equivalent**

---

Dotted line: periodic engagement by invitation or when urgent matters arise

Solid line: consistent engagement

Pink colouring refers to functional or business representatives

Grey colouring refers to an organisational team

Green colouring refers to a committee/forum

*The particular local committee/forum (e.g. Risk Co./Audit Co./Exec Co.) is to be defined by the individual country/region/business lead*
Service Catalogue (15/16)
Responsibility, Accountability, Consulted, Informed (RACI) Matrix

Capability Area: Training and Awareness (1/2)

<table>
<thead>
<tr>
<th>Stakeholders</th>
<th>GPO</th>
<th>LPL</th>
<th>HR</th>
<th>S</th>
<th>D</th>
<th>P</th>
<th>F</th>
<th>IS</th>
<th>C</th>
<th>O</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capability</td>
<td>Notes</td>
<td>Activities</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12. Training and Awareness</td>
<td>-</td>
<td>12.1 Define minimum privacy training materials and computer based trainings per employee type</td>
<td>100</td>
<td>0</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>12.2 Deliver privacy training materials and computer based trainings</td>
<td>0</td>
<td>100</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
</tr>
<tr>
<td></td>
<td></td>
<td>12.3 Define and deliver tailored trainings to specific functions processing personal data</td>
<td>20</td>
<td>80</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
</tr>
<tr>
<td></td>
<td></td>
<td>12.4 Track training completion KPIs against defined target</td>
<td>50</td>
<td>50</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
</tr>
<tr>
<td></td>
<td></td>
<td>12.5 Develop privacy awareness campaigns</td>
<td>100</td>
<td>0</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
</tr>
<tr>
<td></td>
<td></td>
<td>12.6 Deliver privacy awareness campaigns</td>
<td>0</td>
<td>100</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
</tr>
</tbody>
</table>

Stakeholder Abbr. | Explanation
--- | ---
GPO | Group Privacy Office
LPL | Local Privacy Lead
HR | Human Resources
S | Sales
D | Digital
P | Procurement
F | Finance
IS | IT Security
C | Compliance
O | Other

Abbr. | Explanation
--- | ---
R | Responsible – Owns the activity and its completion
A | Accountable – Must sign off or approve the work before it is effective
C | Consulted – Has information needed to complete the work
I | Informed – Must be notified, but not consulted
Communication and Awareness

- **Awareness**
  - Desire
  - Reinforcement
- **Knowledge**
  - Ability
- **Compliance**
  - MODIS: 5S Sustainability Camps (Apr/May)
- **GDPR**
  - GDPR Quiz via Talking Point
  - GDPR Flyer for clients available on Ourspace
  - GDPR integration into PERFORM and Connect Implementation & legacy systems (pre-Connect)
- **Connect**
  - GS Compliance (Q318)
  - PS Compliance (H218)
- **5S Sustainability Camps**
  - Roevin: 5S Sustainability Camps (Mar)
  - Adecco: 5S Sustainability Camps (21-27 Jan)
  - Adecco: 5S Sustainability Camps (Mar)
- **Implementation & legacy systems**
  - GDPR Quiz via Talking Point
  - FAQs for Consultants (late Feb)
- **Talking Point, Our Space, Holding Statement, FAQ’s, Quiz and Communication**
  - Talking Point / Ourspace updates to create base-level awareness and ongoing sources of truth/reference
  - Brand Representatives engage with project and cascade to their teams
- **Webinars / Drop-in surgeries**
  - (late Feb/Mar)
- **GDPR**
  - GDPR Quiz via Talking Point
  - FAQs for Consultants (late Feb)
- **Brand Representative engagement**
  - SMT presentation and updates
- **Adecco**
  - 5S Sustainability Camps (Mar)
  - Adecco: 5S Sustainability Camps (21-27 Jan)
  - Roevin: 5S Sustainability Camps (Mar)

**ADKAR Change Model**

- **Reinforcement**
  - SS Sustainability Camps & implementation
- **Ability**
  - GDPR integration into PERFORM and Connect Implementation & legacy systems (pre-Connect)
- **Knowledge**
  - Connect Immersion Days, Brand representative engagement, SMT presentation and updates
- **Desire**
  - Talking Point, Our Space, Holding Statement, FAQ’s, Quiz and Communication
- **Awareness**
  - Brand Representatives engage with project and cascade to their teams
  - Talking Point / Ourspace updates to create base-level awareness and ongoing sources of truth/reference
  - GDPR Quiz via Talking Point
Key Messages

GET MAPPING NOW!
KNOW YOUR DATA
SORT YOUR DATA
BE ACCOUNTABLE
BE TRANSPARENT
Pat Moran
Cyber Security & Data Privacy Leader
PwC Ireland
Cyber Security Overview

- Criminals are now focussing on technology rather than AK47s
- Technology is such an integral part of business that crimes committed through digital channels are creating fundamental problems, requiring specialist cybersecurity services to mitigate them.

- Cybercrimes such as the distribution of viruses, illegal downloads, phishing and theft of personal information are becoming increasingly common. All cause economic loss and reputational damage.

- A cyber crisis can be one of the most challenging and complicated problems that any organisation will face.

- Companies need investigation and communication strategies, as well as forensic and analytical capabilities. A company’s readiness to handle a cyber crisis can be a marker of its competitive advantage and ensure its survival.
Threats, Hacking, Malware and Other Risks

• There has been an exponential increase in cyber attacks worldwide, forcing clients to address persistent attacks on their business and customers.
• The threat landscape has changed over the years.
• With more sophisticated defences have come more sophisticated offences.

The evolving threats are fuelled by:

• Hackers and their motivations
• Hackers and their resources
• Hackers and their collaborations
• Hackers and their commitments
The Evolving Threat

Cyber crime and viruses initiated, "Morris Worm" and others.

1997: Malicious code, Trojan, Advanced worms

2004: Identity theft, Phishing

2007: DNS attacks, Rise of Botnets, SQL attacks, Anti Spam sites, Competitive sabotage escalation

2010: Social Engineering, DoS, BotNets, Malicious Email, Ransomware attack, PoS comprised

2013: Banking Malware, Keylogger, Bitcoin Wallet Stealer, Identity Theft, Phone Hijacking, Ransomware, PoS attack, Cyber Warfare, Android hack etc.

Present
Example of a Cyber Attack

- Ashley Madison Hack
- NSA Equation Group Hack by the Shadow Brokers
- Equifax
- Stuxnet
- WannaCry Ransomware
- Petya Ransomware
- Bad Rabbit
- US 2016 Presidential Elections
Key Trends - GISS 2018
This year, organizations are prioritizing spending on broad strategies to strengthen their digital ecosystems

Security priorities in 2017 emphasize internal collaboration and new security safeguards for evolving business models. Biometrics and advanced authentication has notably increased as an investment priority compared to 2016 (+3% YoY).

Information security spending priorities for 2017

- Digital enterprise architecture: 59%
- New security needs related to evolving business models: 40%
- Security for the Internet of Things: 40%
- Biometrics & advanced authentication: 40%
- Improved collaboration among business, digital & IT: 59%
Respondents are embracing managed security services to extend and enhance their cybersecurity capabilities

Organizations say they rely on managed security services for highly technical initiatives such as identity & access management, authentication and data loss protection.

Types of managed security services used

- User management (provisioning): 37%
- Real-time monitoring & analytics: 38%
- Data loss protection: 41%
- Authentication: 42%
- Identity & access management: 50%

63% of respondents use managed security services for cybersecurity & privacy.
The impact of data-related security incidents is shifting from compromising data confidentiality to data integrity

Cyberattacks that manipulate or destroy data can undermine trusted systems without the owner’s knowledge and have the potential to damage critical infrastructure.

Report loss or damage of internal records as a result of a security incident (+3% YoY)
Managing Cyber Risks
Leading Cyber Security Practices

1. Board and CEO drive cyber security governance
2. Strong multi-party governance group manages cyber risk
3. Cyber risks are reviewed regularly by the Board
4. Program is threat-driven and assumes a continuous state of compromise
5. Cyber crisis is tested using real world scenarios
6. Cyber crisis response is aligned at all levels within the organization
7. Threat landscape is regularly scanned to understand exposure
8. Resilience is enhanced through intelligence sharing
**Key Questions?**

- What information do you collect, process and store that is critical to the organisation?
- Are critical assets adequately secured?
- How are you protecting high-value information?
- How do you manage cyber security threats?
- How are organization’s cybersecurity strategy aligned with business objectives?
- How do you measure the effectiveness of your cyber security programme?
- Would the organization be able to detect a breach? And what would you do?