Webinar: Deep Dive into “Risk”, “High Risk” and Risk Assessments in the GDPR

Tuesday, 24 May 2016
11:00 AM US EDT

#CIPLGDPR
Webinar Agenda

1. Introduction

2. “Risk”, “High Risk” and Risk Assessments in the General Data Protection Regulation (“GDPR”)

3. Guest Presentations:
   – How you deal with risk in your organisation (e.g. risk methodology, factors which are taken into account during your risk assessment, how do you determine if a processing operation falls within the "risk" or "high risk" category); and
   – Discuss concrete examples on how you approach in the context of (1) data breaches, (2) legitimate interest and (3) data protection impact assessment.

4. Q&A Discussion (*7 Unmute / *6 mute)
Speakers

Moderator: Bojana Bellamy
President
Centre for Information Policy Leadership

Hilary Wandall
AVP, Compliance & CPO
Merck & Co., Inc.

Emma Butler
Senior Director, Privacy and Data Protection
RELX Group

Maria Chiara Atzori
Head Data Privacy Switzerland
Novartis
Risk-Based Approach in GDPR

**Horizontal – Accountability Obligation**
- More flexibility for controllers to build, implement and demonstrate privacy programme and compliance measures
- Based on **likelihood and severity of risks for individuals**
- Based on nature, scope, context and purposes of processing

**Specific obligations based on risk**
- Privacy by design
- Data security
- Security breach notification to DPAs
- Appointment of representative of controller or processor established outside the EU

**Specific requirements only for high risk processing**
- Security breach notification to individuals
- Data Protection Impact Assessment
- Prior consultation with DPAs for high risk processing that cannot be mitigated

**Implied consideration of risk**
- Legitimate interest balancing test
- Purpose limitation - determining compatibility of subsequent purposes
- Fair processing

Further guidance provided by DPAs, EDPB, codes of conduct and certifications, DPO
1. Personal data processing that may result in **physical, material or non-material damage**, in particular:
   - Discrimination
   - Identity theft / fraud, financial loss
   - Reputation damage
   - Loss of confidentiality of personal data protected by professional secrecy
   - Unauthorised reversal of pseudonymisation
   - Any other significant economic or social disadvantage
   - Individuals deprived of rights and freedoms, or prevented from exercising control over their data
   - Processing sensitive data, including genetic data
   - Profiling (personal aspects are evaluated (e.g. analyse or predict work performance, economic situation, health, personal preferences, behaviour, location) to create or use personal profiles
   - Processing children’s and vulnerable persons’ data
   - Processing large amounts of data and individuals

2. High risk
   - High likelihood or severity of risks above, or involve use of new technology, or no DPIA carried out before, or time elapsed since initial processing
   - Pre-defined types of high-risk processing – automated decision taking; large scale processing of sensitive data or criminal convictions; systematic monitoring of public areas
Detailed View of Risk Assessments in the Context of Organisational Privacy Compliance Programs

Risk Assessment

At Programmatic Level
- Determines the Program and its elements
- Periodic Program assessment v. internal and external risks
- Adjusting the Program elements

At Legal Requirement Level
- DPIA and Privacy by Design for new products, services, technology
- Legitimate interest processing
- Purpose limitation
- Security
- Data breach

Consider benefits of processing and mitigations
The Risk Assessment Process – Incorporating Risks, Benefits, Mitigations

Risk determines privacy program, its elements, levels of requirements and applied controls

Risk to individuals
Other factors impact the risk
Regulated country and prominent enforcement
Risks to organisations

- geographic scope
- type of activity
- type of data
- volume of data
- third party involvement

Likelihood and severity

Benefits and mitigations are part of equation

www.informationpolicycentre.com
Guest Speaker

Hilary Wandall
AVP, Compliance & CPO
Merck & Co., Inc.

#CIPLGDPR
Our global Privacy Program supports our company mission of saving and improving lives by promoting and assuring a culture of privacy accountability where four privacy values are embedded into the way we work and how we engage people everywhere we operate.

<table>
<thead>
<tr>
<th>Respect</th>
<th>Trust</th>
<th>Prevent Harm</th>
<th>Comply</th>
</tr>
</thead>
<tbody>
<tr>
<td>We recognize that privacy concerns often relate to the essence of who we are, how we view the world, and how we define ourselves, so we strive to respect the perspectives and interests of individuals and communities and to <strong>be fair</strong> and transparent in how we use and share information about them.</td>
<td>We know that trust is vital to our success, so we strive to build and preserve the trust of our customers, employees, patients and other stakeholders in how we respect privacy and protect information about people.</td>
<td>We understand that misuse of information can create both tangible and intangible harms for individuals, so <strong>we seek to prevent physical, financial, reputational, and other types of privacy harms to individuals</strong>.</td>
<td>We have learned that laws and regulations cannot always keep pace with rapid changes in technologies, data flows, and <strong>associated shifts in privacy risk and expectations</strong>, so we strive to comply with both the spirit and the letter of privacy laws in a manner that drives consistency and efficiency for our global business operations.</td>
</tr>
</tbody>
</table>

www.informationpolicycentre.com
## Our Risk Practices

<table>
<thead>
<tr>
<th>Merck &amp; Co., Inc. (MSD) Risk Management Practice</th>
<th>Alignment to GDPR</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Process-level risk evaluation</strong> <em>(Respect, Prevent Harm)</em></td>
<td></td>
</tr>
<tr>
<td>Privacy impact assessment</td>
<td>Article 25</td>
</tr>
<tr>
<td>• Inherent risk and benefit determination during scope/threshold analysis <em>(Fairness principle)</em></td>
<td>Article 35</td>
</tr>
<tr>
<td>• Control effectiveness analysis</td>
<td>Article 36</td>
</tr>
<tr>
<td>• Residual risk analysis</td>
<td></td>
</tr>
<tr>
<td><strong>Scientific research</strong></td>
<td>Article 9</td>
</tr>
<tr>
<td>• Ethics committee/IRB waiver of consent for minimal risk</td>
<td>Article 89</td>
</tr>
<tr>
<td><strong>Breach notification</strong></td>
<td>Article 33</td>
</tr>
<tr>
<td>• Where not expressly required by law, where risk of harm warrants notification, or, as applicable (e.g., HIPAA) where risk assessment shows greater than low probability of data compromise</td>
<td></td>
</tr>
<tr>
<td><strong>Program-wide risk evaluation</strong> <em>(Comply)</em></td>
<td></td>
</tr>
<tr>
<td>External factors (e.g., laws, policy trends) analyzed by mapping to applicable control effectiveness categories</td>
<td>Article 24</td>
</tr>
</tbody>
</table>
Privacy Risk in Practice

Inherent Privacy Risk
- Impact on the Individual (data sensitivity, activity sensitivity, volume)
- Likelihood of Occurrence (third party involvement, geographic scope, incident and audit history)
- Determines form of assessment required

Privacy Control Effectiveness
- 8 “CE” Categories encompassing more than 50 controls
- Higher inherent risk requires demonstration of more comprehensive set of controls
- Effectiveness ratings based on demonstration of control

Residual Privacy Risk
- Residual Privacy Risk Impact = reduction in inherent privacy risk impact after application of controls
- Residual Privacy Risk Likelihood = reduction in inherent privacy risk likelihood after application of controls

Consistent Quantitative Scale Enables Program-Wide Comparisons

Potential threats “proxies”

Anticipated benefits based on “purpose”
<table>
<thead>
<tr>
<th>Risk Factor</th>
<th>Analysis</th>
<th>Risk Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data</td>
<td>Sensitive</td>
<td>High</td>
</tr>
<tr>
<td>Activity/Context</td>
<td>Sensitive</td>
<td>High</td>
</tr>
<tr>
<td>Data Volume</td>
<td>&gt; 10,000 users</td>
<td>Medium</td>
</tr>
<tr>
<td>Data Subjects</td>
<td>Consumers</td>
<td>Medium</td>
</tr>
<tr>
<td>Third Parties</td>
<td>Yes, Multiple – In country</td>
<td>Medium</td>
</tr>
<tr>
<td>Third Countries</td>
<td>Other Region</td>
<td>High</td>
</tr>
<tr>
<td>Applicable Law</td>
<td>Yes – Recent Enforcement</td>
<td>High</td>
</tr>
<tr>
<td>Incident History</td>
<td>1 Instance</td>
<td>Medium</td>
</tr>
</tbody>
</table>

**Overall Assessment**

**Employee Expense App**

<table>
<thead>
<tr>
<th>Risk Factor</th>
<th>Analysis</th>
<th>Risk Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data</td>
<td>Confidential</td>
<td>Medium</td>
</tr>
<tr>
<td>Activity/Context</td>
<td>Confidential</td>
<td>Medium</td>
</tr>
<tr>
<td>Data Volume</td>
<td>Pilot (&lt;1,000)</td>
<td>Low</td>
</tr>
<tr>
<td>Data Subjects</td>
<td>Employees</td>
<td>Medium</td>
</tr>
<tr>
<td>Third Parties</td>
<td>No</td>
<td>Low</td>
</tr>
<tr>
<td>Third Countries</td>
<td>No</td>
<td>Low</td>
</tr>
<tr>
<td>Applicable Law</td>
<td>Yes – Past Enforcement</td>
<td>Medium-High</td>
</tr>
<tr>
<td>Incident History</td>
<td>No</td>
<td>Low</td>
</tr>
</tbody>
</table>

**Overall Assessment**

www.informationpolicycentre.com
### Application – 2 Projects

#### Applying Inherent Privacy Risk Analysis to Controls Assessment

<table>
<thead>
<tr>
<th>Assessment Criteria</th>
<th>Consumer Health App</th>
<th>Employee Expense App</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personnel Expertise</td>
<td>Expert (Privacy Office)</td>
<td>Advanced (Steward w/ Privacy Office)</td>
</tr>
<tr>
<td>Assessment Documentation</td>
<td>Global Privacy System</td>
<td>Local Inventory and Records</td>
</tr>
<tr>
<td>In Scope of Annual Management Certification</td>
<td>Yes (Functional Leader)</td>
<td>Yes (Country Leader)</td>
</tr>
<tr>
<td>Evidence</td>
<td>Yes, in Global Privacy System</td>
<td>Yes, in Local Records</td>
</tr>
<tr>
<td>Transparency Analysis</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Governance Analysis</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Individual Rights Analysis</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Security Analysis</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Incident Management Analysis</td>
<td>Enhanced</td>
<td>Yes</td>
</tr>
<tr>
<td>Third Party Analysis</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>More Stringent Local Law Analysis</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Online Privacy Certification/Seal</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

6 of 8 Control Effectiveness Categories
Comparing 2 Projects

Evaluating the Effectiveness of Privacy Controls and Program Risk

- Standard Quantitative Measures Enable Program-Wide Averages and Trending

Risk Likelihood

Risk Impact

#CIPLGDPR
Guest Speaker

Emma Butler
Senior Director, Privacy and Data Protection
RELX Group
Determination and Practical Articulation of Risk Appetite

Confidential, for internal use only

Operating and Governance Principles / Internal Control Framework
RELX Group’s Risk Management and Internal Control Framework – Three Lines of Defence

1st Line of Defence:
- Management oversight & control
- 2 x Yearly risk assessment process
- Annual representation / ICO process

2nd Line of Defence:
- Functional Assurance
- 2 x Yearly risk update to Board
- Functional reports incl Compliance, Information Security, M&A Treasury, Tax & Strategy

3rd Line of Defence:
- Audit
- Annual audit plan
- Risk Management & Internal Control Report
- Audit reports

Audit Committees

www.informationpolicycentre.com
Practical Example: Legitimate Interests

- Article 29 opinion WP 217
- Are the interests legitimate? Company (sometimes customer interests); individuals.
- Is the processing necessary to achieve the interests pursued?
- Do the rights of the individual override company interests?
- Are there safeguards we can put in place? Data minimisation, technical and organisational measures, privacy by design, transparency...
- Assessment also covers: broader societal impacts; benefits to individuals / society; risks of not doing the processing.

Practical Example: Data Protection Impact Assessments

- Data types: some flagged as needing more attention.
- Assessment against 8 UK DP Act principles.
- Considers: fairness (transparency); fairness (proportionality and reasonable expectations of consumers).
- Risks identified that could lead to questions about compliance with a particular principle.
- Risks and mitigation factors / solutions granular and specific to project.
Guest Speaker

Maria Chiara Atzori
Head Data Privacy Switzerland
Novartis
Privacy Risk Assessment at Novartis

Maria Chiara Atzori, Head Data Privacy Switzerland
Basel, 24 May 2016
Robust approach to increase control while reducing bureaucracy and combining different assessments

From:

**Different Privacy Assessments**

- **Swiss Privacy Inventory**
  - 30 questions (Online questionnaire)

- **Privacy Impact Assessment (PIA)**
  - 80+ questions (Word document)

- **Business Impact Assessment (BIA)**
  - 28 privacy questions (Excel spreadsheet)

To:

**One user friendly tool**

- 12 questions for the Business Owner
- 6 questions for Information Manager
Novartis current privacy risk assessment towards its further evolution

<table>
<thead>
<tr>
<th>Classification of risk</th>
<th>Need to review the distinction between risk and high risk processing of data</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Increase focus on likelihood and severity of the risk to the individuals</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Balancing risks</th>
<th>Need to improve understanding of data privacy risks and its implications in the context of business initiatives</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Absence of an assessment of the processing benefits</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mitigation options</th>
<th>Not context related and not sector-specific</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Unilateral mitigation of risks</td>
</tr>
<tr>
<td></td>
<td>Establish new set of safeguards to achieve strong protection</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>GDPR opened gaps</th>
<th>Consultation of DPAs for high risk processing</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Legitimate interest balancing</td>
</tr>
<tr>
<td></td>
<td>Purpose limitation (e.g. secondary use of data)</td>
</tr>
</tbody>
</table>
Develop a sound privacy risk assessment to build trust and confidence

Be able to solve the tension between data availability and harm to individual

- Identification of gaps between industry and patients’ interests and potentially threatening activities in public perception
- Sound assessment of privacy risk and fit for purpose mitigation of gaps

Build trust and confidence

- Future use cases (e.g., RWE) depend on patients entrusting industry with personal data and content for far reach analyze
- Sound privacy risk assessment as a cornerstone of accountability
If you would like to ask a question, please hit *7 (star 7) to unmute your phone.

Please hit *6 (star 6) to mute your phone again.

Bojana Bellamy  
President  
Centre for Information Policy Leadership

Emma Butler  
Senior Director, Privacy and Data Protection  
RELX Group

Hilary Wandall  
AVP, Compliance and CPO  
Merck & Co., Inc.

Maria Chiara Atzori  
Head Data Privacy Switzerland  
Novartis
Contacts

Bojana Bellamy
President
Centre for Information Policy Leadership
bbellamy@hunton.com

Hilary Wandall
AVP, Compliance and CPO
Merck & Co., Inc.
hilary.wandall@merck.com

Emma Butler
Senior Director, Privacy and Data Protection
RELX Group
emma.butler@relx.com

Maria Chiara Atzori
Head Data Privacy Switzerland
Novartis International
maria_chiara.atzori@novartis.com

Centre for Information Policy Leadership
www.informationpolicycentre.com

Hunton & Williams Privacy and Information Security Law Blog
www.huntonprivacyblog.com

#CIPLGDPR