Implementing GDPR

Lessons learned across data-driven sectors
Other included: CDO or COO
One respondent had not yet appointed a programme lead
Many organisations admitted that there had been multiple Programme Directors over the last 12 months
When is privacy not something to keep quiet about?

Programme Scope Control Areas

1. Privacy Policy Environment
2. Privacy Accountabilities and Governance
3. Privacy Risk Appetite
4. Lawful conditions and authorisation of processing: Data Protection Notices, Consent
5. Personal data transfer model
6. Privacy Impact Assessments
7. Personal data management
8. IT and Physical security of personal data
9. Records of processing
10. Data Flow Mapping and Data Asset Inventory
11. Third party risk assessment
12. Third party contract remediation
13. Data subject request management
14. Personal data complaints handling
15. Incident and breach management
16. IT enablement
17. Communication and Training
18. Third line (internal audit) review

- All firms taking a risk-based approach
- Broad consensus on scope control areas
- Four respondents excluded third line
- Two respondents excluded dataflow mapping.
- Other activities, included:
  - Active engagement with regulators / forums
  - Legal workstream around monitoring joint ventures

Areas of scope challenge:
- Country/Entities
- Legacy Records Mgt
- Unstructured data
<table>
<thead>
<tr>
<th>Top Priorities</th>
<th>Top issues</th>
<th>Programme Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lawful conditions and authorisation of processing (58%)</td>
<td>Knowing where our data is (76%)</td>
<td>Organisational complexity (82%)</td>
</tr>
<tr>
<td>Data flow mapping and data asset inventory (47%)</td>
<td>Erasure and record retention (71%)</td>
<td>Volume of work to comply (65%)</td>
</tr>
<tr>
<td>Privacy accountabilities and governance (37%)</td>
<td>Behavioural change (71%)</td>
<td>Other (e.g. unstructured data) (47%)</td>
</tr>
</tbody>
</table>
When is privacy not something to keep quiet about?

- Budgets continue to be challenged by senior management
- Actuals likely to be higher
- Strategic change (especially within IT) being excluded
- Future BAU cost uplifts not estimated at this stage
- Some key challenges being excluded from scope (e.g. legacy records management)
When is privacy not something to keep quiet about?

GDPR Programme Headcount

Roughly how many full-time employees (FTE) are assigned to your GDPR programme?

1.0-5
2.5-10
3.10-20
4.20-30
5.30-40
6.40+

0% 5% 10% 15% 20% 25% 30% 35% 40%
Executive Reporting

How often do you receive internal reports on the progress of your GDPR programme?

1. Once a week (10%)
2. Fortnightly (20%)
3. One a month (40%)
4. Every three months (20%)
5. Other (please specify) (10%)

If the GDPR programme, or privacy issues in general, are discussed in board meetings, which of the following topics are typically discussed?

1. Privacy strategy (30%)
2. Legal and compliance issues (30%)
3. GDPR programme budget (20%)
4. IT concerns (10%)
5. Consumer complaints (5%)
6. Managing breaches (5%)
7. Other (10%)

How often do you discuss privacy issues and the GDPR programme in board meetings?

1. Regularly (50%)
2. Occasionally (40%)
3. Only after an incident (10%)
4. Rarely (0%)

- Lack of Board engagement
- Depth and frequency of reporting needs to increase
- Limited risk position / risk reduction conversations being held with Boards
- Differing views between Programme Director v Executive Sponsor
Current & Target compliance

Do you consider your organisation to be fully compliant with the Data Protection Act?

1. No, process in place
2. Yes, but sub-optimal processes in place
3. Yes, adequate process in place, but manual and/or difficult to scale
4. Yes, adequate process, scalable
5. Yes, optimal process in place, fully scalable within expected parameters
6. Not-known/not assessed

What level of compliance is your organisation targeting for GDPR?

1. No process in place
2. Compliant, but sub-optimal processes in place
3. Compliant, adequate process in place, but manual and/or difficult to scale
4. Compliant, adequate process, scalable with effort
5. Compliant, optimal process in place, fully scalable within expected parameters
6. Not-known/undecided

Are these reported compliance positions really reflective of the current positions of firms?
Target Compliance – DSARs

What level of compliance is your organisation targeting for: data subject access requests?

1. No process in place
2. Compliant, but sub-optimal processes in place
3. Compliant, adequate process in place, but manual and/or difficult to scale
4. Compliant, adequate process, scalable with effort
5. Compliant, optimal process in place, fully scalable within expected parameters
6. Not-known/undecided

- 60% of respondents indicated a higher target for compliance
- Focus is in uplifting DSAR capabilities (people, processes)
- Some firms indicated a desire to invest in technology (e.g. self-service, robotics and automation)
- Consideration to transform existing DSARs teams into central rights hubs
- Challenge for global firms (e.g. cross territorial activities, language skills)
- Concerns on level of volume increases post May 2018
## Target Compliance – Data portability

### What level of compliance is your organisation targeting for: data portability?

<table>
<thead>
<tr>
<th>Level</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>No process in place</td>
<td>10%</td>
</tr>
<tr>
<td>Compliant, but sub-optimal processes in place</td>
<td>20%</td>
</tr>
<tr>
<td>Compliant, adequate process in place, but manual and/or difficult to scale</td>
<td>40%</td>
</tr>
<tr>
<td>Compliant, adequate process, scalable with effort</td>
<td>20%</td>
</tr>
<tr>
<td>Compliant, optimal process in place, fully scalable within expected parameters</td>
<td>10%</td>
</tr>
<tr>
<td>Not-known/undecided</td>
<td>5%</td>
</tr>
</tbody>
</table>

- **Lower level of compliance expectations**
- **One respondent indicated that it will not address portability until industry standards are agreed**
- **Firms adopting different approaches**
- **Recognised dependency on other initiatives (e.g. PSD II)**
- **Engagement with industry bodies**
- **Opportunity for further collaboration**
Target compliance – Other Individual Rights

What level of compliance is your organisation targeting for: individual rights?

- 80% of respondents are targeting individual rights compliance to an adequate and scalable level with effort
- Concern with the actual survey responses
- Most firms only focusing on a sub-set of the rights
- Different approaches being adopted to Right to be forgotten/erasure
Use of Technology

Are you using technology solutions to help you achieve compliance with GDPR? If appropriate, please indicate whether technology applied is existing or new.

- Third party solutions
- General robotics
- Process automation
- Consent management
- Secure file transfer services

- No
- Yes, applying existing technology solutions
- Yes, applying new technology solutions

- Firms generally applying existing technology
- DFM – mixed response to using technology
- 79% not deploying robotics
- 70% not considering process automation
- Current focus is on people and manual processes uplift

There is an opportunity for firms to consider how technology could be better used to deliver more cost effective compliance
100% of respondents are confident they will deliver their target compliance state.
Areas of focus post-May 2018

What are your biggest compliance concerns/areas of focus post-May 2018? Please select all that apply.

- Lawful collection of personal data
- Portability
- Assessing risk of detriment to data subject (Privacy by Design)
- Handling data subject requests
- Maintaining adequate personal data records
- Maintaining adequate records of personal data processing
- Safeguarding personal data
- Meeting new individual rights
- Responding appropriately to a data breach
- Cross-border data movement (i.e. to third countries outside the EU)
- Liaising with regulators/regulator expectations

Key questions raised

- Major concern: Maintaining records of processing and Meeting new Rights
- How to transition and embed GDPR processes into BAU (e.g. Article 30)?
- When and how to address legacy issues and records management?
- How will these be funded?
Funding timeline, budget & FTE

How many years do executive sponsors expect to fund your GDPR programme post the compliance deadline (May 2018)?

- 1.0-6 months: 20%
- 2.6 months-1 year: 40%
- 3.1-2 years: 20%
- 4.2 years+: 10%

Please indicate the range of budget for your overall programme budget, post-May 2018?

- Less than 1mn: 10%
- 2.1-5mn: 20%
- 3.5-20mn: 40%
- 4.20-50mn: 20%
- 5.50mn+: 10%
- Don’t know: 10%

Approximately how many additional FTE will you require post-May 2018, to comply with the GDPR?

- 1.0-5: 30%
- 2.5-10: 30%
- 3.10-20: 10%
- 4.20-30: 10%
- 5.30-40: 10%
- 6.40+: 10%

- Limited funding expectations post May 2018
- Expectation that BAU activities will address ‘the tail’
- Budget’s and timelines generally risk being underscoped and may reflect a short-term view on GDPR compliance
- Limited discussion on the strategic vision for privacy (i.e. their true target state)
### Outsourcing

Have you considered outsourcing any of the following data protection and or privacy functions? Please select all that apply.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. GDPR Programme</td>
<td></td>
</tr>
<tr>
<td>2. Data Protection Officer</td>
<td></td>
</tr>
<tr>
<td>3. Privacy Policy Environment</td>
<td></td>
</tr>
<tr>
<td>4. Privacy Impact Assessments</td>
<td></td>
</tr>
<tr>
<td>5. Data subject request management</td>
<td></td>
</tr>
<tr>
<td>6. Privacy Accountabilities and Governance</td>
<td></td>
</tr>
<tr>
<td>7. Lawful conditions and authorisation of processing: Data...</td>
<td></td>
</tr>
<tr>
<td>8. Personal data transfer model</td>
<td></td>
</tr>
<tr>
<td>9. Personal data management</td>
<td></td>
</tr>
<tr>
<td>10. IT and Physical security of personal data</td>
<td></td>
</tr>
<tr>
<td>11. Records of processing</td>
<td></td>
</tr>
<tr>
<td>12. Data Flow Mapping and Data Asset Inventory</td>
<td></td>
</tr>
<tr>
<td>13. Third party risk assessment</td>
<td></td>
</tr>
<tr>
<td>14. Third party contract remediation</td>
<td></td>
</tr>
<tr>
<td>15. Personal data complaints handling</td>
<td></td>
</tr>
<tr>
<td>16. Incident management, breach reporting, business...</td>
<td></td>
</tr>
<tr>
<td>17. IT enablement</td>
<td></td>
</tr>
<tr>
<td>18. Communication and Training</td>
<td></td>
</tr>
<tr>
<td>19. Third line (internal audit) review</td>
<td></td>
</tr>
<tr>
<td>20. Risk reduction mapping</td>
<td></td>
</tr>
<tr>
<td>21. Other (please specify)</td>
<td></td>
</tr>
</tbody>
</table>
Regulatory Guidance

Where would more guidance be useful from local regulators, e.g., ICO, or the Article 29 Working Group? Please select all that apply.

1. Legal and compliance advice
2. Data Protection Officer
3. Portability rights
4. Privacy notices (capture and consent)
5. Privacy breach reporting and management
6. Privacy by design
7. Privacy governance
8. Personal data flow mapping/inventory management
9. Supplier due diligence
10. Consumer complaints
11. Training and awareness
12. UK derogations
13. Other (please specify)
About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

© 2016 EYGM Limited.
All Rights Reserved.

BMC Agency
GA 1005423

ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

ey.com