GDPR Case Study:
Operational Implementation
on a Global Scale

Ben Westwood:
UK Data Protection Officer 25 January 2018
Agenda:

- eBay Inc. overview
- Global privacy function
- eBay European operations
- Binding Corporate Rules
- Operationalizing the GDPR
  - User rights
  - Vendor management
  - Privacy Ops
- Article 30 records of processing
- Questions
eBay Inc. at a Glance

- **168M** Global active buyers
- **380M** App downloads
- **12.6K** Members of staff
- **>100** Sites globally

Data as of Q4 2017
eBay Global Privacy Team:
Overview of eBay European operations
Goal: To apply uniform, adequate and global data protection and privacy standards for the handling of personal information throughout eBay.

Approved by CNPD in 2012

- Commitment to processing principles
- Staff privacy awareness training
- Complaint handling procedures
- Regular auditing and reporting
- Cooperation with DPAs
In addition to eBay Inc.'s privacy principles and the practices described in our privacy policies, eBay Inc. has established a set of Corporate Rules (also referred to as Binding Corporate Rules), approved by the Luxembourg National Data Commission.

These Corporate Rules are a commitment by eBay Inc. to adequately protect your personal information regardless of where the data resides, and depending upon your location, may provide additional privacy rights through your privacy regulator or a court. Translations of our User Corporate Rules are available below:

- English
Operational GDPR at eBay

User Rights
• The right to be informed (Art. 13)
• The right of access (Art. 15)
• The right to rectification (Art. 16)
• The right to erase (Art. 17)
• The right to restrict (Art. 18)
• The right to data portability (Art. 19)

Vendor Management
• Privacy Impacts Assessments
• Operational capabilities
  • User rights
  • Breach notifications
• Contract revisions

Privacy Operations
• Privacy Impacts Assessments
• Online resources
• Training
• Champions
• Culture
User Rights Management:

Phase 1
1. Subject Access Requests
2. Data Erasure
3. Data Portability

Approach
1. Gap analysis
2. Focused compliance audits
   • On-site interviews
   • Electronic surveys
3. Documented and reported findings
   • Recommendations for improvements
Creating a Paper Shield

User Rights Policy

- Data Portability Standard
- Subject Access Standard
- Erasure Standard

- Subject Access Guideline
- Redaction Guideline
- Regulatory Exemption Guideline
- Manifestly Unfounded Guideline

Standard Operating Procedures
Standard Operating Procedures
Standard Operating Procedures
Standard Operating Procedures
Standard Operating Procedures
Embed in to Business
Vendor Management:

2014
- Annual template reviews
- Security risk classification
- Privacy risk classification
- Periodic review
- Security assessment platform

2015
- GDPR contract refresh (internal)
- Privacy impact assessments
- Privacy / security collaboration
- PIA Platform Launch

2016
- GDPR contract review (external)
- Risk based prioritisation
- GDPR contract updates
- GDPR capability reviews

2017
- GDPR contract review (external)
- Risk based prioritisation
- GDPR contract updates
- GDPR capability reviews

2018
Vendor Privacy Security Platform:

- Tracks assessment of all vendors / suppliers
- Documents all data types being processed
- Categories of personal data
- Categories of data subjects
- Documents all processing purposes
- Documents all processing locations
- Central documentation repository
- Automated tracking and management
Operational Privacy Compliance at eBay

<table>
<thead>
<tr>
<th>Training and awareness</th>
<th>Online resources</th>
<th>Privacy Champions</th>
</tr>
</thead>
<tbody>
<tr>
<td>• New training modules</td>
<td>• Privacy Impacts Assessments</td>
<td>• Building the network</td>
</tr>
<tr>
<td>• On site awareness days</td>
<td>• Privacy policies and standards</td>
<td>• Enhanced training</td>
</tr>
<tr>
<td>• IPad competitions</td>
<td>• Brand Privacy</td>
<td>• Incentives</td>
</tr>
<tr>
<td>• Lunch and learn</td>
<td>• Privacy FAQs</td>
<td>• Social collaboration</td>
</tr>
<tr>
<td>• Privacy stalls / booths</td>
<td>• Ask privacy</td>
<td></td>
</tr>
<tr>
<td>• Onsite certifications</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Privacy Champion Program:

**Global Recruitment**
Utilising existing networks
Subject matter experts
Business contacts
Privacy advocates

**Two distinct groups**
1. Builders
2. Defenders

**IAPP Membership**
Free membership
Discounted certifications
CIPP as the baseline

**Resources & Support**
Social collaboration
Career development
Enhanced training
Sense of community

---

**Global Recruitment**
Utilising existing networks
Subject matter experts
Business contacts
Privacy advocates

**Two distinct groups**
1. Builders
2. Defenders

**IAPP Membership**
Free membership
Discounted certifications
CIPP as the baseline

**Resources & Support**
Social collaboration
Career development
Enhanced training
Sense of community
Practical advantages
• Builders - Prevention rather than cure
• Defenders - First responders
• Open lines of communication
• GDPR policies, standards and processes
• Raises organisational awareness of privacy
• Develops a culture of privacy compliance

Culture of privacy
“It’s about moving away from seeing the law as a box ticking exercise, and instead to work on a framework that can be used to build a culture of privacy that pervades an entire organisation”

Elizabeth Denham – UK Information Commissioner
Privacy Champions:

Implementation

• Defined roles and responsibilities
• Career progression / personal development
  o Bespoke personal objectives
• Regular meetings
  o One to ones
  o Quarterly information sharing forums
    ✓ GDPR updates
    ✓ Current / emerging issues
  o Annual conferences / events
• Don’t forget the Swag!
  o Lanyards, mouse mats, pens etc.
Article 30, Records of Data Processing

- Name and contact details of the controller
- Description of the security measures
- Details of the data protection officer
- The purposes of the processing
- The categories of data subjects
- The categories of personal data
- The categories of recipients of the data
- The categories of recipients outside of the EEA
- The mechanism used to permit data transfer outside of the EEA
- Retention schedules
- Details of recipients outside of the EEA

Article 30, Records of Data Processing
Questions?