GDPR at the WBG

44th ICA SIO Meeting

May 25th, 2018
NYC, New York, US

Paloma Beneito
Daniele Balduzzi

This material is a product of the staff of the International Bank for Reconstruction and Development/The World Bank. The findings, interpretations, and conclusions expressed in this presentation do not necessarily reflect the views of the Executive Directors of The World Bank or the governments they represent. The World Bank does not guarantee the accuracy of the data included in this work. This material should not be reproduced or distributed without The World Bank's prior consent.
1 Context

2 Where we are

3 Recommended actions

4 Where we want to be
Personal Data at the WBG

- WBG uses Personal Data;
- WBG handles personal data from EU individuals;
- Personal data supports WBG activities and business process;
- Use of emerging technologies, introduce even more privacy vulnerabilities.
Nice wake up call

The EU’s General Data Protection Regulation (GDPR) was the ultimate ‘wake-up call’ for the WBG to initiate a privacy program.
1 Context

2 Where we are

3 Recommended actions

4 Where we want to be
Where we are

• Some WBG policies and processes already address data privacy rights and obligations to some extent: Staff Rules, Information Security, Access to Information, Management of Records.

• WBG Privileges and Immunities reduce risk of legal liability.

• Still, lack of structured governance & awareness, and lack of optimal protection controls, translate into unavailability to fully comply with GDPR and other regulations posing some risks.
WHY DO YOU GET THAT LOOK WHENEVER WE TALK ABOUT GDPR COMPLIANCE?
Steps taken so far

In November 2017, the Bank initiated some actions to estimate risks;

As a first step, an initiative was launched to gather:

- List of IT applications that handle personal data in each WBG unit;
- A Data Privacy Risk Matrix that identifies the types of personal data and the purposes for processing it for the identified applications.

ITS Knowledge and Information - us 🧑‍💻 - has been identified as key stakeholder and involved - thankfully! - in all the activities.

External consultants have been hired to:
(i) assess how Privacy could impact the Bank;
(ii) determine how a WBG Privacy Policy should look like;
(iii) provide an opinion on where the Data Privacy function should sit within the organization;
(iv) suggest an implementation roadmap for the Bank Data Privacy program.

ITSKI also asked the consultants to:
(v) shed some light on GDPR implications for RM/Archives.
1 Context

2 Where we are

3 Recommended actions

4 Where we want to be
External consultants’ assessment: how the GDPR could impact the bank?

- **Business risks**: The flow of personal data to the Bank may be disrupted because partners and others subject to the GDPR might consider themselves unable to lawfully transfer personal data to the Bank.

- **Reputational risks**: The public perception that the Bank does not abide by or respect privacy principles could result in a loss of trust by the Bank’s staff, member country governments, vendors, and/or donors.

- **Legal risks**: - Without a formal, GDPR compliant, privacy framework within the Bank, national courts might not be willing to respect the Bank’s immunities in cases related to data privacy rights.  
  - Staff may already assert claims related to personal data before the Administrative Tribunal, even in absence of a Privacy Policy.
External consultants’ recommendations: where should the data privacy function sit?

- New delegation of authority from the President to the General Counsel for data privacy compliance;

- Independent “Data Privacy Office” (DPO) under the direct authority of the General Counsel with two staff positions;

- Corporate Data Council and Development Data Council to facilitate the design and implementation of the data privacy program – and move to privacy by design;

- Access to Information Committee to assist the DPO in addressing requests from external data subjects and in establishing an appropriate “redress mechanism” in cases where privacy rights are presumed to have been compromised.
Records Management & Archives’ assessment

• As a knowledge organization, the WBG processes personal data for research, statistical and archival purposes, creating records of enduring value for general public interest, transparency, research/historical purposes, etc.

• EU legislators realized the social and political importance of Libraries and Archives and the need to protect them from the general obligations that organizations have under GDPR.

• The GDPR allows EU Member States to introduce derogations or exceptions from certain provisions (rectification, erasure, etc.) or to create supplemental laws to allow for the lawful processing of personal data for such specific processing situations.

• But IOs cannot benefit from such exceptions. Where does that leave us?
Records Management & Archives’ recommendations

To ensure that a GDPR-compliant privacy program does not have a negative effect in the WBG’s ability to process records in the public interest:

⚠️ Consider the processing of personal data for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes as a key legitimate (and primary) processing activity and as an exception, e.g., to the data subjects’ right to erasure of their personal data.

🔒 Ensure that organizational and technical measures are in place, in particular, to comply with the principle of data minimization. Such safeguards could include the pseudonymization or even anonymization of the data, where possible.

读后感 business processes to ensure that the personal data gathered, processed and archived are only the ones actually needed, minimizing as much as possible the personal data becoming part of our collections.
Records Management & Archives’ recommendations

Review policy documents to ensure that they are consistent with the Privacy Policy, specifically:

- The Management of Records policy to take into account the storage limitation and security principles;
- The Access to Information policy to extend the exception set forth in Section III.B.2(a) to cover personal data of external data subjects;
- The Information Classification and Control Policy to take into account personal data and security principles;
- Retention schedules to consider different periods for activities producing records containing personal data.

Apply a balancing test as to whether personal data in historical records can be published:

- Balance is not the same in the access regimes in different EU Member States, although generally privacy rights are strongly protected.
1. Context
2. Where we are
3. Recommended actions
4. Where we want to be
Next steps

BRACE YOURSELF

GDPR IS COMING

here

TODAY!!!
### External consultants’ recommendations: next steps

Implementation plan – critical requirements
(to be implemented within 18-24 months by Data Privacy policy’s owner, the Legal department):

<table>
<thead>
<tr>
<th>Pillar</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Governance</td>
<td>I. Define governance structure supported by adequate resources</td>
</tr>
<tr>
<td></td>
<td>II. Set Policy, Directives and Procedures</td>
</tr>
<tr>
<td>Business</td>
<td>III. Implement Policy, Directives and Procedures</td>
</tr>
<tr>
<td></td>
<td>IV. Develop standard privacy notices and consent forms</td>
</tr>
<tr>
<td></td>
<td>V. Create internal records of data processing activities</td>
</tr>
<tr>
<td></td>
<td>VI. Develop a training program to increase awareness on Data Privacy</td>
</tr>
<tr>
<td>Technology</td>
<td>VII. Implement critical IT controls and “privacy by design”</td>
</tr>
</tbody>
</table>
Thank you!

Paloma Beneito
+1 202 473 2042
pbeneitoarias@worldbankgroup.org

Daniele Balduzzi
+1 202 473 2273
dbalduzzi@worldbankgroup.org