WSGR

Data inventories under the GDPR

Laura De Boel
Senior Associate
Wilson Sonsini Goodrich & Rosati
Agenda

• Introduction.
• Data inventory, DPO & DPIA.
• In practice.
• What’s in it for you?
• Sanctions.
• Q & A.
Introduction
GDPR: Where do we stand?

1995: adoption of the current Data Protection Directive

2012: EU Commission’s proposal for a GDPR

April 2016: adoption of the final text of the GDPR

14 months left to prepare for the GDPR

May 25, 2018: DEADLINE
GDPR will apply in all EU member states
## Getting the terminology right

<table>
<thead>
<tr>
<th>Personal Data</th>
<th>Data Controller</th>
<th>Data Processor</th>
</tr>
</thead>
</table>
| Any information relating to an:  
  - identified  
  or  
  - identifiable individual.  
  As soon as individuals can be singled out (e.g., online identifiers). | The entity that, alone or jointly with others, determines:  
  - the purposes ("why")  
  and  
  - the means ("how") of the data processing. | The entity that processes personal data:  
  - on behalf of and  
  - under the instructions of the controller. |
Goodbye, registrations!
Hello, data inventories!

Data Protection Directive 1995

Obligation for controller to notify data processing to DPAs

GDPR applicable as of May 25, 2018

Obligation to keep a data inventory

Controller

Processor

NEW!
Who is concerned?

- There is a risk for the rights and freedoms of individuals.
- The processing is not occasional.
- Sensitive data is processed (racial origin, religion, sex life, biometric data etc.).
- Data relating to criminal convictions and offences is processed.

Unless...

- Unless organization employs less than 250 persons.
- Unless...

You!

Wilson Sonsini Goodrich & Rosati, LLP
Data inventory, DPO & DPIA
New triangle system

DPIA

DPO

Data inventory
Article 29 WP guidance on DPO (December 2016)

Under Article 30(1) and (2), it is the controller or the processor, not the DPO, who is required to ‘maintain a record of processing operations under its responsibility’ or ‘maintain a record of all categories of processing activities carried out on behalf of a controller’.

In practice, DPOs often create inventories and hold a register of processing operations based on information provided to them by the various departments in their organisation responsible for the processing of personal data. This practice has been established under many current national laws and under the data protection rules applicable to the EU institutions and bodies.37

Article 39(1) provides for a list of tasks that the DPO must have as a minimum. Therefore, nothing prevents the controller or the processor from assigning the DPO with the task of maintaining the record of processing operations under the responsibility of the controller. Such a record should be considered as one of the tools enabling the DPO to perform its tasks of monitoring compliance, informing and advising the controller or the processor.
# Data inventory and DPIA

<table>
<thead>
<tr>
<th>Data inventory</th>
<th>DPIA</th>
</tr>
</thead>
<tbody>
<tr>
<td>• For all processing activities.</td>
<td>• Only for “high risk” processing.</td>
</tr>
<tr>
<td>• For both Controllers and Processors.</td>
<td>• Only for Controllers.</td>
</tr>
<tr>
<td>• Content is limited to description of processing (type of data, purpose etc.).</td>
<td>• Contains an assessment of impact of processing on data protection.</td>
</tr>
<tr>
<td>• Made available to DPA upon request.</td>
<td>• Mandatory prior consultation of DPA if DPIA indicates “high risk” in absence of mitigating measures.</td>
</tr>
</tbody>
</table>
In practice
### Minimum content of a data inventory

#### Data Controller & Data Processor

- **the name and contact details of the controller / processor** (+ if applicable, of the representatives, the joint controller and the DPO).

- where applicable, **transfers of personal data** to third countries, including:
  - which country?
  - documentation of suitable safeguards if the transfer is based on legitimate interests.

- general description of the **technical and organizational security measures** (“where possible”).

<table>
<thead>
<tr>
<th>Data Controller</th>
<th>Data Processor</th>
</tr>
</thead>
</table>
| - **purposes** of the processing.  
- categories of:
  - **data subjects**.  
  - **personal data**.  
  - **recipients**.  
  - **retention periods** ("where possible"). | - name and contact details of **each controller**.  
- **categories of processing** carried out on behalf of each controller. |
Example of an approach to a data inventory

Data Controller

Purpose 1
Data subject category 1
Type of data 1
Type of data 2
Type of data...

Purpose 2
Data subject category 2
Type of data...

Purpose 3
Data subject category...

Purpose...

Retention period | Recipient            | Transfer
-----------------|----------------------|---------
Ex: 1 year       | Ex: Service provider | Ex: U.S.

Retention period | Recipient | Transfer
-----------------|-----------|---------
...              | ...       | ...     

Wilson Sonsini Goodrich & Rosati, LLP
Example of an approach to a data inventory

Company X, address... telephone...

List of HR purposes

Employees

- Identification data (e.g., ...)
- Financial data (e.g., ...)
- Performance data (e.g., ...)

Applicants

Ex-employees

Retention period | Recipient | Transfer | Security measures
--- | --- | --- | ---
Until the end of the employment | HR department, external processor | Transfer to the U.S. based on Privacy Shield | Physical safeguards, password, encryption

Wilson Sonsini Goodrich & Rosati, LLP
In practice

**Preparation:**

- Identify roles & responsibilities within company.
- Prepare data inventory template (in writing, including in electronic form). Consider additional useful data fields (e.g., notice, consent).
- Monitor guidance from Belgian and other DPAs, WP29 / EDPB.

**Getting started:**

- Gather existing resources (e.g., DPA registrations, previously conducted DPIAs) and obtain input from all departments (e.g., audit, questionnaires).
- Complete inventory.

**Keep inventory up-to-date:**

- Implement internal procedures to be informed of any changes / new processing activities.
- Organize trainings for employees.
What’s in it for you?
What’s in it for you? (1/2)

Compliance and accountability

BUT ALSO:

Your data inventory

Your personal organizer, instruction guide, to-do list and calendar

FOR ALL OTHER GDPR OBLIGATIONS
What’s in it for you? (2/2)

Example for a Controller

Data breach

Notification

Within 72h

If “high risk” without undue delay

To be found in your data inventory!

Data subject categories
Personal data categories

DPA

Data subjects

Wilson Sonsini Goodrich & Rosati, LLP
Sanctions
GDPR fines for non-compliance with data inventory requirements

As of May 25, 2018

up to € 10 000 000

or

2 % of the total worldwide annual turnover

of the preceding financial year

(whichever is higher)
Questions?

Thank you!

Laura De Boel
Senior Associate
ldeboel@wsgr.com
WSGR Resources

• WSGR Data Advisor: [www.wsgrdataadvisor.com](http://www.wsgrdataadvisor.com)

• WSGR EU Data Protection Observatory: [www.wsgr.com/EUDataRegulation](http://www.wsgr.com/EUDataRegulation)

• Articles:
  


  – C. Burton, L. De Boel, S. Cadiot, "EU Reaches Milestone Towards the Adoption of Revised Data Protection Framework", WSGR Alert, 15 June 2015