SQUIRE PATTON BOGGS

Maintaining a Record of Data Processing Activities under the GDPR

17 November 2016

Your Speaker

SQUIRE PATTON BOGGS

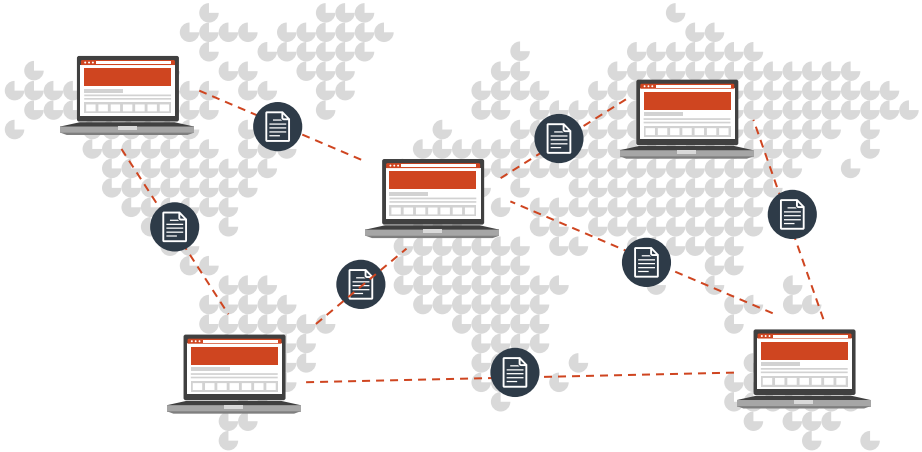
Dr. Annette Demmel, Berlin

Our Need-to-know GDPR Webinars Series

SQUIRE PATTON BOGGS

- First five sessions scheduled:

1. Record of Data Processing Activities
2. Consent and Information - 1 December 2016
3. Privacy Impact Assessments – 15 December 2016
4. Getting Started as a DPO – 12 January 2017
5. Data Breach Response Plan – 26 January 2017



The GDPR (General Data Protection Regulation)

SQUIRE PATTON BOGGS

- 4 May 2016: **Publication**
- 25 May 2016: **Date of entry into force** of the GDPR
- As of 25 May 2018: **Applies** for companies and authorities

Companies that process personal data outside of the EU but also offer their services within the EU are to be subject to Europe's data protection requirements in the future.

Art. 30 GDPR: Records of Processing Activities

SQUIRE PATTON BOGGS

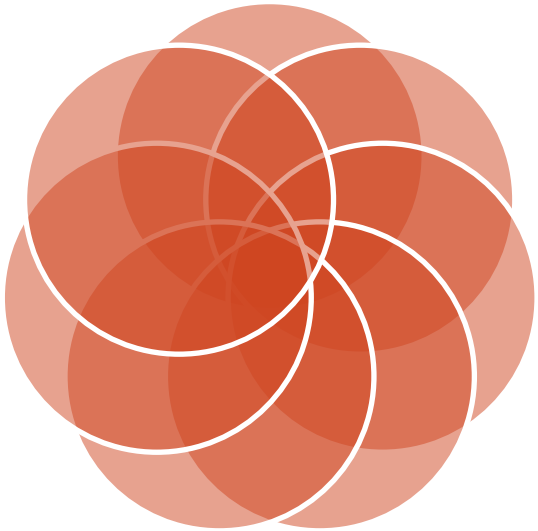
- Art. 30 is prescribing the content of the Record(s)
- Non compliance with Art. 30?
  - Administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher (Art. 83 par. 4 (a) GDPR)

To avoid any confusion…

Other terms for Record of Processing Activities…

Processing Register

Data Flow Chart



Verarbeitungsübersicht
Internes Verfahrensverzeichnis

Processing Operations Index

Data Inventory

Data Mapping

Data Index

In this webinar, we will use the term „Record“.

Who is obliged to maintain a Record?

- Each controller and, where applicable, the controller's representative
- Each processor and, where applicable, the processor's representative

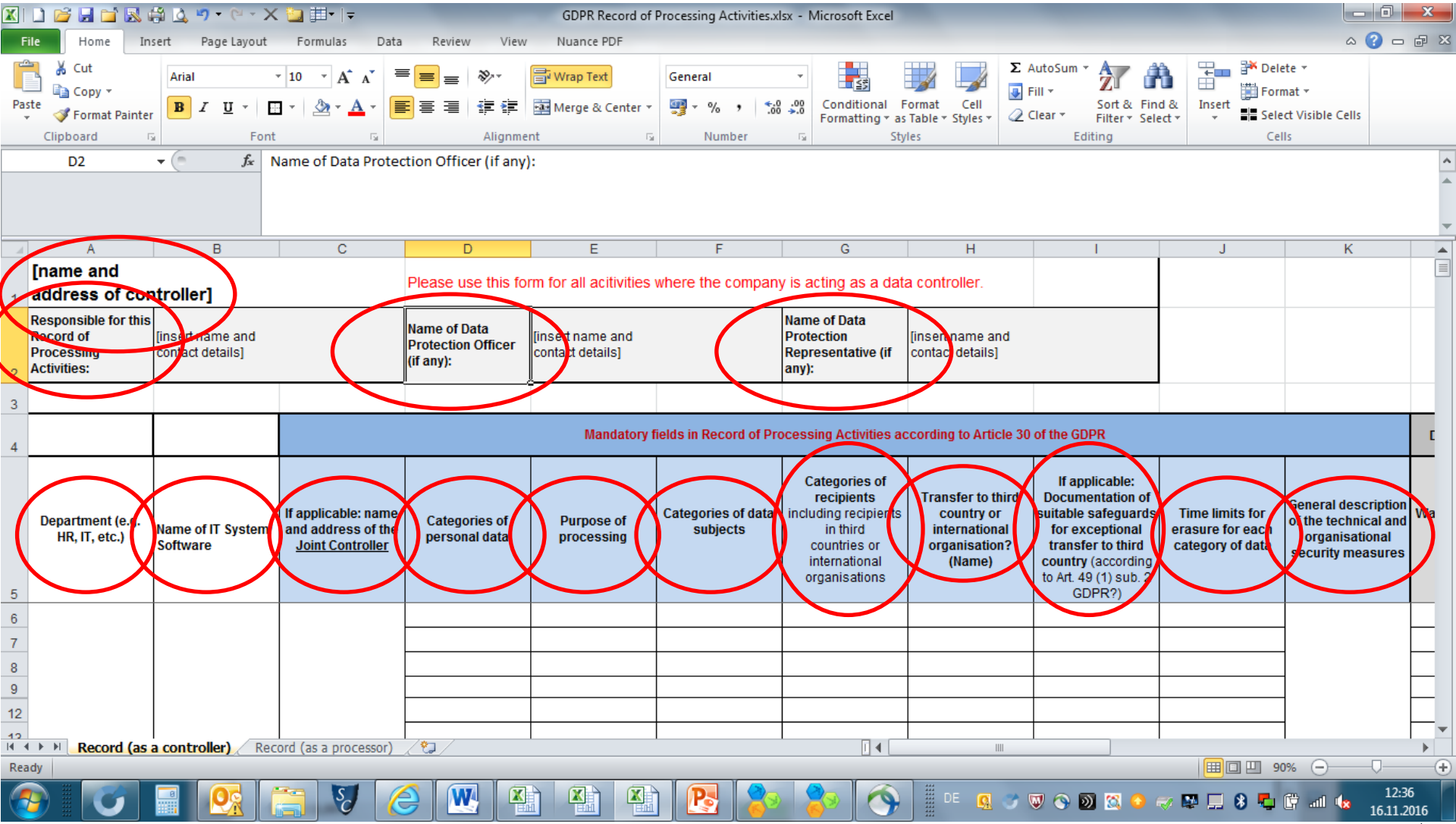
- Exemptions:
- An enterprise or organisation employing fewer than 250 persons **unless**
  - the processing is likely to result in a risk to the rights and freedoms,
  - the processing is not occasional, or
  - the processing includes special categories of data, or criminal convictions and offences

How should a Record look like?

- In writing, including in electronic form
- The 17 (!) German Data Protection Authorities have formed a working group to develop a **Model Processing Operations Index** for Article 30 compliance
- Expected for mid 2017

Content of the Record (Controller)

SQUIRE PATTON BOGGS



Categories of Personal Data – a few examples

SQUIRE PATTON BOGGS

- Employee data, such as:
  - name, job title, birth date, passport data, private address, private telephone number, private email address, emergency contact, employee number, status (active or not), birth date, department ID, name of department, supervisor ID, name of supervisor, work location, days of absence and cause, holiday entitlement
  - education details, CV, work history with the firm, working hours (full or flex time)
  - performance data, compensation data, payroll data, bank account data
  - credit card data, transaction data from credit cards,
  - frequent flyer program data, travelling preferences (window seat or aisle seat), driving license data

- Customer data, such as:
  - Name, address, telephone number, email address, contractual details, contract history, etc.

Purpose of processing – a few examples

SQUIRE PATTON BOGGS

- Some short examples:
  - Employee administration
  - Employee management
  - Ethics and compliance trainings for employees
  - Supplier screening
  - Travel administration
  - IT administration
- A detailed example (a relocation service):
  - temporary living coordination, global immigration services, expense administration, home marketing assistance, property management, cross cultural training, language training, household goods move management, destination services including home search and school search, educational counselling, financial services coordination, travel coordination, family transition assistance, pet transport, furniture rental coordination, host transportation coordination, security briefing coordination, emergency and evacuation services, etc.

Categories of Data Subjects – a few examples

SQUIRE PATTON BOGGS

- Current and former employees, job candidates, employee emergency contact person, trainees
- Shift workers, sales employees, field staff, HR administration staff in location xyz
- Employees holding corporate credit cards
- Customers, suppliers
- Study participants, call center agents
- University employees, external lecturers, students

Categories of Recipients

SQUIRE PATTON BOGGS

- Recipient means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.
- Exemption:
  - Public authorities which may receive personal data in the course of a particular inquiry in accordance with EU or Member State law shall not be regarded as recipients

⇒ List all categories of people who have acces to the data

⇒ Do it for each category of data separate, if there is a distinction

- Examples:
- Officers/directors, HR manager, HR administration staff, IT administrators, application developers, external IT maintenance company, facility management staff, department xyz, etc. ⇦

⇒ Mark recipients in a third country or international organisation

Suitable Guarantees for Exceptional Transfer

SQUIRE PATTON BOGGS

- Following Art. 49 (1) subpar. 2 GDPR the transfer without adequate safeguards is only permissable if
  - it is not repetitive,
  - concerns only a limited number of data subjects,
  - is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and
  - the controller has assessed all the circumstances surrounding the data transfer and
  - the controller has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data.
- The Authority must be informed of such transfer.

Time limits for erasure of each category

- How to handle for comprehensive list of data categories?
- How to handle for different countries?
- Refer to retention schedule?
  - GDPR: *„where possible, the envisaged time limits for erasure of the different categories of data"*

Technical and organisational measures

SQUIRE PATTON BOGGS

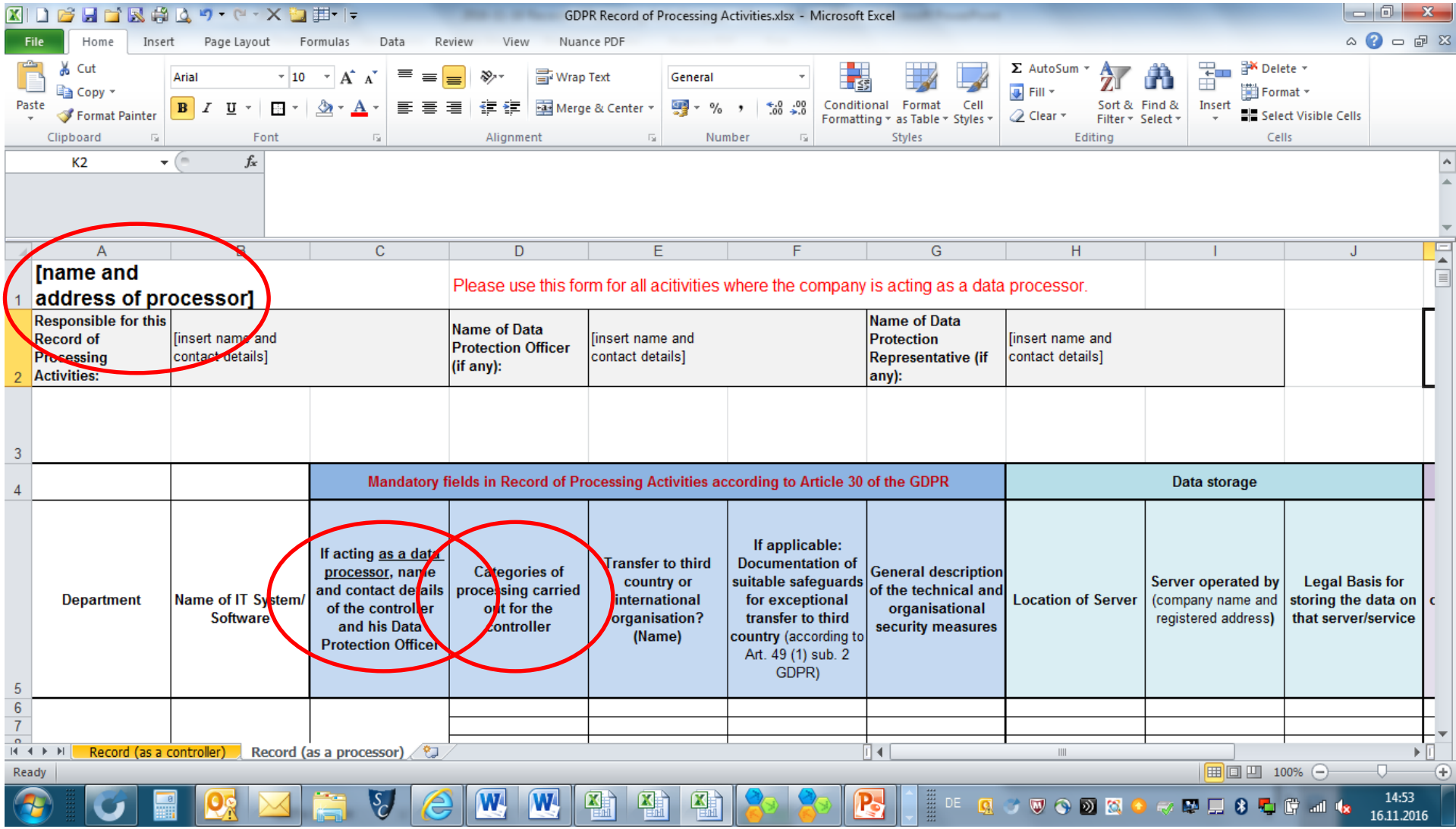
- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing

- Refer to a security concept?

- GDPR: *"where possible, a general description of the technical and organisational security measures"*

Content of Record (Processor)

SQUIRE PATTON BOGGS



GDPR Record of Processing Activities.xlsx - Microsoft Excel

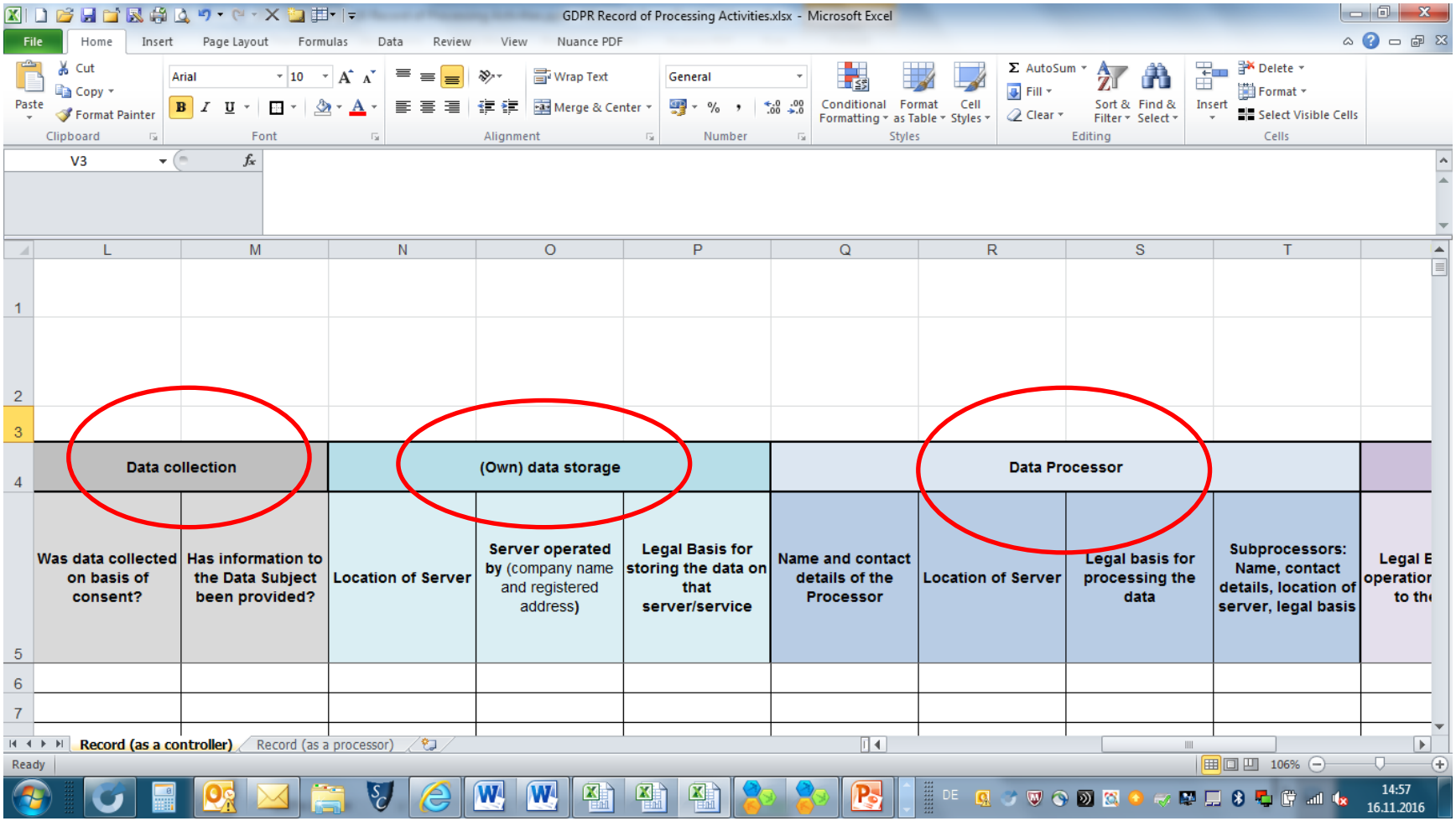
	A	B	C	D	E	F	G	H	I	J
1	[name and address of processor]			Please use this form for all acitivities where the company is acting as a data processor.						
2	Responsible for this Record of Processing Activities:	[insert name and contact details]		Name of Data Protection Officer (if any):	[insert name and contact details]		Name of Data Protection Representative (if any):	[insert name and contact details]		
3										
4			Mandatory fields in Record of Processing Activities according to Article 30 of the GDPR					Data storage		
5	Department	Name of IT System/ Software	If acting as a data processor, name and contact details of the controller and his Data Protection Officer	Categories of processing carried out for the controller	Transfer to third country or international organisation? (Name)	If applicable: Documentation of suitable safeguards for exceptional transfer to third country (according to Art. 49 (1) sub. 2 GDPR)	General description of the technical and organisational security measures	Location of Server	Server operated by (company name and registered address)	Legal Basis for storing the data on that server/service
6										
7										

Record (as a controller) | Record (as a processor)

Ready

Useful other information to include into the Record

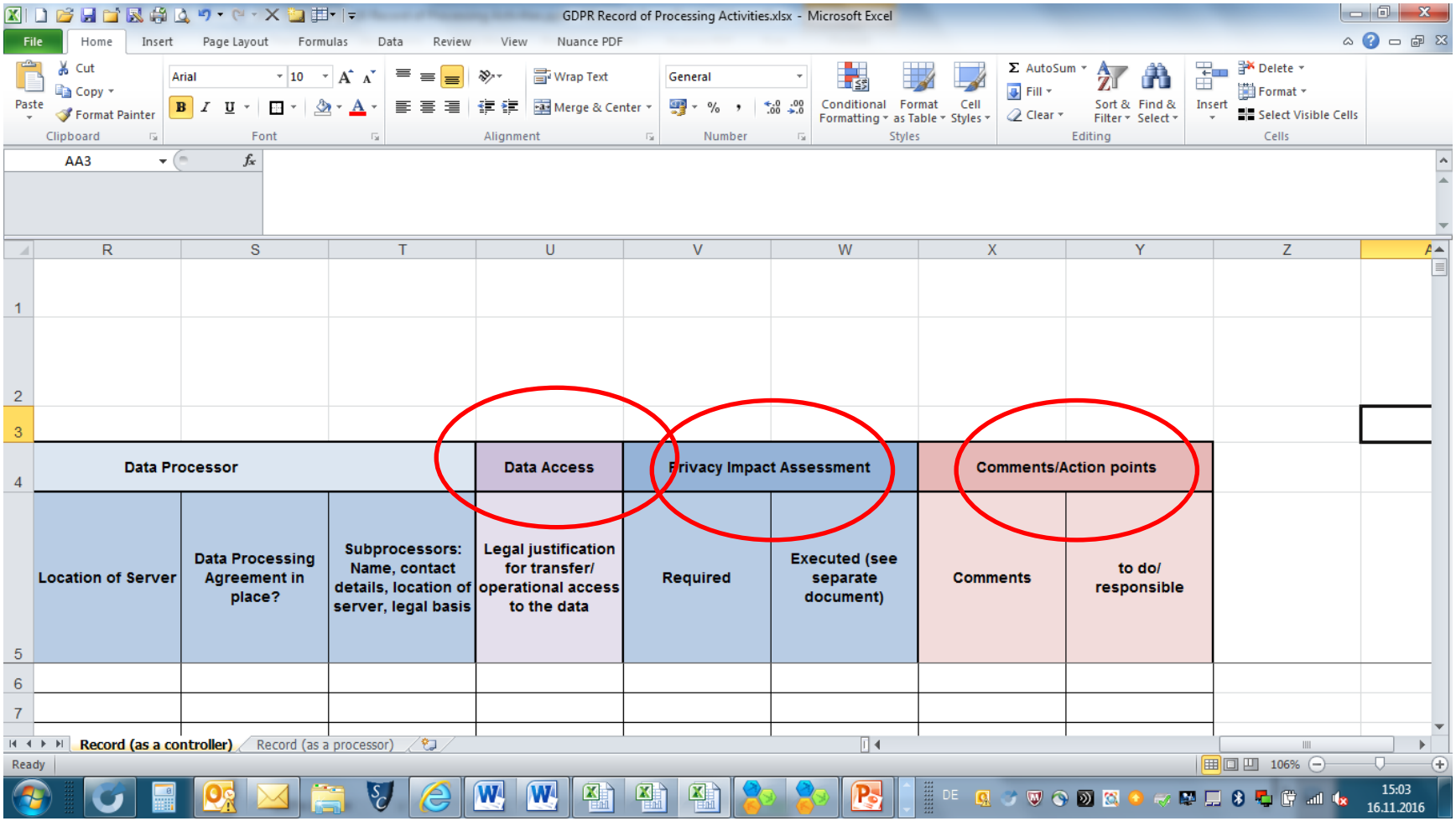
SQUIRE PATTON BOGGS



Data collection		(Own) data storage			Data Processor				
Was data collected on basis of consent?	Has information to the Data Subject been provided?	Location of Server	Server operated by (company name and registered address)	Legal Basis for storing the data on that server/service	Name and contact details of the Processor	Location of Server	Legal basis for processing the data	Subprocessors: Name, contact details, location of server, legal basis	Legal E operatior to th

Useful other information to include into the Record, cont.

SQUIRE PATTON BOGGS



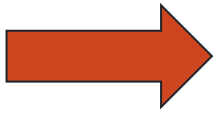
Data Processor			Data Access	Privacy Impact Assessment		Comments/Action points	
Location of Server	Data Processing Agreement in place?	Subprocessors: Name, contact details, location of server, legal basis	Legal justification for transfer/ operational access to the data	Required	Executed (see separate document)	Comments	to do/ responsible

How to manage to collect all the information…

SQUIRE PATTON BOGGS

… and maintain the Record up to date?

- Define responsibilites in the various departments
- Give the department a simple document at hand where new processes have to be documented
- Implement a process in each department for collecting information on changes/updates
- Organize regular calls/in-person meetings with the responsible people
- Insist



Never stop working on the Record

SQUIRE PATTON BOGGS

Questions and Answers

Thank you!

SQUIRE PATTON BOGGS

Dr. Annette Demmel

Partner
Rechtsanwältin
Certified Specialist for Information Technology Law
Certified Specialist for Copyright and Media Law

annette.demmel@squirepb.com