SQUIRE PATTON BOGGS

Prepare and Conduct an Internal Privacy Audit

May 6, 2020

The content of this webinar is for information purposes only and is not intended to serve as legal advice, nor should it be regarded as a substitute for taking legal advice or be construed as Squire Patton Boggs providing legal advice.

Your Speakers

Dr. Annette Demmel,
Berlin

Mareike Lucht,
Berlin

Content

SQUIRE PATTON BOGGS

General	What is a privacy audit and why is it necessary?
	Who needs to conduct one?
	When is an audit necessary?
How to …	The Plan, the auditor, the team
	Audit by topics, by goals or by processes?
	Close gaps at short notice

What is a privacy audit?

It is not a procedure that is formally prescribed in details in the GDPR. It is a check.

- Do we have … in place?
- Have we considered ...?
- Are we able to prove…?
- Have we carried out …?
- Is there a control for…?
- Have we organized…?
- Are we documenting….?
- Have we tested…?
- Have we finished…?

Why is it necessary?

- To ensure regulatory compliance
- To detect weakness
- As a selling point

Art. 5 GDPR
The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).

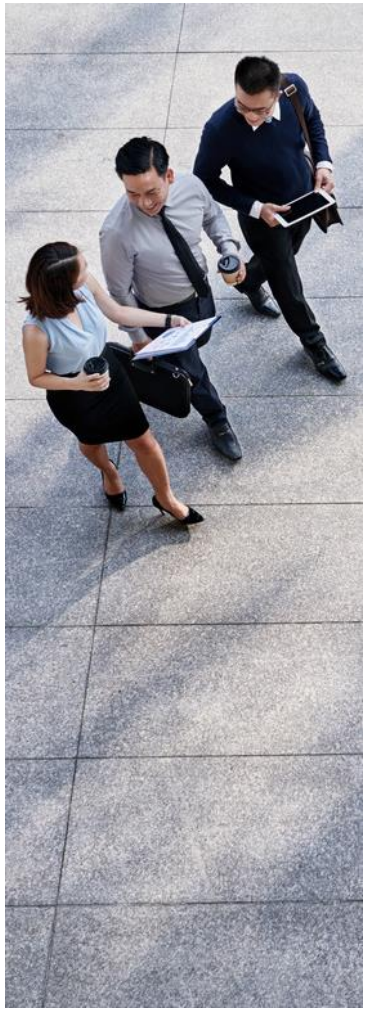
(… meaning the lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation of the processing)

Art. 32 GDPR
[…] the controller and the processor shall implement […] a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Who needs to conduct a privacy audit?

- Controllers
- Processors
- AND:

  Shareholders and Stakeholders may wish to conduct one (often with a particular focus)



When to conduct a privacy audit?

Time of conducting it?

Now

(after already 2 years of GDPR)

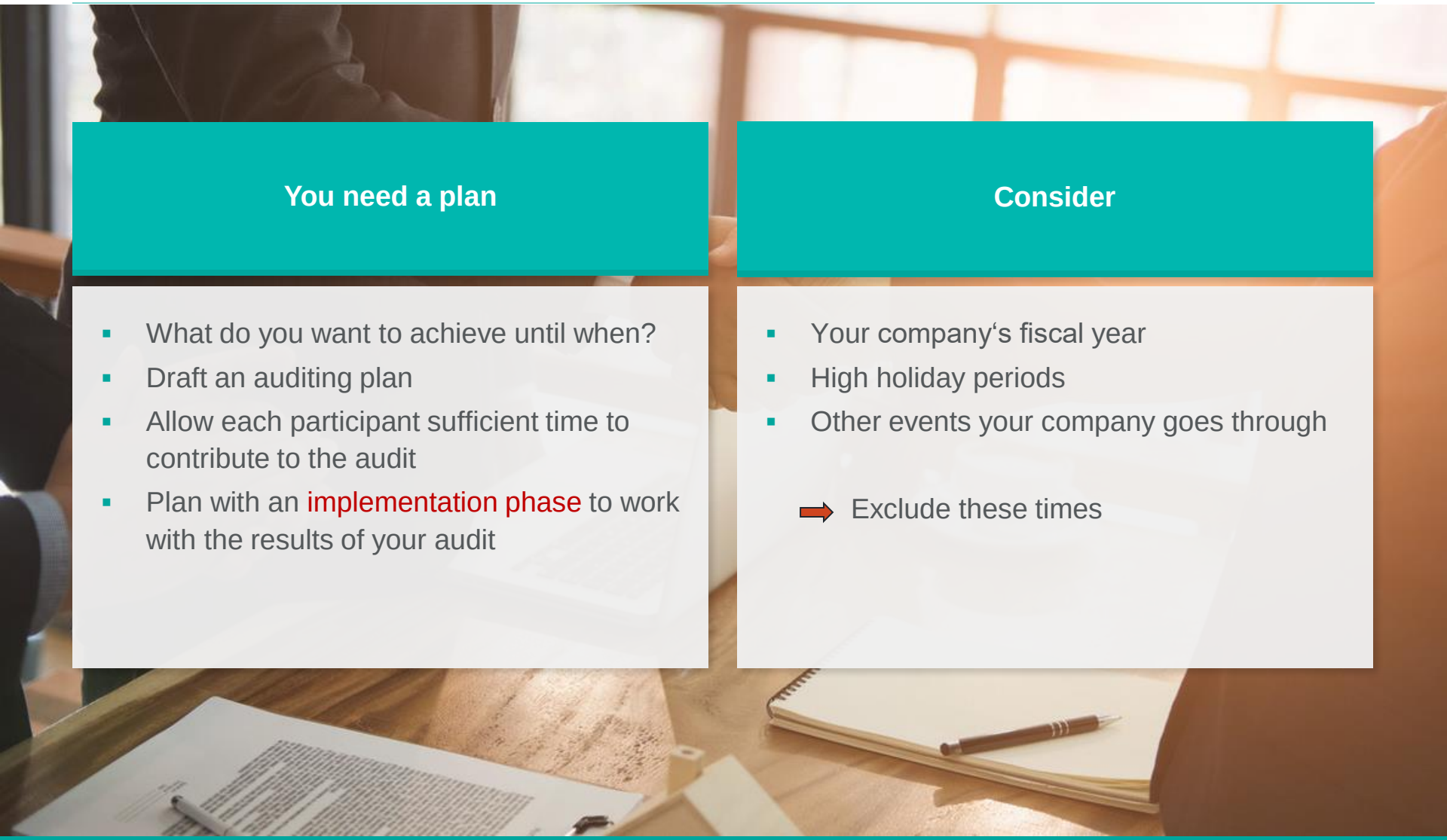
How **often** to conduct it?

Plan for every 1/1,5 years for general audits
Depending on the audit focus, plan several special audits
Important: Find a proper audit interval to generate benefit for the company and do not make it a solely burdensome exercise

AND: Conduct an audit after an incident or if you need to investigate certain processes.

How to… – the Plan

SQUIRE PATTON BOGGS



You need a plan

- What do you want to achieve until when?
- Draft an auditing plan
- Allow each participant sufficient time to contribute to the audit
- Plan with an implementation phase to work with the results of your audit

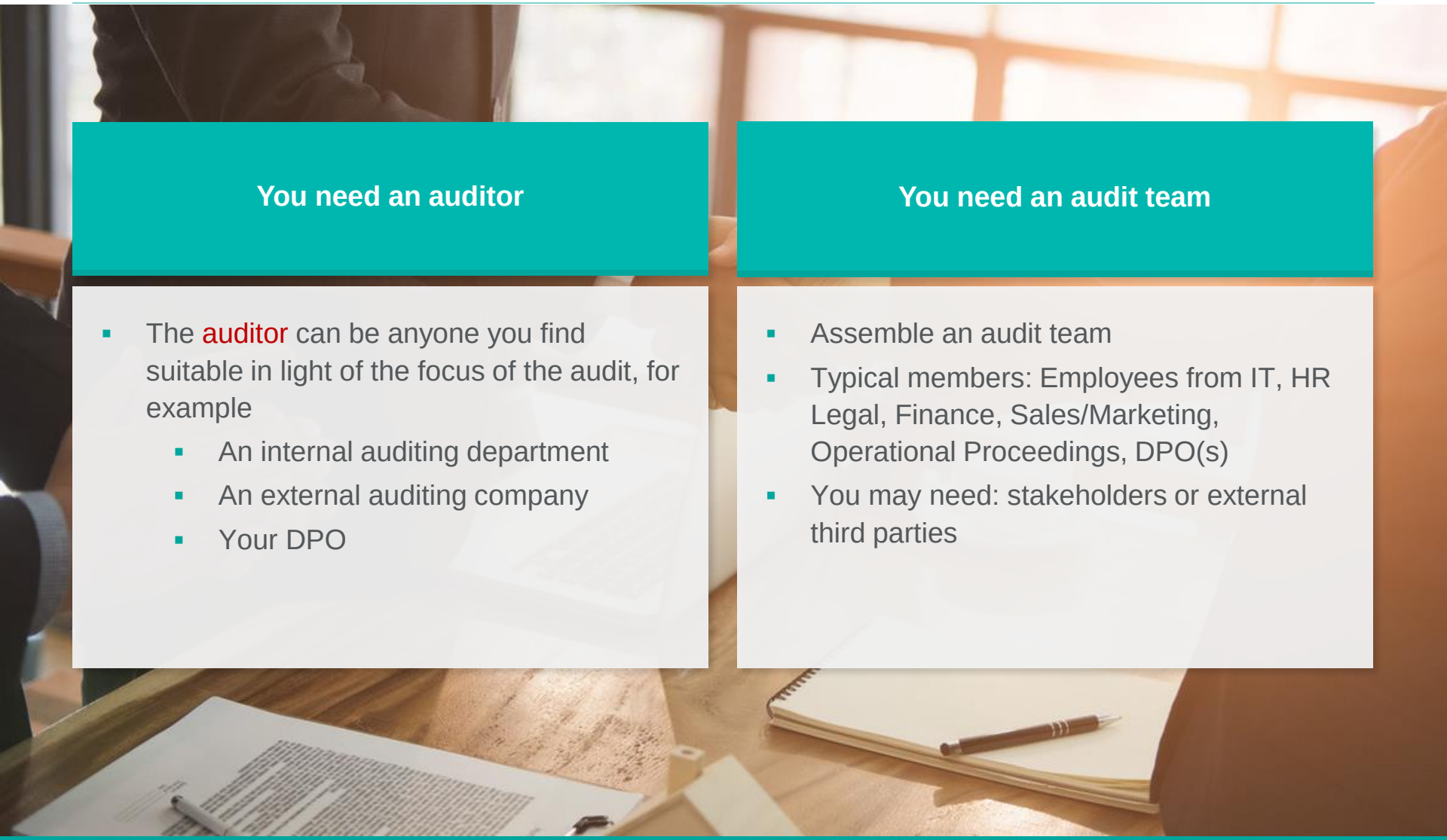
Consider

- Your company‘s fiscal year
- High holiday periods
- Other events your company goes through

➡ Exclude these times

How to… – the Auditor and the Team

SQUIRE PATTON BOGGS



You need an auditor

- The auditor can be anyone you find suitable in light of the focus of the audit, for example
  - An internal auditing department
  - An external auditing company
  - Your DPO

You need an audit team

- Assemble an audit team
- Typical members: Employees from IT, HR Legal, Finance, Sales/Marketing, Operational Proceedings, DPO(s)
- You may need: stakeholders or external third parties

How to… - the Focus of the Audit

SQUIRE PATTON BOGGS

Audit by topics

Audit by goals

Audit by processing

How to… - Audit by Topics (examples)

SQUIRE PATTON BOGGS

- Data Protection Officer
- Lawfulness of processing
- Processing Register
- Privacy by Design and by Default
- Technical and Organisational Measures
- Deletion Concept
- Rights of Data Subjects
- Data Breach Responsiveness
- Data Processing Agreements
- Data Transfers

How to… - Audit by Goals (examples)

SQUIRE PATTON BOGGS

Data Minimisation

Prevent unsolicited marketing mails

Regular updates of the ROPA

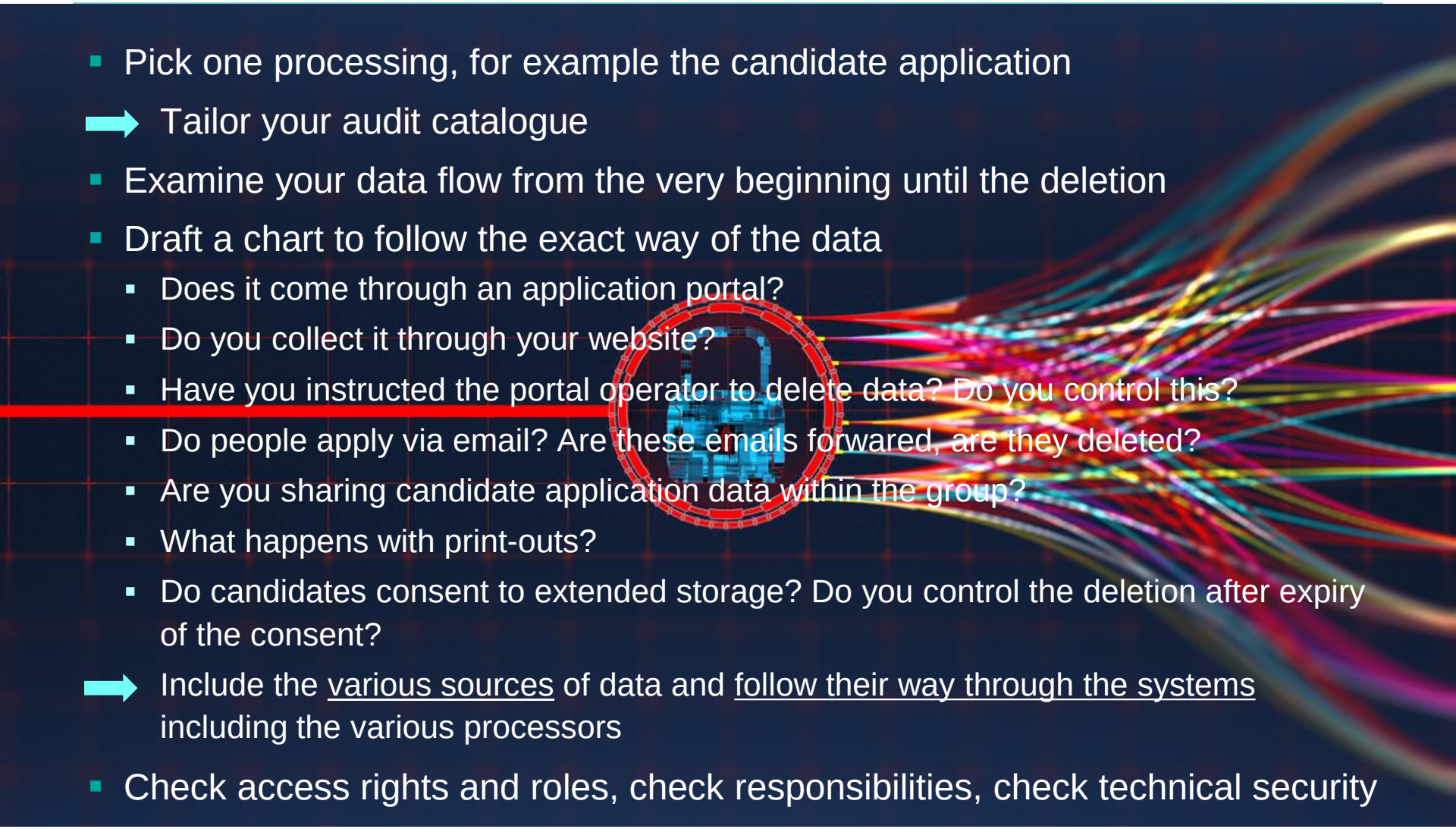
Detect old databases

Security of Passwords

Prepare the sale of the company

How to… - Audit by Processings (examples)

SQUIRE PATTON BOGGS



- Pick one processing, for example the candidate application

➡ Tailor your audit catalogue

- Examine your data flow from the very beginning until the deletion
- Draft a chart to follow the exact way of the data
  - Does it come through an application portal?
  - Do you collect it through your website?
  - Have you instructed the portal operator to delete data? Do you control this?
  - Do people apply via email? Are these emails forwared, are they deleted?
  - Are you sharing candidate application data within the group?
  - What happens with print-outs?
  - Do candidates consent to extended storage? Do you control the deletion after expiry of the consent?

➡ Include the various sources of data and follow their way through the systems including the various processors

- Check access rights and roles, check responsibilities, check technical security

How to… - Close gaps at short notice

- Prioritize the gaps in A, B, C

- Escalate within the firm
  - Escalation might provide you with more resource
  - Escalation will give the Directors the chance to react
  - Escalation will stress the importance of privacy compliance

- For A-gaps, don‘t wait for a smart solution but improvise
  - Don‘t look for volunteers to take a task, determine someone

- Schedule regular working sessions/calls to implement the results BUT

Try to be simple in implementation.

Strategies that are too ambitious will end up at a 25-40% implementation quote.

SQUIRE PATTON BOGGS

Questions and Answers

Thank you!

Dr. Annette Demmel

Partner, Berlin

Rechtsanwältin

Certified Specialist for Information Technology Law

Certified Specialist for Copyright and Media Law

T +49 30 72616 8226

E annette.demmel@squirepb.com

Mareike Lucht, LL.M.

Associate, Berlin

Rechtsanwältin

Attorney at Law, New York

T +49 30 72616 8131

E mareike.lucht@squirepb.com

Berlin

Unter den Linden 14
10117 Berlin
T +49 30 72616 8000

Frankfurt am Main

Eurotheum
Neue Mainzer Straße 66-68
60311 Frankfurt am Main
T +49 69 1739 2400

Böblingen (Stuttgart)

Herrenberger Straße 12
71032 Böblingen
T +49 7031 439 9600