5 STEPS TOWARDS GDPR COMPLIANCY IN PRACTICE

Pekka Vepsäläinen
Tikkasec Ltd

Speaker Background

- Pekka Vepsäläinen – Tikkasec Ltd
- Information Security part of my job since 2001 (Nokia smartphone projects)
- Privacy became a matter of interest when working as Global Head of Competence Development at Teleca (2010-2012)
- Cyber Security studies at Jyväskylä University (2012-2014)
- Cyber Security Development Manager at Jykes Ltd (2012-2017)
- Entrepreneur since 2017 – Cyber Security and GDPR consulting & coaching

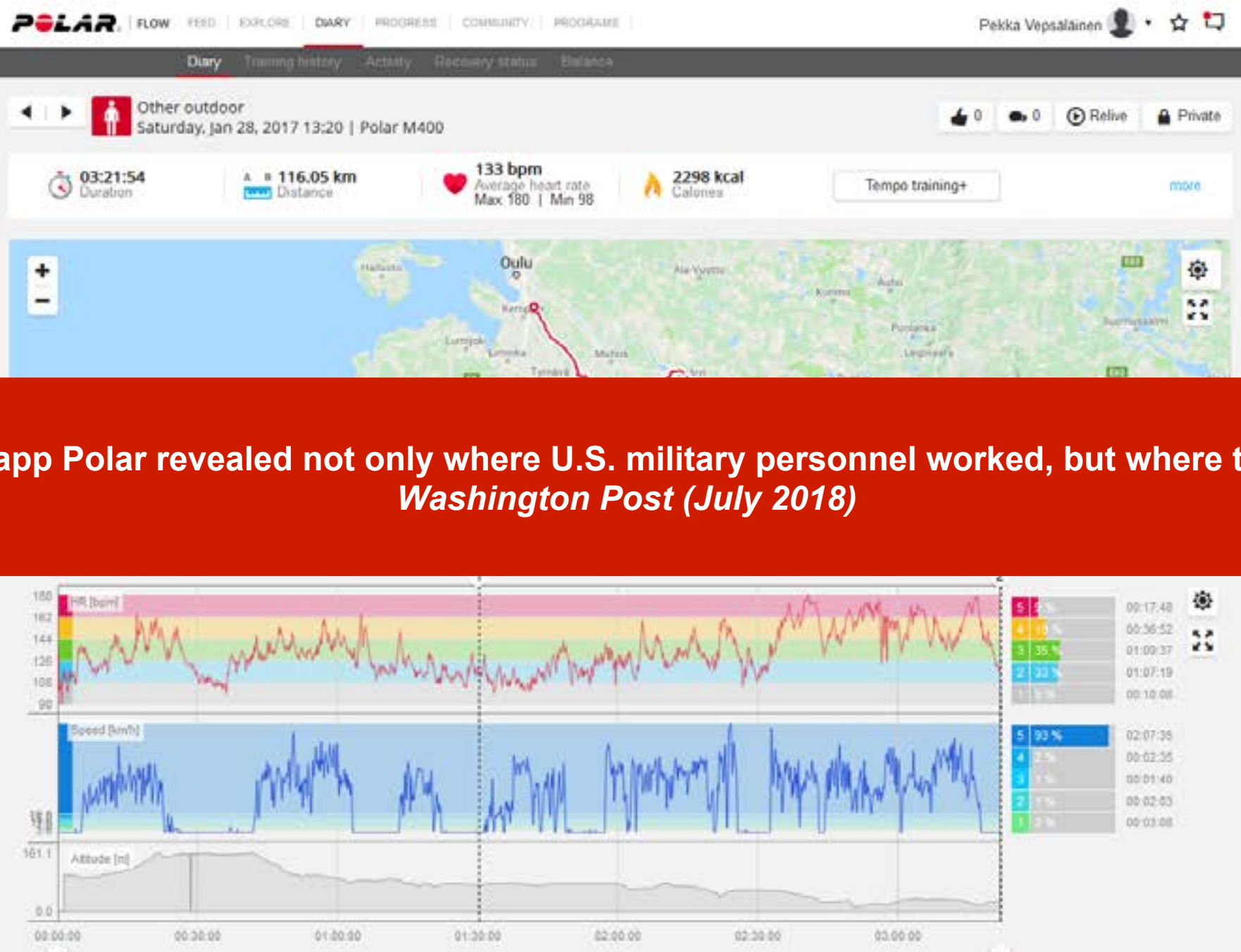
Contents

Some background & basics about GDPR

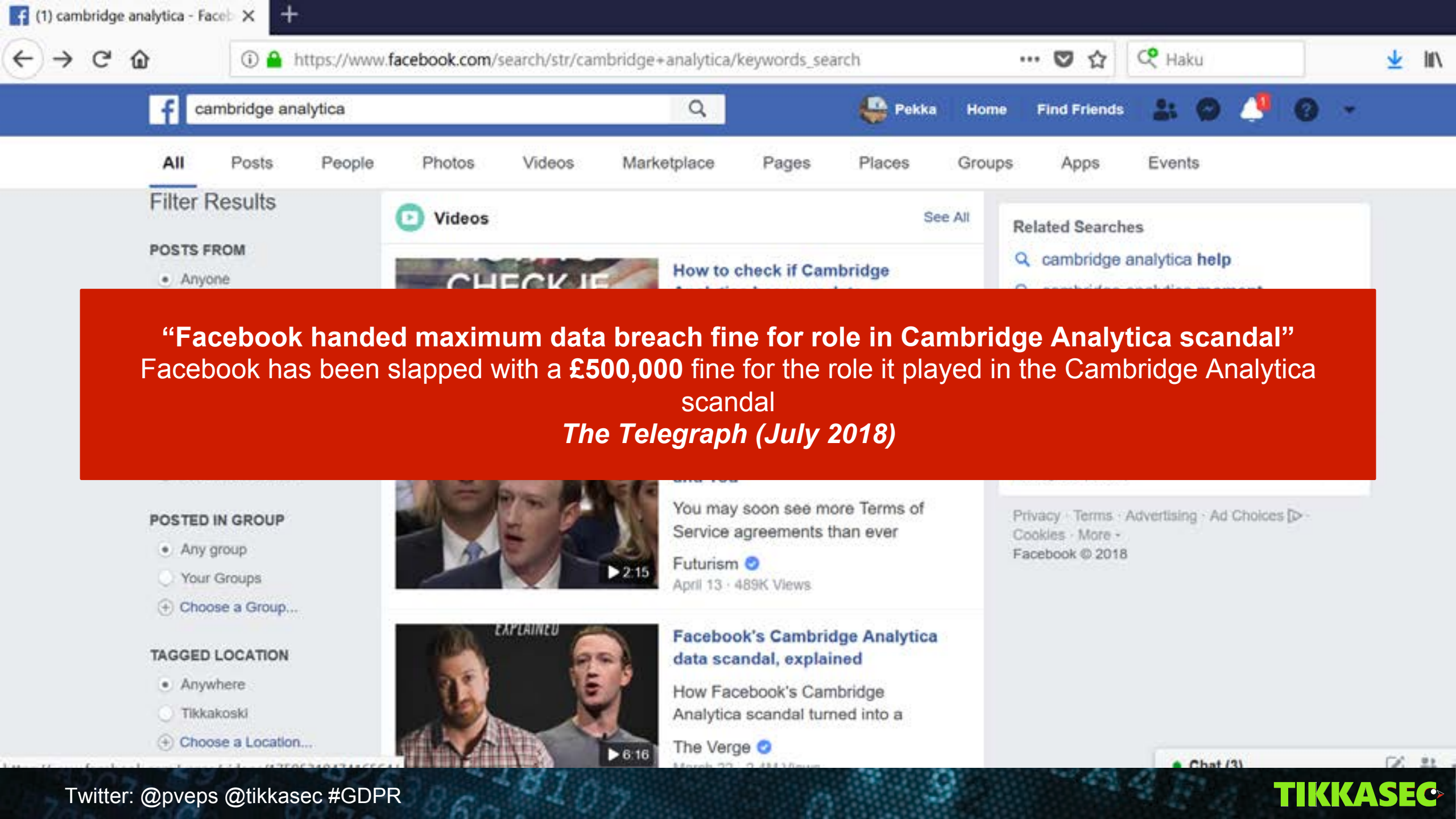
5 Steps Towards GDPR Compliancy in Practice

1. Board room awareness & privacy task force
2. Data inventory – where is all the personal data?
3. Risk assessment – what are the TOP risks to manage?
4. Executing GDPR action plan – from data security to data requests
5. Preparing required documents & contracts


CHALLENGE



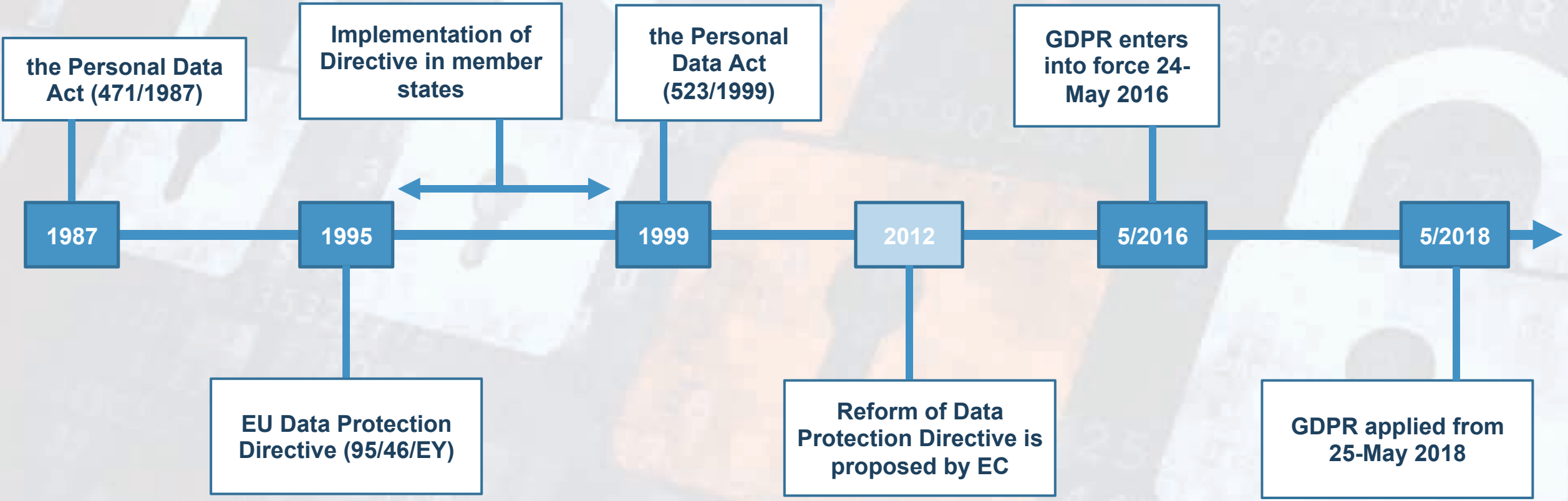
“Fitness app Polar revealed not only where U.S. military personnel worked, but where they lived”
Washington Post (July 2018)


(1) cambridge analytica - Faceb
https://www.facebook.com/search/str/cambridge+analytica/keywords_search
Haku
cambridge analytica
Pekka
Home
Find Friends
All
Posts
People
Photos
Videos
Marketplace
Pages
Places
Groups
Apps
Events
Filter Results
POSTS FROM
Anyone
Videos
See All
How to check if Cambridge
Related Searches
cambridge analytica help
“Facebook handed maximum data breach fine for role in Cambridge Analytica scandal”
Facebook has been slapped with a £500,000 fine for the role it played in the Cambridge Analytica scandal
The Telegraph (July 2018)
POSTED IN GROUP
Any group
Your Groups
Choose a Group...
You may soon see more Terms of Service agreements than ever
Futurism
April 13 · 489K Views
2:15
Privacy · Terms · Advertising · Ad Choices
Cookies · More
Facebook © 2018
TAGGED LOCATION
Anywhere
Tikkakoski
Choose a Location...
EXPLAINED
Facebook's Cambridge Analytica data scandal, explained
How Facebook's Cambridge Analytica scandal turned into a
The Verge
6:16
Chat (3)

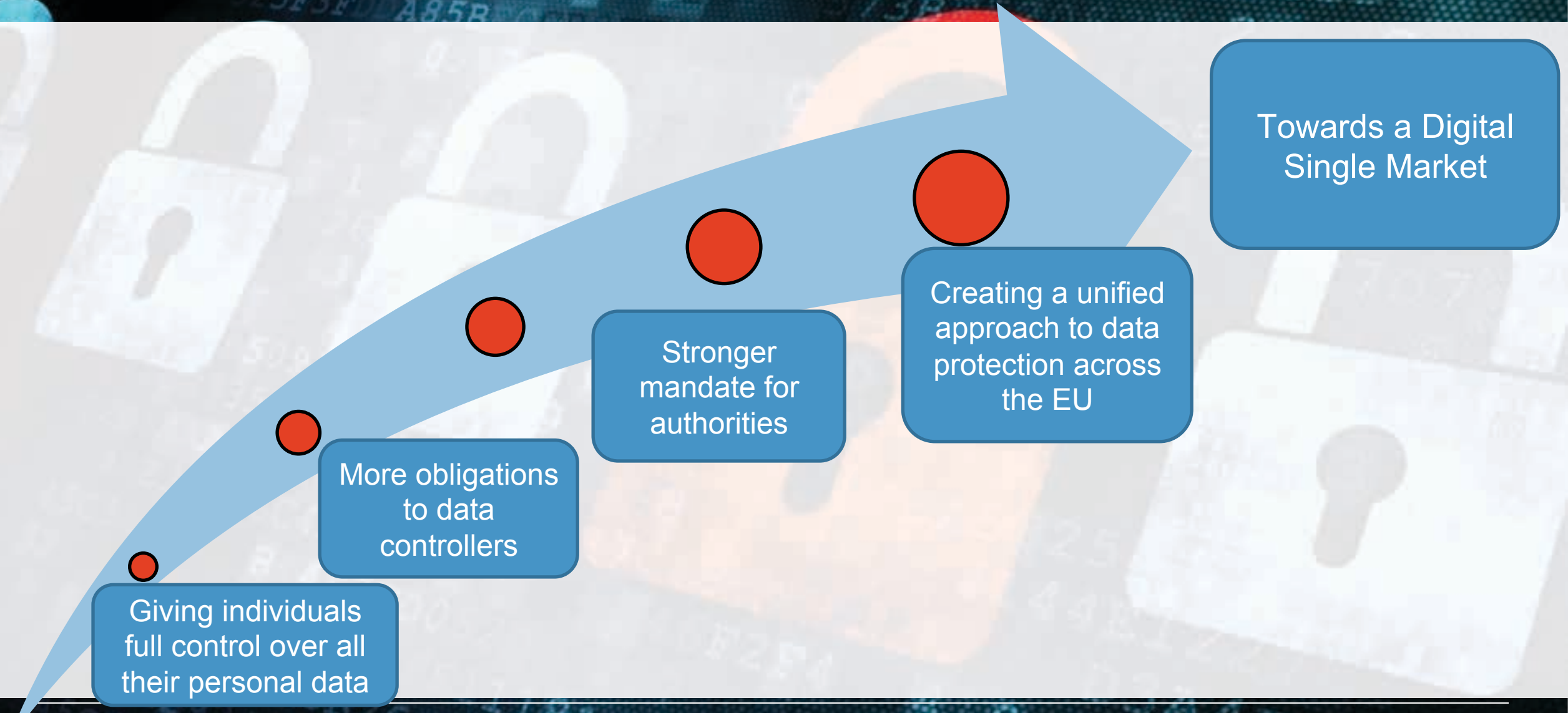
“Google to shut down Google+ after failing to disclose user data breach”
The Guardian (October 2018)

“U.S., European regulators investigating Google glitch”
Reuters (October 2018)

History of privacy regulation in Finland / EU



GDPR Objectives

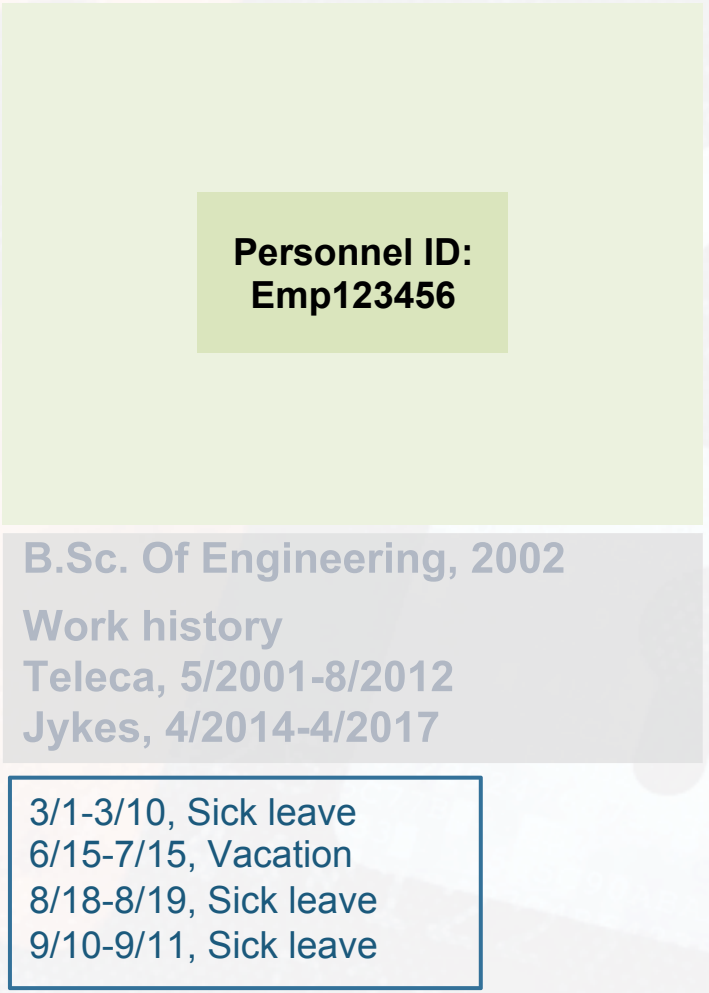


SOME KEY FACTS ABOUT GDPR

GDPR widens the definition of Personal Information

PII (USA) vs. Personal Data (EU)??

- **NIST**: PII is distinguishing individual identity
- **European Commission:** Personal data is "**any information that relates** to an identified or identifiable living individual"
- So in this case Personal Data = PII + any other information related to such a person



Data Controller vs. Data Processor

- Data Controller - determines the **purposes and means** of the processing of personal data
- Data Processor - processes personal data on behalf of the controller

Clarify your role – sometimes it's data controller, sometimes data processor even within the same application!

- E.g. Facebook is a data controller for private users but in some cases data processor for your company's followers' data

Basic **principles for the processing of personal data**

1. Personal data shall be:
   a) Processed **lawfully**, **fairly** and in a **transparent manner**
   b) Collected for **specified**, **explicit** and **legitimate purposes**
   c) Adequate, **relevant** and **limited** to what is necessary
   d) Accurate and, where necessary, **up to date**
   e) Identification of data subjects for **no longer than is necessary**
   f) Processed in a manner that **ensures appropriate security** of the personal data
2. The controller shall be responsible for, and be **able to demonstrate** compliance with, paragraph 1 -> ”**accountability**”

(GDPR Article 5)

Lawfulness of data processing

1. Data subject has **given consent** to the processing
2. For the **performance of a contract**
3. For **compliance with a legal obligations**
4. To **protect the vital interests** of the data
5. Carried out in the **public interest** or in the exercise of **official authority**
6. For the purposes of the **legitimate interests** pursued by the controller or third party

Some key rights of the data subjects

- **Transparency** of data processing – privacy notices
- **Information** and **access to personal data**
- Right to erasure – **'right to be forgotten**'
- Right to **object marketing** and **profiling**

Data breach notifications

- Data breach notification window is only **72 hours**
  - Clock starts ticking when the data breach has been detected
- You have to be able to detect & then react real fast
- It’s not only about Cyber Attacks – human errors & bugs are counted too!

Do you have your processes in place and have you practiced them?

Some myths about GDPR

- Consent is always needed from data subjects – not true
- Data is always needed to delete after request from data subject – not true
- Right to data portability is always applied – not true

1. BOARD ROOM AWARENESS & PRIVACY TASK FORCE

Some challenges & risks

- Huge fines if things go wrong
  - “Under Germany’s old data protection law, Google would be fined a maximum of 300,000 Euros. However, GDPR would fine a company up to **4 percent of its annual global turnover**. ” – *interestinengineering.com (October 2018)*
- But it’s not only about the fines – **your company’s reputation is at stake**
- Are there some other risks?
  - Blackmailing by Cyber Attackers: ”Pay me or I’ll report to authorities”
  - “Be Prepared – The German DPAs will start random GDPR audits” – *globalcompliancenews.com (October 2018)*

Commitment of Board Room

- Any company that works with information relating to EU citizens will have to comply with the requirements of the GDPR
  - If GDPR is not yet on your board room's agenda, do it now
- But this can be a competitive advantage too!
- What is your **strategy towards GDPR?**
  - Some U.S. Companies have selected NOT to offer services to EU citizens anymore
  - OR you may take it seriously and grow your business within the EU

Set up Privacy Task Force

- It's not just an IT issue, it's **a cultural change**
  - Get your personnel committed to the change – include them in the project

- Set up a **privacy task force:**

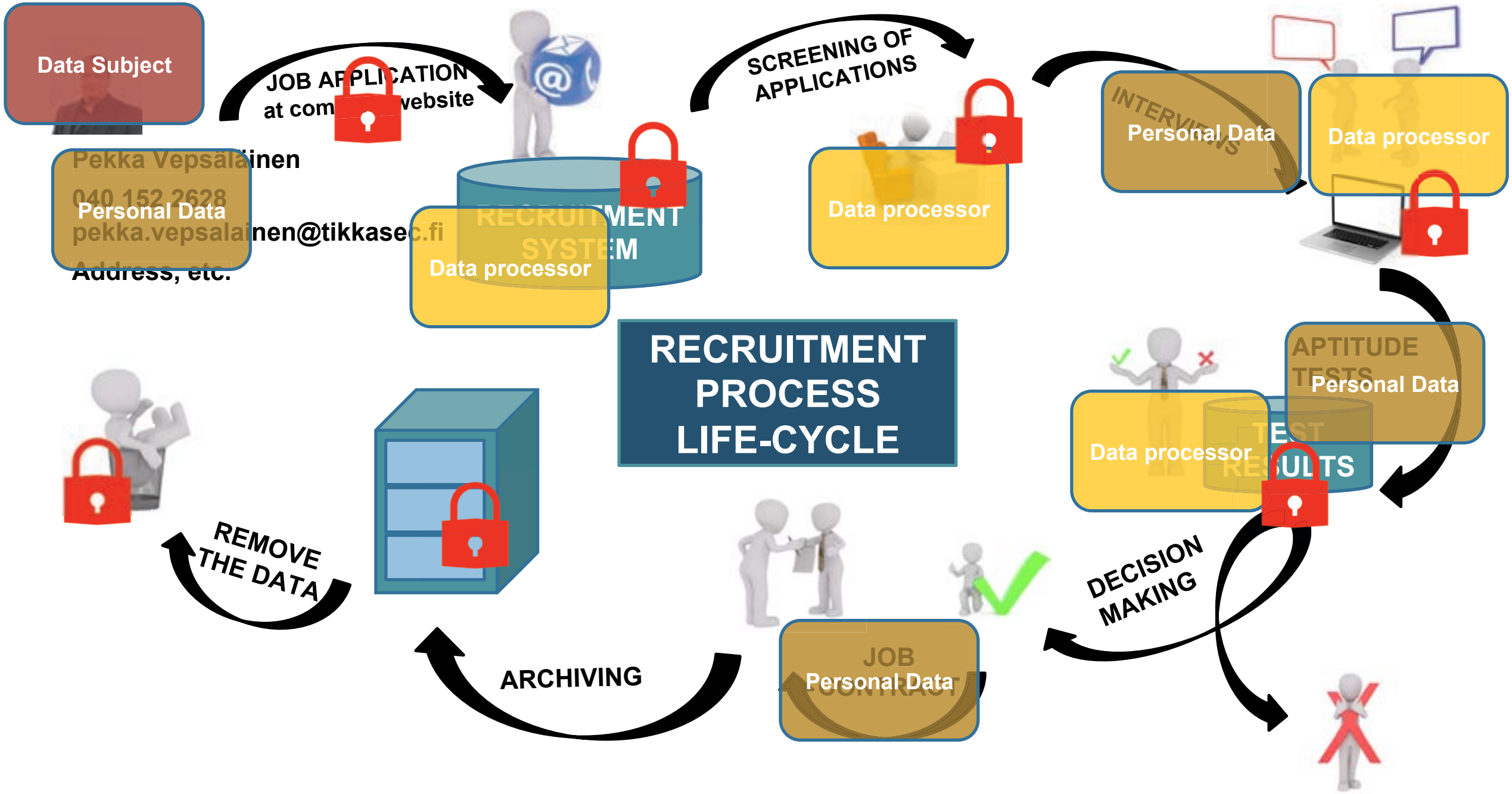
1. DPO to lead the task force
2. Include relevant business directors – they define the purposes of data processing!
3. Include people at the grassroots level – they know how the data is processed in practice!
4. Include your contract lawyers – you need to work on the contracts too

2. DATA INVENTORY – WHERE IS ALL THE PERSONAL DATA?

Data inventory

- What and how personal data is processed? In which filing/information systems?
- Who has access to the data in different phases of **personal data life cycle** – from data capture to archiving and removal? How long do you store the data?
- Roles of internal and external parties: data controller vs. data processor + subcontractors
- Identify special categories of personal data processed
- How are data subjects' rights and other GDPR requirements implemented in different data processing activities?

RECRUITMENT PROCESS LIFE-CYCLE



3. RISK ASSESSMENT – WHAT ARE THE TOP RISKS TO MANAGE?

GDPR Risk Assessment

- DPIA (Data Protection Impact Analysis)
  - Must be done for high risk data processing activities
- Risk assessment workshop
  - To identify pitfalls of data processing, especially when processing special categories of personal data or larger amounts of data
  - Internal and external threats, both technical and organizational
  - Information systems, data processors, subcontractors
- Depending on what kind of personal data is processed, you need to take different actions
  - Example: B2B contact information vs. employee health information

Data Protection is a Risk Management activity

- Data protection should be implemented based on identified risks!
  - Put effort & money where it's really needed
  - GDPR also recognizes the costs of implementation + you can't have 100% security

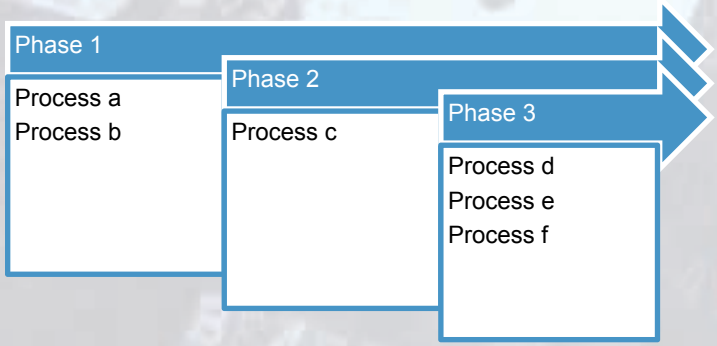
RISK ASSESSMENT

- **Identify the risks** that may have impact to personal data protection
- **Analyze the risks:** determine the likelihood and consequence of each risk
- **Evaluate or rank the risks:** Risk magnitude is combination of likelihood and consequence. Make decisions about whether the risk is acceptable or whether it needs treatment activities.
- **Treat the risks.** Create a plan to treat or modify these risks to achieve acceptable risk levels.
- **Monitor, track and review the risks on regular basis.**

4. EXECUTING GDPR ACTION PLAN – FROM DATA SECURITY TO DATA REQUESTS

Cyber Security for Personal Data

- Cyber Security development based on Risk mitigation plans
- Cyber Security is implemented in
  - IT systems
  - Processes
  - Communication



Prepare for Requests from Data Subjects

- Data subjects have many rights for their personal data – and they may use these rights
- You need to have processes & tools in place to respond to these requests
- Identifying the data subject
  - When is it enough to rely on just an email address, and when should you use stronger authentication methods?

Training of your organization

- Prepare your organization for GDPR – educate your people
- Everyone needs to understand their own role in your privacy framework
- Your organization is as strong as its weakest link

5. PREPARING REQUIRED DOCUMENTS & CONTRACTS

Some mandatory documentation

- Informing the data subjects –> **Privacy notices**
- Risk assessments – **Risk mitigation plans**
- Records of requests from data subjects
- Records of processing activities – article 30
- Documented instructions for data processors

- Other documentation as part of Accountability
  - E.g. Process descriptions of data processing in different functions

Contracts

- **DPAs (Data Processing Agreements)** must be in place in the whole supply chain of data processing
  - Data Controller vs. Data Processor – clarify the roles!
  - NDAs with data processors
  - Documented instructions
  - Other terms based on article 28 – Processor, and article 32 – Security of processing

- **The whole supply chain must be covered**
  - You are responsible of your subcontractors too!
  - This includes cloud & information system vendors with access to the personal data

SUMMARY

Practical Changes in Everyday Life

- Rights of Data Subjects
- Risk assessment as an ongoing process
- Data Breach notifications
- Lots of documentation, legal work, contracts, …
- Continuous development
- It's not only about IT – it's about people
- **Accountability of GDPR compliancy**

- You shouldn't worry about huge fines, but **focus on customer trust** instead
  - What's the impact to your company's **reputation**?

Q & A

Pekka Vepsäläinen
Tikkasec Ltd

+358 40 152 2628
pekka.vepsalainen@tikkasec.fi