D5.2 Risk Assessment

Deliverable Number	5.2
Work Package	WP5
Version	1.0
Deliverable Lead Organisation	WU
Dissemination Level	Public
Contractual Date of Delivery (release)	2017/11/30
Date of Delivery	2017/11/30
Status	**Final**

Editor

Ben Wagner (WU)

Contributors

Ben Wagner (WU), Harald Zwingelberg (ULD), Karina Schuller (LDA), Patrick Murmann (KAU), Agnieszka Kitkowska (KAU), Poornigha Kumar (USE), Majid Hatamian (GUF), Alexandr Railean (ULD), Juan Quintero (UNI), Yefim Shulman (TAU), Luiza Rezende (TAU), Lamya Abdullah (UNI), Alexandros Mittos (UCL), Andreas Gutmann (VDS), Mark Warner (UCL).

Reviewers

Harald Zwingelberg (ULD), Leonardo Martucci (KAU)

Privacy&Us www.privacyus.eu
This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 675730.

Executive Summary

This report is part of a series planned within work package 5 “Risk analysis, Risk Perception and Law” of the Marie Skłodowska-Curie innovative training network Privacy&Us. Thirteen early stage researchers (ESR) will be trained to face both current and future challenges in the area of privacy and usability as part of their PhD-programme. Work package 5 fits into this by integrating several ESRs in the process of preparing a privacy risk analysis. This project report (D5.2) continues the work of work packaged 5 based excellent foundation laid by privacy principles (D5.1) for this planned series of reports and addresses the relevant aspects of privacy and usability:

D5.1 Privacy Principles
D5.2 Risk Assessment
D5.3 Risk Mitigation
D5.4 Risk Awareness Creation

In respect to the GDPR, this report exemplifies that usability aspects will be more important for data protection compliance in the future. The definition of usability according to ISO 9241-210:2009 is "the extent to which a system, product or service can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use.” The data protection goal of transparency is closely related to such aspects. As transparency requirements had been sharpened in the GDPR, e.g. the regulation now clearly demands that declarations must be presented in an easy language. To effectively provide the information necessary according to the GDPR data controllers need to consider such concepts broadly. Where possible the capabilities of user interfaces to communicate with audio and voice or haptic feedback should be considered. Likewise, the accepted practices for accessibility should be adhered to, allowing better access to e.g. vision impaired and easing the difficulty of reading texts. Likewise, this could be stipulated for the enforcement of data subjects’ rights which should be easy to accomplish or at least not too complex to enforce.

However, not only the law became stricter but also the systems and processes become more complex. It poses a challenge to understandably explain processes and data flows involved in cloud computing. In the field of IoT one often faces devices missing input and output devices such as a screen forcing to recourse to external devices. In order to understand these processes and the associated risks better, it is important not to randomly select potential risks, but rather to follow a structured methodological process. This risk assessment process is the core of deliverable 5.2, because of which the deliverable was structured around the risk assessment process. As this process needs to be experienced for it to be learned effectively, the consortium decided to engage in risk assessment exercise as part of the third doctoral training event in Tel Aviv. As part of the summer school three application domains relevant to all ESRs were discussed. The results of the risk assessment exercise were communicated in relevant press and policy channels.

Table of Contents

1 Introduction

This report is part of a series planned within work package 5 “Risk analysis, Risk Perception and Law” of the Marie Skłodowska Curie innovative training network Privacy&Us. Thirteen early stage researchers (ESR) will be trained to face both current and future challenges in the area of privacy and usability as part of their PhD-programme. Work package 5 fits into this by integrating several ESRs in the process of preparing a privacy risk analysis. This project report (D5.2) continues the work of work packaged 5 based excellent foundation laid by privacy principles (D5.1) for this planned series of reports and addresses the relevant aspects of privacy and usability:

D5.1 Privacy Principles
D5.2 Risk Assessment
D5.3 Risk Mitigation
D5.4 Risk Awareness Creation

In respect to the GDPR, this report exemplifies that usability aspects will be more important for data protection compliance in the future. The definition of usability according to ISO 9241-210:2009 is "the extent to which a system, product or service can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use.” The data protection goal of transparency is closely related to such aspects. As transparency requirements had been sharpened in the GDPR, e.g. the regulation now clearly demands that declarations must be presented in an easy language. To effectively provide the information necessary according to the GDPR data controllers need to consider such concepts broadly. Where possible the capabilities of user interfaces to communicate with audio and voice or haptic feedback should be considered. Likewise, the accepted practices for accessibility should be adhered to, allowing better access to e.g. vision impaired and easing the difficulty of reading texts. Likewise, this could be stipulated for the enforcement of data subjects’ rights which should be easy to accomplish or at least not too complex to enforce.

However, not only the law became stricter but also the systems and processes become more complex. It poses a challenge to understandably explain processes and data flows involved in cloud computing. In the field of IoT one often faces devices missing input and output devices such as a screen forcing to recourse to external devices. In order to understand these processes and the associated risks better, it is important not to randomly select potential risks, but rather to follow a structured methodological process. This risk assessment process is the core of deliverable 5.2, because of which the deliverable was structured around the risk assessment process. As this process needs to be experienced for it to be learned effectively, the consortium decided to engage in risk assessment exercise as part of the third doctoral training event in Tel Aviv. As part of the summer school three application domains relevant to all ESRs were discussed. The results of the risk assessment exercise were communicated in relevant press and policy channels.

The work follows the privacy impact assessment (PIA) methodology. However, since the planning phase of the project the European General Data Protection Regulation (GDPR) has been ratified and entered into force – to be directly applied as of May 2018, this provided a major change in the legal setting. With uptake of the GDPR, also our terminology underwent a change: instead of following the privacy impact assessment (PIA) methodology, we base our outline on the data protection impact assessment (DPIA) as set forth in Art. 35 GDPR. For this, a unified methodology or framework has not been agreed on yet.

As a result, rather than presenting students with a final methodological framework which does not exist, this deliverable will make ESRs aware of the current methodological frameworks which exist in the area of risk assessment.

Frameworks for Data protection impact assessments (DPIA) as required by Art. 35 GDPR are currently under development. Pre-existing to the GDPR had been methods for privacy impact assessment (PIA) and other assessment methods which are now modified and suggested for application. By April 2017 the Art. 29 Working Party identified four methods propagated by data protection authorities within Europe:[1]

- Germany, Conference of the Independent Data Protection Authorities (DSK): Standard Data Protection Model, V.1.0 – Trial version.[2] Since then a DPIA-quick-guide paper has been published as well by the DSK.[3]
- Spain, Agencia española de protección de datos (AGPD): Guía para una Evaluación de Impacto en la Protección de Datos Personales.[4]
- France, Commission nationale de l'informatique et des libertés (CNIL): Privacy Impact Assessment.
- Great Britain, Information Commissioner's Office (ICO): Conducting privacy impact assessments code of practice[5]

What these frameworks share is a joint process of 1) preparation, 2) evaluation and 3) reporting and safeguards. This process is described in detail by Felix Bieker, Michael Friedewald, Marit Hansen, Hannah Obersteller and Martin Rost in their paper describing *A Process for Data Protection Impact Assessment under the European General Data Protection Regulation,*[6] which is in turn based on the GDPR. As a result, this deliverable has been structured based on this three-part methodology, to ensure that the relevant content flows through the whole deliverable. An overview of this methodology is provided in **Figure 1**. A widely revised version of the white paper on the DPIA Methodology will be available by the deadline for the publication of this deliverable.[7]

However, as this deliverable is focussed on risk assessment, a significant section of last part of this methodology on safeguards cannot be discussed in the context of this deliverable (D5.2) and will instead be discussed extensively in the next deliverable in this work package D5.3.

The following document will thus first provide an overview of the three steps taken as part of this methodology: first the preparation stage, second the evaluation stage and third the reporting stage. As the second stage took place in the context of the third ESR training school, the second stage will also include reflections on methods of teaching and conducting risk evaluation procedures, both in an academic and a private sector context. Finally, the third reporting stage will focus on how the results of this deliverable can be published and most effectively disseminated, in particular in relevant press and policy channels.

[1] Art. 29 WP 248, p. 20.

[2] DSK, SDM, pp.

[3] DSK, DSFA, pp. 1 et seq.

[4] AGPD.

[5] ICO, PIA.

[6] Bieker, Felix, Michael Friedewald, Marit Hansen, Hannah Obersteller, and Martin Rost. 2016. 'A Process for Data Protection Impact Assessment under the European General Data Protection Regulation'. Pp. 21–37 in Annual Privacy Forum. Springer.

[7] Friedewald, M., Bieker, F. et al. 2017 (to appear). White Paper: Datenschutz-Folgenabschätzung – Ein Werkzeug für einen besseren Datenschutz; online: https://www.forum-privatheit.de/forum-privatheit-de/publikationen-und-downloads/veroeffentlichungen-des-forums/themenpapiere-white-paper/Forum_Privatheit_White_Paper_Datenschutz-Folgenabschaetzung_2016.pdf.

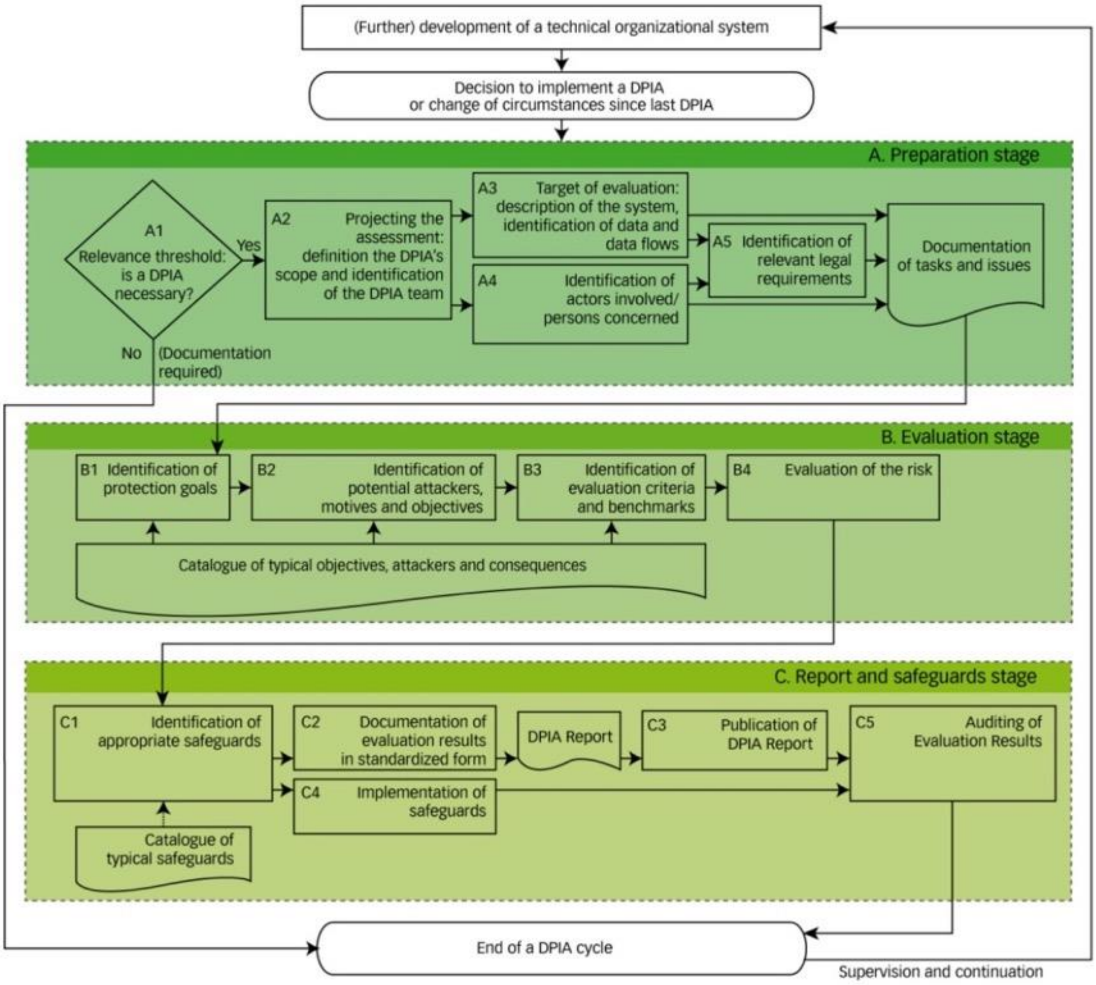

(Further) development of a technical organizational system
Decision to implement a DPIA or change of circumstances since last DPIA
A. Preparation stage
A1 Relevance threshold: is a DPIA necessary?
Yes
No
(Documentation required)
A2 Projecting the assessment: definition the DPIA's scope and identification of the DPIA team
A3 Target of evaluation: description of the system, identification of data and data flows
A4 Identification of actors involved/ persons concerned
A5 Identification of relevant legal requirements
Documentation of tasks and issues
B. Evaluation stage
B1 Identification of protection goals
B2 Identification of potential attackers, motives and objectives
B3 Identification of evaluation criteria and benchmarks
B4 Evaluation of the risk
Catalogue of typical objectives, attackers and consequences
C. Report and safeguards stage
C1 Identification of appropriate safeguards
C2 Documentation of evaluation results in standardized form
DPIA Report
C3 Publication of DPIA Report
C5 Auditing of Evaluation Results
C4 Implementation of safeguards
Catalogue of typical safeguards
End of a DPIA cycle
Supervision and continuation

Figure1: DPIA process from Bieker et al.[8]

[8] Bieker, Felix, Michael Friedewald, Marit Hansen, Hannah Obersteller, and Martin Rost. 2016. 'A Process for Data Protection Impact Assessment under the European General Data Protection Regulation'. Pp. 21–37 in *Annual Privacy Forum*. Springer.

2 Preparation: stage one

In order to conduct a meaningful risk assessment, it is important to engage in a rigorous and systematic preparation phase. This mainly involves establishing what organisational and technical processes are currently taking place that might be relevant from the perspective of the GDPR. This phase is often one of the hardest and most time consuming, as it involved collection of a wide-set of relevant information about data flows, process, roles and risks, as well as numerous follow-up questions.

In the context of this deliverable, it was important to ensure that the preparation stage of the risk assessment process took place before the doctoral training workshop in Tel Aviv. This was both to ensure that the relevant information was available for a risk assessment to take place, and to ensure that ESRs were able to ask follow-up questions about relevant risk-assessment frameworks. At the same time, it is important to ensure that the cases discussed are sufficiently concrete for an effective risk assessment to be possible.

Conducting a risk assessment in the abstract on a general field such as genomics or area of research such as health care provides very vague risks that are not sufficiently granular to conduct an effective risk assessment. Specific technically implementable cases are necessary to ensure an effective risk assessment process can be conducted.

As not all ESRs are able to provide such a processes, one of the organisers of the workshop at WU Dr. Ben Wagner – in consultation with the Privacy&Us scientific coordinator Prof. Simone Fischer-Hübner – selected the research projects of ESR5, ESR7, ESR10 & ESR12 as having the most relevant processes for a risk assessment exercise. In order to ensure sufficient information was available to ESRs during the doctoral training event in Tel Aviv, Dr. Wagner sent a questionnaire to these four researchers in advance of the training event, asking them for additional data about their research projects. The questionnaire is attached to this document in the Annex, and was asked the ESRs to respond to the following three basic questions:

- Q1: What is the target of the DPIA Evaluation? Describe the system, identify relevant data and data flows.
- Q2: Which actors are involved in the systems? What roles and permissions do these actors have?
- Q3: Which data flows are present? How do actors interact with them? Please draw a diagram of the relevant data flows and actors so that their relationship to each other is clear.

This questionnaire was completed by all researchers in advance of the training event in Tel Aviv and provided to all researchers as the basis for the risk assessment exercise as part of stage two. The answers provided by the ESRs will be integrated into the outcomes of the three research areas discussed in stage 2.

3 Evaluation & Workshop: Stage two

3.1 Introduction

Based on the results of the preparation phase in stage one, a risk evaluation workshop led by Dr. Ben Wagner (WU) and Karina Schuller (LDA) took place on Monday 13 November 2017 as part of the doctoral training event in Tel Aviv. It should be noted at this point that an extensive and rigorous full GDPR-compliant risk evaluation would typically take much longer than the time available at a doctoral training event. Thus the goal of the training event was not to produce final risk assessments by students but rather to provide useful first drafts in the time available that would help the students learn and apply the risk assessment methodology. The risk assessment workshop on 2017/11/13 was structured as follows:

- 14:10 – 15:20: Overview Presentation by Karina Schuller, LDA
- 15:20 – 16:00: Evaluation of privacy impacts of three cases
- 16:00 – 16:15: Brief (working) coffee break
- 16:15 - 17:00: Finalise first three drafts of privacy impacts
- 17:00 – 17:45: Discuss draft privacy impacts together as a group

In order to ensure that students were familiar with the basic principles of risk assessment methodology under the GDPR, they were provided with an initial overview of the relevant sections of the GDPR by Karina Schuller from the Bavarian Data Protection Agency LDA. Ms Schuller also provided a detailed overview of the current DPIA methodologies that are under discussed, ensuring that ESRs were aware of the fact that they were many methodologies currently up for debate and that on 13 November 2017 no final decision had yet been made which risk assessment methodology would be used throughout Europe.

In the ensuing discussion, there was considerable debate about the feasibility of such a methodology in a practical context for businesses. While some participants in the training were concerned about the extensive documentation requirements, others saw this as an opportunity for companies to better understand their own business processes.

As noted by Karina Schuller and others, this also provided an excellent opportunity for ESRs and other seminar participants to provide feedback on these methodologies, which will be fed back into the ongoing policy development process around GDPR-compliant risk assessment methodologies.

3.2 Setup of the working groups

Following this initial presentation, the whole group of ESRs and senior researchers was then split into three small groups, which each discussed one of the three research cases that had been prepared prior to the workshop. These three research cases were:

1. Collection of highly sensitive interview data during the research process (ESR12)
2. The implementation of a usage-based insurance model (ESR7 & ESR10)
3. The implementation of a privacy-protecting Android app (ESR5)

Both ESRs and senior researchers were free to join whichever working group they wanted. However, the workshop leads ensured that the groups were well balanced and had sufficient support from three experts who have sufficient experience in conducting risk assessments to be able to support the risk assessment process: Karina Schuller, Harald Zwingelberg and Ben Wagner. These three experts rotated between the three groups, ensuring that they had sufficient information in order to be able to conduct a draft risk assessment.

Specifically, to facilitate the risk assessment process, the three groups were asked to:

1) Identify protection goals based on the GDPR
2) Identify potential attackers, their motives and objectives
3) Provide a preliminary evaluation of the risks these attackers posed

As this is a considerable challenge based on the 1:40 available to the group, it was made clear that these risk assessments are preliminary draft and constitute a best-effort risk assessment in the time available rather than the final word on the risks present within relevant cases studied.

3.3 Group 1: Collection of highly sensitive interview data during the research process

3.3.1 Relevant preparation phase data

During the preparation phase ESR12 provided initial information about the process he believed could be relevant for conducint a risk assessment: a semi-structured interview study of men who identify as having sex with men, some of whom are HIV positive. During this interview study, the following data was collected by ESR12:

Data being collected before interview
participants name, e-mail address, sexual orientation (by assumption), HIV status (optional), Social media usage, Wordpress data

Data collected during interview
participants name, e-mail address, age range, sexual orientation, HIV status, HIV testing regularity, Social media usage, Sexual preferences, Sexual history, Names of family members and loves ones, Names of hospitals, Name of place lived, Intimate experiences, Intimate experiences of others

In order to ascertain the exact data flows around the interview process, ESR12 further went on to specify precisely how he went about recruiting and interviewing participants in his interview, as well as during the post interview process:

Data Flow - Recruitment

1. Recruitment via Twitter or Scruff
2. Potential participant visits website (wordpress)
3. e-mail sent to researcher via an e-mail provider (i.e. Yahoo Mail, Google)
4. E-Mail received by UCL e-mail server
5. Details of potential participant added to excel document stored on encrypted laptop and encrypted USB key
6. Participant e-mailed from UCL e-mail server to participants e-mail server
7. Participant interview arranged

Data Flow - Interview

1. Participant attends interview (may use Google Maps to find UCL office)
2. Pre interview questionnaire data collected and stored on paper
3. Interview recorded on Dictaphone
4. Participant handed Amazon Voucher
    a. Participant logs onto Amazon.co.uk to redeem voucher
5. Consent forms and paper notes handed to Principle Researcher to store in locked filling cabinet.

Data Flow – Post Interview

1. Dictaphone recording transferred to encrypted laptop
2. Encrypted container on laptop backed up to USB drive
3. Pre interview data copied from paper to excel document on encrypted laptop
4. Audio interview transcribed on encrypted laptop
    a. Audio interview anonymised
    b. Transcription backed up on encrypted USB
5. Audio interview deleted from encrypted laptop after encryption and kept on USB
6. After 6-12 months, original audio interview deleted

At the request of workshop lead Dr. Wagner, ESR12 agreed to visualise these data flows within the context of the following flow chart:

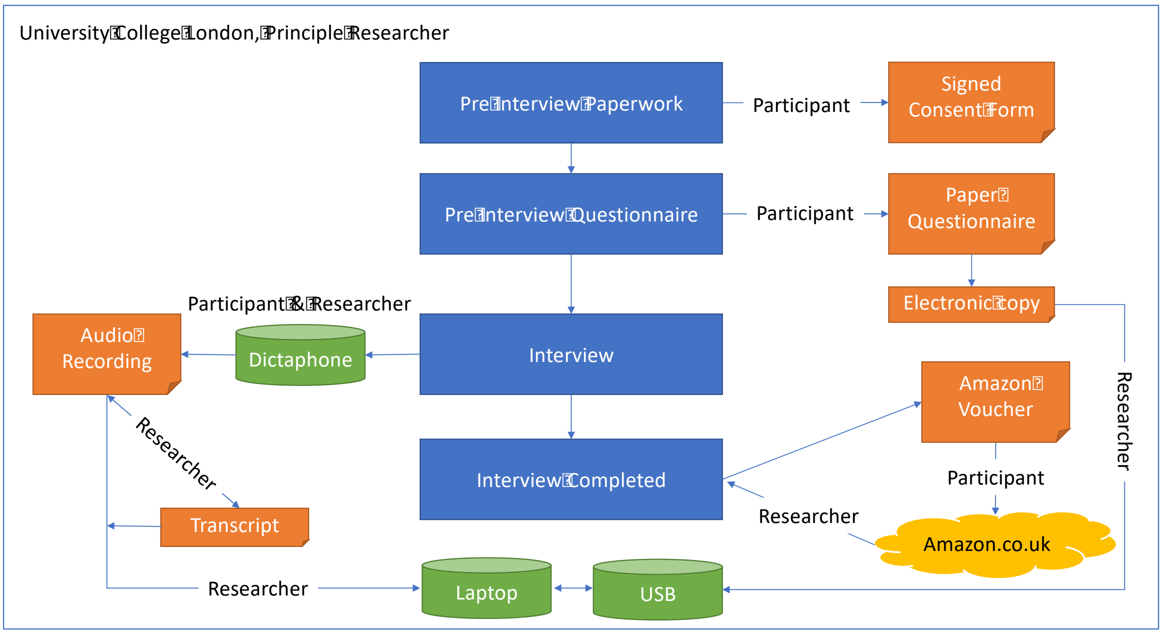


Figure 2: Case 1 flowchart

Finally, ESR12 identified the following actors who were engaged in or had power to control the data flows in some way or another, as well as identifying which actors had control over which data:

Actor Name	Actor Description	Individual (i), Organisation (O), System or Component (S)
University College London	The University with responsibility for the study	O
Prof. Ann Blandford	The principle research who has overall responsibility for the study	I
Mark Warner	The student researcher who is conducting and managing the study	I
Participants	People who have contacted the student and wishing to be involved in the study	I
UCL e-mail server	The mechanism for communicating with the participants	S
Wordpress	The hosting service hosting the research website	S
Twitter/Twitter Ads	Online social environment used to disseminate information about the study	S
Scruff App	Dating application used to disseminate information about the study	S
Encrypted Laptop	Equipment used to store audio interview files	S
Dictaphone	Equipment used to record the interview	S
Encrypted USB	Equipment used to store study data	S
Amazon.co.uk	Used to purchase amazon vouchers, and used by participants to redeem their vouchers	O
Transcription Service	Used to professionally transcribe the audio recorded interviews (not currently used)	O
Participants E-mail provider	Used by the participant to send e-mail to researcher	S/O
Skype	Used to facilitate over-the-web interviews	O
Researchers home Wifi Network	Used to perform encrypted back-up of encrypted laptop	S
Researchers home encrypted mac	Used to perform encrypted back-up of encrypted laptop	S

Data Flow	Actors Involved	Data
Recruitment	University College London Principle Researcher Researcher Participant Twitter Scruff App UCL E-mail server Wordpress Participants e-mail server Encrypted Laptop Encrypted USB Researchers home wifi Researchers home encrypted backup	participants name, e-mail address, sexual orientation (by assumption) HIV status (optional) Social media usage Wordpress data
Interview	University College London Principle Researcher Researcher Participant Dictaphone Encrypted Laptop Encrypted USB Researchers home wifi Researchers home encrypted backup Skype (optional) Amazon.co.uk	participants name, e-mail address, age range, sexual orientation, HIV status, HIV testing regularity Social media usage Sexual preferences, Sexual history, Names of family members and loved ones Names of hospitals, Name of place lived Intimate experiences Intimate experiences of others
Post Interview	University College London Principle Researcher Researcher Dictaphone Encrypted Laptop Encrypted USB Researchers home wifi Researchers home Researchers home encrypted backup Transcription (optional)	participants name, e-mail address, age range, sexual orientation, HIV status, HIV testing regularity Social media usage Sexual preferences, Sexual history, Names of family members and loved ones Names of hospitals, Name of place lived Intimate experiences Intimate experiences of others

3.3.2 Protection Goals

Based on this excellent data provided by ESR12, the group launched into a debate about the precise processes involved in this process. It was acknowledged that despite extensive documentation provided, considerable additional questions and uncertainties arose during the debate that needed to be clarified by ESR12.

Only after all processes had been clarified were the group able to move on to discussing protection goals. According to the group, the protection goals in this case could be considered to be the following:

1) Protect the data and reputation of the principal investigator,
2) Protect the data and reputation of the participants
3) Protect the data and reputation of the institution conducting the study
4) Protect the anonymity of participants

3.3.3 Potential attackers, motives, and objectives

Having defined these protection goals, the group one then discussed which potential attackers might have an incentive to harm these protection goals. They also discussed what the motives of such attackers might be and how they would go about achieving these objectives. As a result they developed the following chart of potential attackers, motives and objectives:

Attackers	Motives	Objectives
1. Principal investigator	A. Revenge	!. Fake data
2. Academic institution	B. Monetary gain	@. Identify participant
3. Colleagues	C. Political gain	#. Erode trust
4. PI's supervisor	D. Jealousy	$. To learn
5. IT staff at Academic institution	E. Misinformation	%. To harm
6. Participants	F. Curiosity	
7. Police	G. Anger	
8. Security agencies	H. Error	
9. Research competition	I. Competitive advantage	
10. Marketers	J. Sabotage	
11. Hacktivist		
12. Politically motivated person		
13. Economically motivated person		
14. Relatives / flat mates		
15. Media / journalists		

Following the development of this chart, they then attempted to cross-reference the different attackers with potential motives and objectives, developing the following list:

Assignments:

1. A.B.C.D.E.G.H.I.J.	|	!.@.#.$.%.
2. B.C.E.F.H.I.	|	!.@.#.$.%.
3. A.B.C.D.E.F.G.H.I.J.	|	!.@.#.$.%.

For example, these assignments suggest that the respective academic institution hosting this process might make an error, because of which participants in ESR12's study could be identified. It also suggests that colleagues attempting to attain a competitive advantage could attempt to sabotage his work.

3.3.4 Evaluation of risk

Based on this draft assessment of relevant risks, group one began a wider evaluation of the risks involved. They discussed the tension between existing national regulation to keep original personally identifying information to avoid research fraud and the requirements of the GDPR.

They also made aware of the fact that many researchers were likely to use comparatively unsafe tools in the data gathering process, for example by conducting ‘virtual interviews’ via unsafe online tools. A discussion ensued about which such tools had the lowest risk profile and how to ensure that academics were aware of such tools. There was also general agreement in the group that existing ethics review processes within academia do not sufficiently consider privacy aspects and will likely need to be updated in the context of the GDPR.

There are also dangers due to the convenience of outsourcing transcription to research assistants at the university or even external private companies. Here the incentives are strongly tilted towards of outsourcing transcription as it is very time consuming, however there are considerable privacy risks involved. The group discussed potential ways in which some such services are more privacy compliant – typically in the field of medical transcription where providers strive for HIPAA compliance - while also acknowledging that there is considerable additional cost associated with using such providers.

An additional risk is related to unexpected interactions between different technologies. During the research process, on connecting the Dictaphone to the encrypted laptop, google drive tried to automatically sync the content to Google Drive. The risk here is that even a highly skilled scholar would not be able to predict all possible interactions of technologies, resulting in unexpected and unpredictable sharing of data.

In conclusion participants of the group suggested that scholars require a far greater level of institutional support in order to be able to implement high security and privacy solutions in the data gathering process. It is unreasonable for academic institutions to expect scholars to setup these kind of solutions themselves, rather they should be provided at an institutional level and streamlined within the research process. This may however also provide difficulties for participants to take part in these kinds of interview processes, as many of the privacy-protecting solutions are more difficult to use the comparable less privacy protecting products.

3.4 Group 2: The implementation of a usage-based insurance system

3.4.1 Relevant preparation phase data

In order to prepare for the workshop, ESR7 and ESR10 provided valuable preliminary information about the technical and operational process of the process being studied.

According to the GDPR art 35, one target of the DPIA Evaluation is a process where “a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person”. That is close to the following artefact and application scenario described.

The artefact is a structural model for cloud-based application implementing sealed computation concept. The application scenario is Usage-Based Insurance (UBI). UBI is a technical term referring to an auto insurance system that “enables insurance companies to collect individual consumer’s driving data and provide individually targeted price discounts based on each consumer’s driving behaviour”[9]. Typically, such kind of applications utilizes cloud computing to gain scalability and high availability.

The data flow will be described later, including the roles and actors involved in the application. One major actor is the cloud service provider. In this model, the cloud system is proposed to implement the sealed computation mechanism. It is an abstract computation model that could be defined by for properties. The properties are summarised as below:

- Data and application **Sealing**: Sealed storage and privilege access management. The data is protected by binding it to privileged platform including hardware and software. It requires two main abstract primitives: seal and unseal.
    - **Seal**: the operation of encrypting data and save it in the corresponding storage.
    - **Unseal**: decrypting the data only by the allowed process running on correct machine.

A combination of cryptography and key distribution mechanisms in addition to policy integration and enforcement approaches is required to ensure the property of sealed storage.

- **Attestation**: As long as the process has not terminated, the service can generate a token that proves to the systems is running as expected, i.e., any changes will result in a different token (will be detected).
- **Black-box**: Information flow between parties in the system is restricted by the interface specification of the interfaces i.e., nothing about the internal state of the system can be learned apart from what is given away at the interface.
- **Tamper-resistance**: Any usage of system that does not satisfy the specification results in termination and the destruction of data and processes such that neither code nor data can be retrieved.

Any computing service that guarantees the four properties is a sealed computation service. Implementation examples of the concept are:

- **SGX** (Software Guard eXtension) is an Intel technology to allow application developers to protect code and data from modification and disclosure via the use of what so-called of *enclaves*, which are protected areas of execution in memory. SGX technology supports sealing and attestation mechanisms and it allows lower trust in the operator and/or environment that runs the application.

[9] Miremad Soleymanian, Charles Weinberg, and Ting Zhu. The value of usage-based insurance beyond better targeting: Better driving. 2016

- **Hardware security module** (HSM) is a physical computing device to manage and safeguard keys for strong authentication and perform protected computation. Based on the design of the HSM, it ensures tamper resistance by hardware-based sensor mechanisms that delete internal data upon detection of unusual environmental conditions. It is possible to install specific software modules on HSMs and create cryptographic keys with the hardware device that never leave it, thereby supporting attestation.
- **Secure Encrypted Virtualization (SEV)** is a security model designed by AMD for virtualized environment. It aims at isolating execution between low privileged code and high privileged code to protect guest machines' execution. It integrates the “Secure Memory Encryption” with the virtualization architectural of AMD-V and therefore also protects data-in-use and not only data-at-rest via protecting read/write data from/to memory. Moreover, SEV firmware provides three main properties: platform authenticity, attestation of launched guest machine and guest’s data confidentiality.
- **Sealed Cloud** is a technology that implements sealing of data and computation provided by Uniscon GmbH. In practice, a sealed segment is a computer within a physical container (usually a server rack) that is protected by means of state-of-the-art perimeter security. This includes various types of sensors and detectors that capture unauthorized access (similar to burglary protection systems in cars). In case of attack detection, the system sets off an alarm and triggers internal protection procedures that includes data clean-up. The servers utilize secure boot and secure key distribution to provide software integrity.

In UBI scenario, the data are collected from the car which is typically equipped with a telematics device (dongle, blackbox, embedded system, or smartphone app). Data could be: car-related information and driving data such as: location, driving time, location, speeding, acceleration, braking, steering, direction and distance travelled, etc. Some of this data can be directly collected using various car sensors, other data types can be calculated from the collected data, depending on the telematics device. Improve driving behaviour, reduction of accidents and/or economic incentives are possible useful outcomes.

One current program of UBI is SmartDriver (Figure 3). It is a UBI program implemented by HUK-COBURG (Germany), Robert Bosch GmbH, and HUK-COBURG Datenservice und Dienstleistungen (HDD) for young people (18-25) or people who got their driving license less than 5 years ago. SmartDriver uses a blackbox as a telematics device to collect the driving data. HUK proposes this solution taking into account the segmentation of user data in:

- **Driving data**: It contains only data collected by the blackbox. They are sent to HDD and stored on a server in Germany
- **Personal data**: These data are collected at the moment the user enrols at the insurance policy and maintained in a server of HUK-Coburg in Germany.

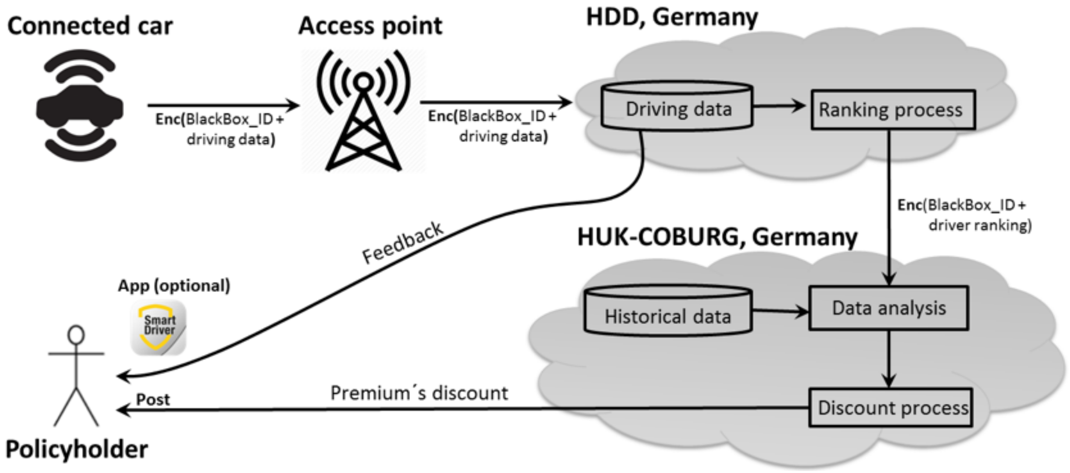


Figure 3. SmartDriver. HUK-COBURG

In SmartDriver program, the smartphone app is optional. The policyholder can use it to get the feedback. The premium´s discount is calculated on September 30 and can be maximum 30%. The insurance company offers to the policyholder three different certified technical services where he/she can install the blackbox. The technical service installs the blackbox and sends to the insurance company the information about the policyholder such as name and mobile number, also the identification of installed blackbox (blackbox_ID).

The blackbox is produced by Robert Bosch GmbH. It has a detector of traffic accidents, which is activated in case the blackbox detects some abrupt change in the speed of the vehicle. The blackbox collects all traffic accident data and send it to the insurance company, also it calls to the policyholder phone to report the incident. This service only works in Germany. It stores the collected data in an internal memory until it can send it to HDD server. If the connection between the blackbox and HDD server is not possible and the memory is full, the oldest data in the blackbox memory are overwritten.

The collected driving data are speeding, acceleration, braking, steering, and time and place of the trip. The direction and distance travelled are calculated from collected driving data. The blackbox sends the collected driving data to HDD server, where they are processed to calculate a driver ranking associated to a blackbox_ID. The driver ranking is a number between 0-100. The identification device (blackbox_ID) is the connection between the blackbox, insurance company, and HDD.

To calculate the discount is not important how many kilometres the policyholder drives. The policyholder will receive the discount by post and he/she can use it for the next contract (next year).

Actors in the system can be summarized into the below categories:

- **Data producer (subject/car drivers):** could be the owner of the car and/or the driver of the car. This actor represents implicitly the details about the car and the driver (including the policy holder) .
- **Insurance compa**ny (**Results Consumers)**: receives the final processed result which is the premium result out of the calculation of the driver ranking.
- **Application developer** (analytical SW): develop the analytics software to be run on the collected data. The software is the ranking calculation and the premium calculation processes.
- **Cloud Service Provider**: provides the cloud service that includes the infrastructure, visualization, platforms, configuration and deployment environment and security of the system as well as availability.

- **Telematics provider:** This actor is an indirect stakeholder, who is responsible for providing mechanisms of collecting data. (it is not included in the data flow as it is not in the path of information moving)

ESRs also provided an overview of the relevant data flows: The data flow might take different forms based on the specific application design decision. For simplicity of the discussion here, we describe the below data flow that could be extended.

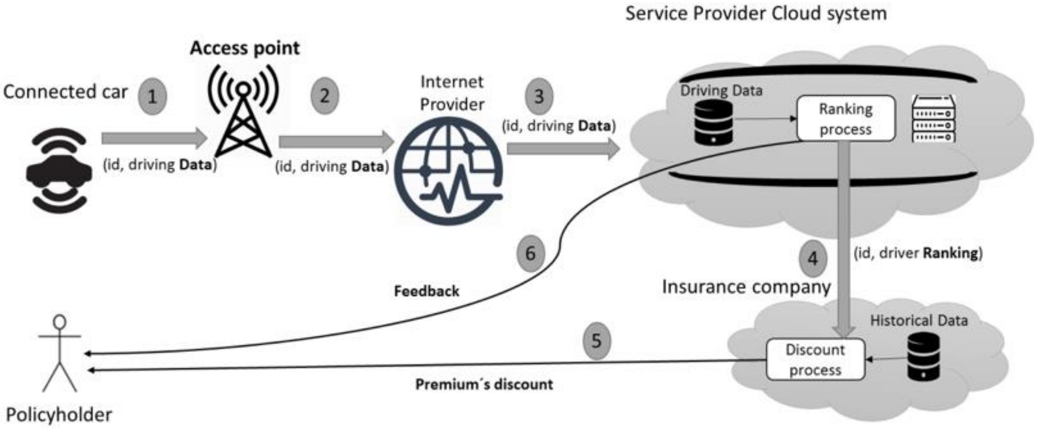


Figure 4. Data flows in connected car. Usage-Based Insurance scenario

Figure 4 illustrates how the connected car sends the collected driving data, using a cellular network infrastructure, to the Service Provider Cloud system where they are processed (*Ranking process*) to calculate a driver ranking associated with telematics device identification (**id**). By mapping this **id** to the policyholder identification is required to access the ***Historical data*** database, where all policyholder data are stored. Using the driver ranking and the historical data, the insurance company performs (*Discount process*) the discount and sends the premium´s discount to the Policyholder. The driver ranking generally is a number (score).

Finally, the Policyholder gets the premium´s discount and feedback about his/her driving style.

3.4.2 Protection Goals

Based on this comprehensive preliminary information, the group discussed protection goals. They quickly realized that in the short time available it will be cumbersome to discuss all protection goals. Instead, they decided to discuss one specific protection goal: confidentiality, in detail, rather than discussing a large number of protection goals in a more superficial manner.

3.4.3 Potential attackers, motives, and objectives

Group 2 identified several attackers, their motives and objectives, as is visualised below:

Attackers	Motives	Objectives
Employees	Curiosity	Discrimination
Service personnel	Revenge	Fraud
Hackers	Financial gain	Financial loss
Business partners (of insurance company)	Challenge	Damage reputation

Competitors		
Former employees		
Relatives (trusted)		
Friends (trusted)		
Processor & Affiliates		

The identification of attackers, motives, and objectives was a result of brainstorming of all participants with the support of workshop´s conductors to considering the GDPR articles (5, 32, and 75). After the attackers and motives were defined, the participants proposed connections between them, for example: curiosity is a motive for employees, hackers, relatives, and friends to attack the confidentiality.

Using the identified attackers, motives, and their connections the participants discussed the objectives. Among the identified objectives were discrimination, fraud, financial loss, and damage reputation.

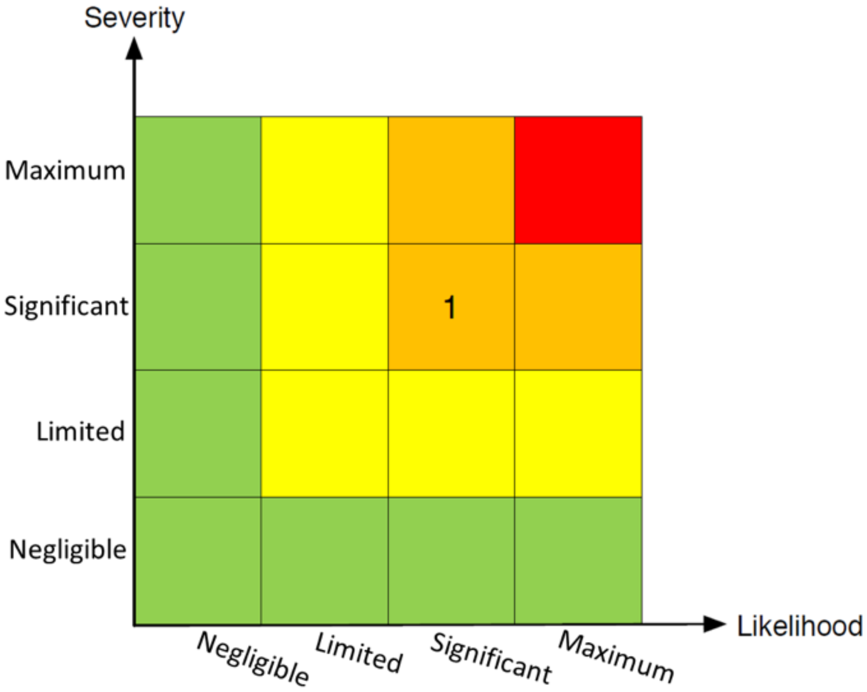
Motives **Attackers**	Curiosity	Revenge	Financial gain	Challenge
Employees	✓			
Service personnel			✓	
Hackers	✓		✓	✓
Business partners (of insurance company)			✓	
Competitors			✓	
Former employees		✓		✓
Relatives (trusted)	✓	✓		✓
Friends (trusted)	✓		✓	
Processor & Affiliates		✓		

3.4.4 Evaluation of risk

Based on the identified attackers in 3.4.3 and risk classes visualized below, the participants proceeded to position the potential attack into the risk´s matrix (Severity of damage vs likelihood of risk´s occurrence) using the scale: Negligible (Neg), Limited (Lim), Significant (Sig), and Maximum (Max).

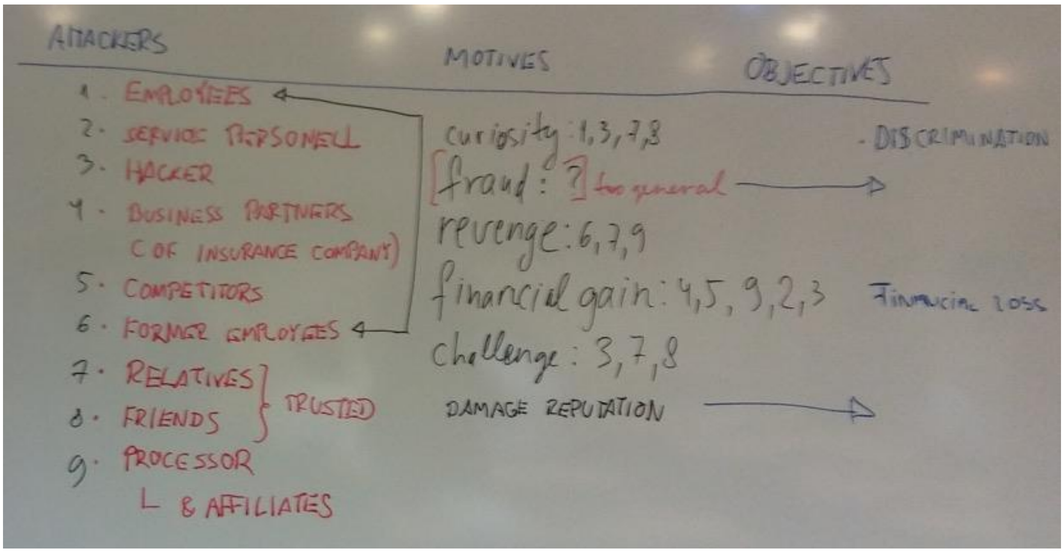
Risk classes	Factor
High risk	16
Risk	12-15
Reduced risk	6-11
Low risk	1-5

After a long discussion and due to time constraints, the participants only positioned one attacker (employees) in the risk matrix.



	Negligible	Limited	Significant	Maximum
Maximum	🟩	🟨	🟧	🟥
Significant	🟩	🟨	🟧 1	🟧
Limited	🟩	🟨	🟨	🟨
Negligible	🟩	🟩	🟩	🟩

As documentation of the workshop, the participants provided the following pictures.



ATTACKERS

1. EMPLOYEES
2. SERVICE PERSONELL
3. HACKER
4. BUSINESS PARTNERS (OF INSURANCE COMPANY)
5. COMPETITORS
6. FORMER EMPLOYEES
7. RELATIVES
8. FRIENDS
9. PROCESSOR
   └ & AFFILIATES

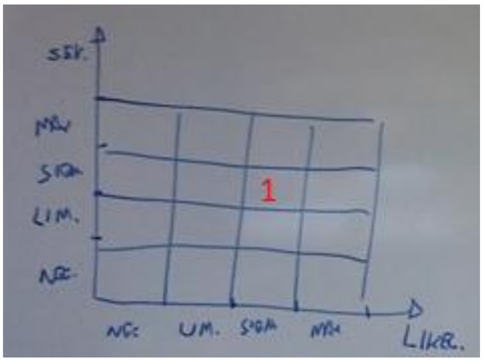
7., 8.: TRUSTED

MOTIVES

curiosity: 1,3,7,8
[fraud: ?] too general
revenge: 6,7,9
financial gain: 4,5,9,2,3
challenge: 3,7,8
DAMAGE REPUTATION

OBJECTIVES

- DISCRIMINATION
Financial loss



Conclusions:

- The preparation stage in the DPIA is very important and should not be omitted. An extensive documentation and strong reference descriptions are necessary to ensure an effective and high quality risk assessment. Such documentation increases understanding of the case and enables improved identification of the possible attackers, motives and objectives.
- The DPIA is a challenging process that requires a systematic approach. The systematic methodology should be supported by external sources available throughout the process, such as the GDPR and its recitals that can be referred to when necessary.
- The assessment process needs more time, so this exercise was the first learning trial to understand the necessary protection goals and the participants needed more time to focus on the evaluation stage.

3.5 Group 3: The implementation of a privacy-protecting Android app

3.5.1 Relevant preparation phase data

During the preparation phase, ESR5 provided extensive preparatory data as the basis for the risk assessment. The artefact being assessed here is a tool (app) for Android phones that its ultimate goal is to inform users about privacy deviated behaviours observed from installed apps on user's phone while they are running. The app reads the logs (the frequency of permission/resource accesses, the time of accesses, etc.) from the Android system program and merges this information with pre-defined rules in order to identify privacy invasive activities from installed apps. The app does not collect any personal relevant information and does not have access to any permission on the user's device and it is only allowed to read the device's logs in which no PII is included/stored.

Based on the transparent and privacy awareness information which are being sent to their user by the app with regards to the privacy invasive behaviours, the user will be given this possibility to report privacy deviated behaviours that he has observed based on the information that he received from the proposed app. As a result, if the user really feels that such behaviour is privacy invasive (e.g. Audio permission was accessed while the device was on the table and the screen was of, meaning that the user was not using the device), the user will be able to send report/feedback to the server. These feedbacks will be further used and processed in order to come up with a consensus decision making regarding the apps' behaviour. In this phase, the only information processed is the users' feedback (as a form of text) that is anonymised and it cannot be linked to any actual identity.

ESR5 also noted that the following actors are involved in managing data in the system:

Actor	Role	Permission
Developer	The *Developer* is the person who has designed, developed and implemented the system (the app)	The *Developer* is only allowed to read the logs produced by installed apps on the user's device. By defualt, these logs are produced by Android system and they are not visible to the *User*. These logs do not include any PII and they only contain information regarding the frequency of accesses to the user's resources (e.g. camera, microphone, etc.), the time of accesses, etc.
User	The *User* is the person who uses the system implemented by the *Developer*	The *User* has the permission to send report to the *Server* regarding the privacy invasive activities that he has observed. By default, the *User's* identity is anonymised. The *User* can selectively mark (optionally) the resources (e.g. contacts, camera, etc.) that he thinks their privacy has been violated along with a text (optionally) to explicitly mention why he feels those resource accesses are privacy invasive.
App Store	*App Store* is the place in which the system (the app) is placed to be shared among the *Users*	
Server	*Server* is an entity in which the reports sent by the users will be stored	The *Server* has the permission to send the data related to the users' reports to the *Admin*.

Admin	The *Admin* is a person who manages the *Server*	The *Admin* has the permission to read and process the reports sent by the *Users* to the *Server*. These reports may contain the name of the resources that the *User* thinks their privacy has been violated and an optional text that describes the reason of such report which are anonymised and cannot be linked to any actual identity.

Based on this preliminary data, ESR5 also developed an overview of the data flows within the app that can be visualised as follows:

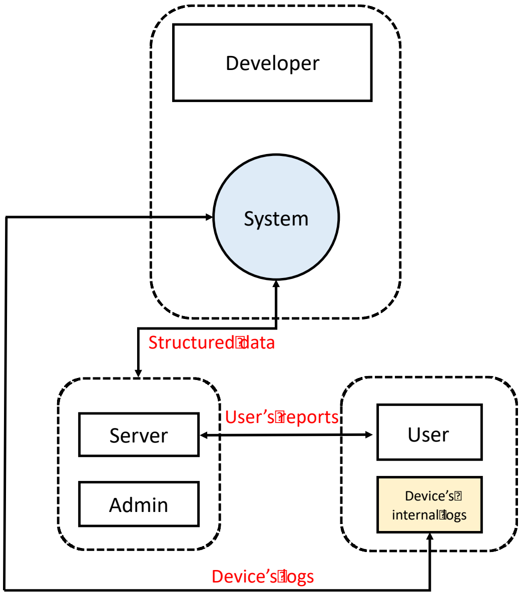


Figure 1: An overview diagram of the actors and relevant data flows.

Despite this extensive description, the workshop working group still required considerable time to work out what exactly Android app was doing and the precise data flows that were involved. This working group not only included participants present in Tel Aviv, but was also complemented by ESRs joining remotely via conferencing system. The use case had been introduced on basis of a document provided by ESR5.

The first round of discussion was dedicated to understanding the details of the use case. In short the artefact to be provided by the ESR will as an application running on the user's android phone accessing log files about the privilege use of other installed applications, identifying and displaying unusual and potentially harmful or privacy-invasive activities of these other applications. The ESR provided the use case participated in the working group and was available for further questions regarding details of the planned structure, data flows etc. Already at this stage of identifying more details of the use case the participants identified potential risks by means of their questions for understanding details.

Updates of the use case description from the discussion process:

- Within the use case description, the assumption was made that the app does not collect or process personally identifiable information. Given the GDPR as benchmark for data protection in Europe it was suggested to refer to "personal data" as defined in Art. 4. (1) GDPR instead. Also as part of the dialogue it was found that the log files accessed by the app and forwarded to the server may contain sensitive information that is also potentially linkable to a particular user with additional knowledge or information available by the file transfer.

- The app uses the "USB debugging mode" to allow access to log files also of other apps installed. Beyond this additional groups of rights as defined within the android environment are not required.
- The developer does not have access to all log files on the device. The app gains this possibility. The app will, however, only send those files for further inspection that the user chose to send.
- A log file dataset will contain information regarding the app monitored, the privilege used and the timestamp of the privilege use.
- The artefact does not foresee a backchannel to inform users outcomes and result of the analysis of log files sent.

3.5.2 Protection Goals

To focus the following discussion on protection goals the data protection goals as descried in the standard data protection methodology had been quickly re-introduced to the participants. During D5.1 the protection goals in smartphone ecosystems had been described.[10] To ensure these principles were fully understood, they were visualised again by Harald Zwingelberg, including confidentiality, integrity, availability, transparency, intervenability and unlinkability.

3.5.3 Potential attackers, motives, and objectives

The artefact underlying the use case is in itself a process to address the identified aspects of transparency and intervenability in smartphone ecosystems.
The working group then identified potential attackers for the use case:

- Hackers with the aim to use the rights of the app
- Evil developer of the app accessing more data on the phone and transmitting more information than intended by the user to the central server
- Evil administrator of the server abusing data.
- Data miners: The data collected on the server about the app usage data of persons may be of interest to data miners who may come in as internal attackers, e.g. business unit of the developer or server administrator or some third party.
- The legal entity representing the developer or server administrator may severely change its policy e.g. due to merger / or acquisition with another controller – potentially from third countries. This party may use the data beyond the initial purposes intended.
- Competitors or app programmers: The service may be abused to discredit a specific application by intentionally sending negative information about an app. Competitors of app developers or also blackmailers.
- A hacked developer's system may be used to blackmail developer or to insert malware in the artefact.

3.5.4 Evaluation of risk

Based on this view of potential attackers some risks could be identified within the timeframe and the group discussed the likelihood of the risk to occur.

- De-anonymisation and Re-identification of reports sent to the server. Even where the data is sent by the artefact without identifiers such as usernames a (re-)identification of users may be possible based on IP-addresses, timestamp or the selection of specific apps. The likelihood

[10] Railean/Zwingelberg, pp. 28 et seq.

for the risk to occur was identified as medium. The severity of such a de-anonymisation depends highly on the type of application. E.g. the name of specialized medical apps may contain health information while the data on the use of dating apps allows conclusions on sexual interests and behaviour.
Mitigation: Measures for the database on the server include adding noise or differential privacy. Transparency by describing potential risks to users beforehand enhances the awareness of data subjects.

- A dishonest administrator or developer may abuse the data. The likelihood is medium. The risk depends on the data submitted, in particular the type of application monitored.
- Access to identifiers existing on the phone by the artefact. Unless identifiers exist as part of the log files this should not be possible as this would require additional permissions under android. The likelihood for the risk to occur is low.
- The users themselves may providing identifying information. The process requires a means for users to provide information what particular behaviour of an app they want to report. For this allowing entries as free text appear to be necessary and highly desirable for users to express themselves and for the researchers to obtain information. The likelihood is high the severity depends on the further information provided. Mitigation methods that came to mind include checkboxes for typical answers, having the text field greyed out and a clear statement that users must not provide identifying information in the clear text field.
- The developer may send false warnings to the community. This was found to not be a data protection related risk.

Given that the artefact is intended to work as a privacy enhancing technology and only has a limited scope and few data that are processed.

3.6 Lessons learned from risk assessment workshop

As a result of the risk assessment workshop we were able to identify several more general lessons, both about teaching risk assessment as well as the actual risks discovered during the risk assessment process. Notably, several German data protection authorities have engaged in similar model-exercises to verify the feasibility of selected DPIA models proposed on basis of a fictional use case for a pay-as-you-drive car insurance. The results of the assessment by the team of the authorities of federal states of Mecklenburg-Vorpommern and Schleswig-Holstein (ULD) have been published and contain a section on lessons learned.

1) Difficulties ascertaining operational and technical processes
The first 45 min of each risk assessment exercise was typically needed to clarify the use case. This shows the importance of a very good and exhaustive preparation phase. In particular data types, data flows must be described in detail. Even with extensive preparation it is still important

2) Challenges assessing risk likelihood
Assessing the likelihood of a risk to occur was difficult for all groups. This suggests that despite the four existing methodologies, there is an urgent need for clearer and more objective risk likelihood assessment methodologies to ensure that this process is easier, particularly for those new to and therefor unfamiliar with this risk assessment processes.

3) Developing protection goals can lead to varying results
Some of the groups developed the protection goals on an ad hoc basis rather than focussing on the specific framework of the GDPR. It is important, even for individuals familiar with PIA or other impact assessment methodologies to reiterate that risk assessments under the GDPR need to develop the protection goals based on the GDPR text.

4) Considerable time and resources required
A risk assessment is time-consuming and needs participation of several persons and a well organised assessment process. Given the existing time constraints it was suggested to limit the timeframe for the risk assessment process and by this to have the participants focus on specific risks and prioritise these risks effectively to streamline the process.

5) Need for divergent inputs from at least 3 (preferably more) different perspectives
Risk assessments require a interdisciplinary and collaborative approach. The assessment should take place as a collaborative exercise involving not just lawyers, not just engineers and not just social scientists, but rather integrating all through groups as well as other groups with relevant expertise.

Depending on their disciplinary background, participants often come up with specific mitigation techniques first, i.e. saying we need to encrypt this data. Rather than stopping at the point of mitigation, it is important to acknowledge the risk at the base of this mitigation strategy and then think ‘backwards’ to properly describe the risk.

6) Selection of the appropriate measure
Where several measures may be taken, it appears preferable to select measures that avoid processing of data and thus affect the process design. This would also be in accordance with the data protection by design principle laid out in Art 25 (1) GDPR. The risk assessment must therefore be timed early enough in the decision process to still allow relevant influences on the design of the process structure, data flows or the selection of systems. This should ideally result in an iterative process.

4 Reporting: Stage three

Based on the risk assessment made in stage two and in particular the lessons-learned in section two, we have included a short reporting section to complete the process. As noted above this section cannot consider potential mitigation strategies, which will be discussed in detail in the forthcoming deliverable D5.3. Instead, this stage will focus on reporting the major risks that were identified during the risk assessment process. These major risks have been communicated in relevant press and policy channels, to ensure that they are considered as part of a wider societal debate.

Despite the short time available to the group, it is possible to consider several major risks that were discussed during phase two and constitute relevant outcomes of the risk assessment workshop conducted in stage two. These major risks are:

1) **Need to update university ethics review procedures in the light of the GDPR:** University ethical review board (ERB) procedures are not currently equipped to integrate the extensive risk assessment methodologies required by GDPR. Considerable updates will be necessary to make these ERB procedures GDPR-compliant.

2) **Even for technically highly competent-users, ensuring GDPR-compliance a challenge:** this is due to existing technical design issues in commonly used technologies, when many technologies are 'automatically' set to upload data into a geographically-unspecified 'cloud' server, or conduct other practices which are likely to be privacy-invasive.

3) **Technology design and risk assessment go hand in hand:** in responding to potential risks, it is important that risk assessment starts early and directly influences the technical design process. By doing so, it is more easily possible for technologies and operational process to adapt in a manner that systematically considers risks.

4) **Rapidly changing risk environment:** due to rapid technological change the risk environment is constantly changing. Risks that couldn't even be imagine even a few years ago have now become normal. Thus, risk assessment are never a one-off initiative, but rather the beginning of an ongoing process to safeguard the protection goals enshrined in the GDPR.

In order to ensure that these risks are appropriately communicated, Dr. Ben Wagner ensured that these risks were communicated in the following policy channels:

- 16.11.2017: Meeting with the Israeli Foreign Ministry, as part of which the Privacy & Us project and the implementation of the GDPR were discussed.
- 16.11.2017: Talk at the University of Haifa, where several judges and high level government officials were present and where the Privacy & Us project and sustainable technological responses to the risks were discussed.
- 29.11.2017: Permanent Stakeholders Group meeting of the European Network Security Agency (ENISA), where these findings and the role of ENISA in safeguarding privacy in Europe were discussed.

Bases on a close coordination with colleagues in the Pricacy & Us Project about appropriate dissemination, Dr. Ben Wagner submitted some of these findings to journalists in Brussels and Berlin. While these findings will likely not be directly referenced in publications, they will considerably contribute to the ongoing reporting on Privacy in Europe.

5 Literature

Agencia española de protección de datos (AGPD): Guía para una Evaluación de Impacto en la Protección de Datos Personales (EIPD), 2014., https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf.

Art. 29 WP 248: Article 20 Data Protection Working Party (2016). Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, Adopted on 4 April 2017, online: https:// http://ec.europa.eu/newsroom/document.cfm?doc_id=44137.

Commission nationale de l'informatique et des libertés (CNIL), Privacy Impact Assessment (PIA) Methodology - how to carry out a PIA, 2015, online: https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf.

DSK, DSFA: Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK, engl: °Conference of the Independent Data Protection Authorities of the Bund and the Länder) (2017). Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO, 2017, online: https://www.lda.bayern.de/media/dsk_kpnr_5_dsfa.pdf

DSK, SDM: Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK, engl: °Conference of the Independent Data Protection Authorities of the Bund and the Länder) (2016). The Standard Data Protection Model – A concept for inspection and consultation on the basis of unified protection goals, online: https://www.datenschutz-mv.de/datenschutz/sdm/sdm.html

Friedewald, M., Bieker, F. et al. (2017, to appear), White Paper: Datenschutz-Folgenabschätzung – Ein Werkzeug für einen besseren Datenschutz; online: https://www.forum-privatheit.de/forum-privatheit-de/publikationen-und-downloads/veroeffentlichungen-des-forums/themenpapiere-white-paper/Forum_Privatheit_White_Paper_Datenschutz-Folgenabschaetzung_2016.pdf

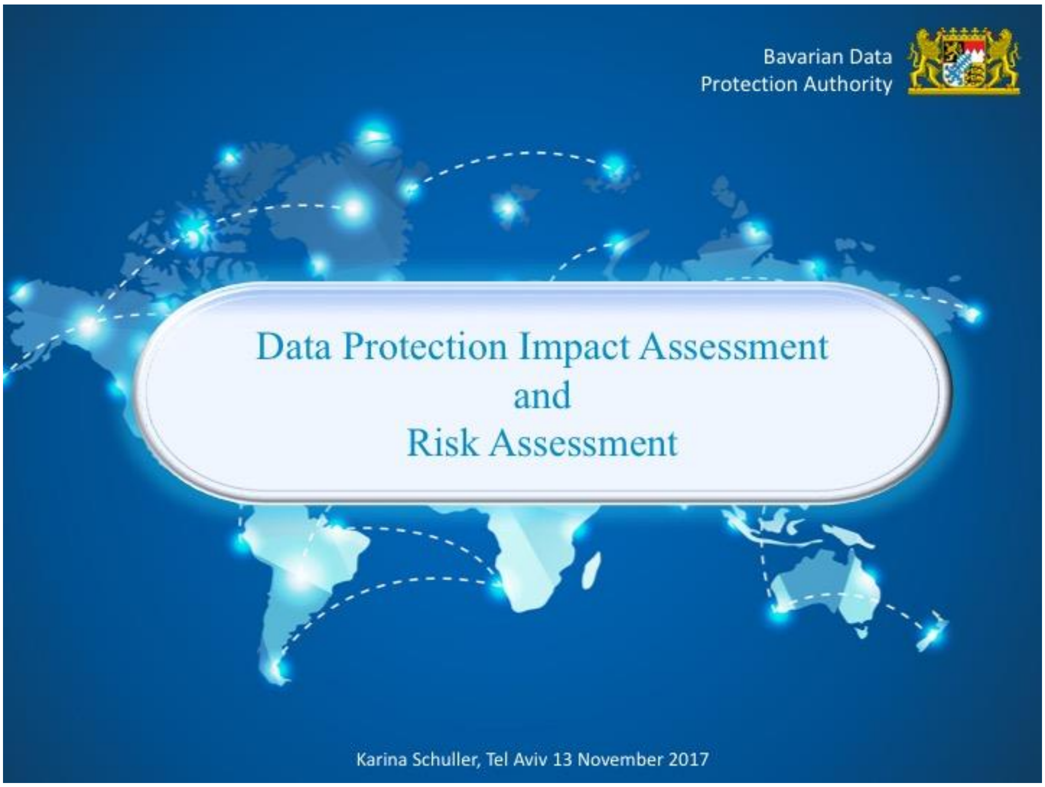
Gonscherowski, S; Herber, T.;Robrahn, R. Rost, M.; Weichelt, R.; Durchführung einer Datenschutz-Folgenabschätzung gem. Art. 35 DSGVO auf der methodischen Grundlage eines standardisierten Prozessablaufes mit Rückgriff auf das SDM am Beispiel eines „Pay as you drive"-Verfahrens (V 0.10), online: https://www.datenschutzzentrum.de/uploads/datenschutzfolgenabschaetzung/20171106-Planspiel-Datenschutz-Folgenabschaetzung.pdf

Paal, B. P., Pauly, D. A. (2017). Datenschutz-Grundverorndung – DS-GVO, Munich 2017

Railean, A. Zwingelberg, H. [Eds.], D5.1 Privacy Principles, Privacy&Us project deliverable, 2017, online: https://privacyus.eu/wordpress/wp-content/uploads/2017/10/D5_1.pdf.

Spiekermann, Sarah and Marie Caroline Oetzel. 2012. *Privacy-by-Design Through Systematic Privacy Impact Assessment – A Design Science Approach*. Rochester, NY: Social Science Research Network. Retrieved 3 October 2016 (http://papers.ssrn.com/abstract=2050872).

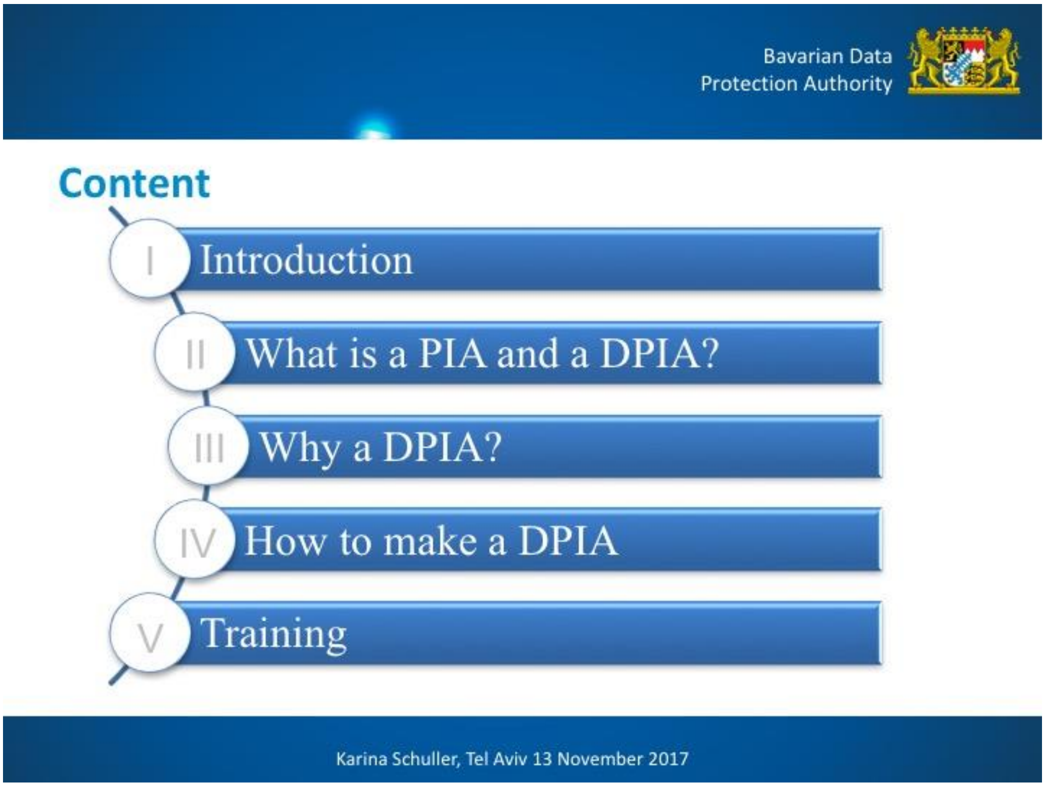
6 Annex 1: 2017/11/13 presentations by Karina Schuller and Dr. Ben Wagner



Bavarian Data
Protection Authority

Data Protection Impact Assessment
and
Risk Assessment

Karina Schuller, Tel Aviv 13 November 2017



Bavarian Data
Protection Authority

Content

I Introduction

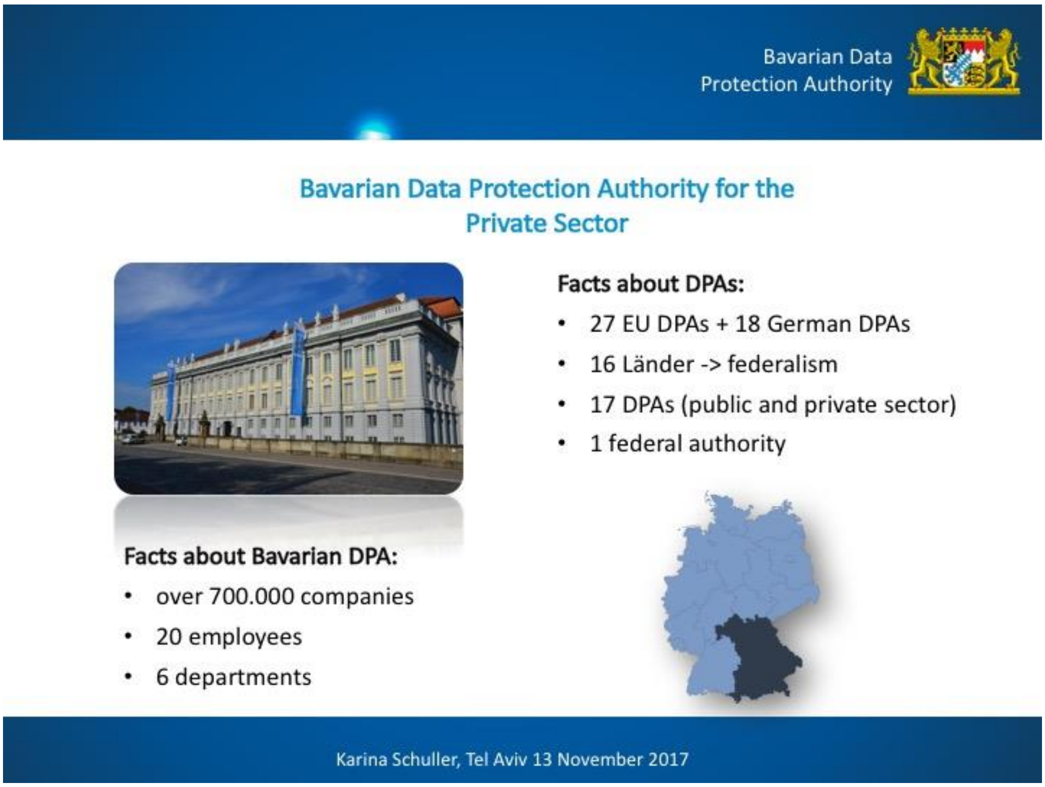
II What is a PIA and a DPIA?

III Why a DPIA?

IV How to make a DPIA

V Training

Karina Schuller, Tel Aviv 13 November 2017



Bavarian Data Protection Authority

Bavarian Data Protection Authority for the Private Sector

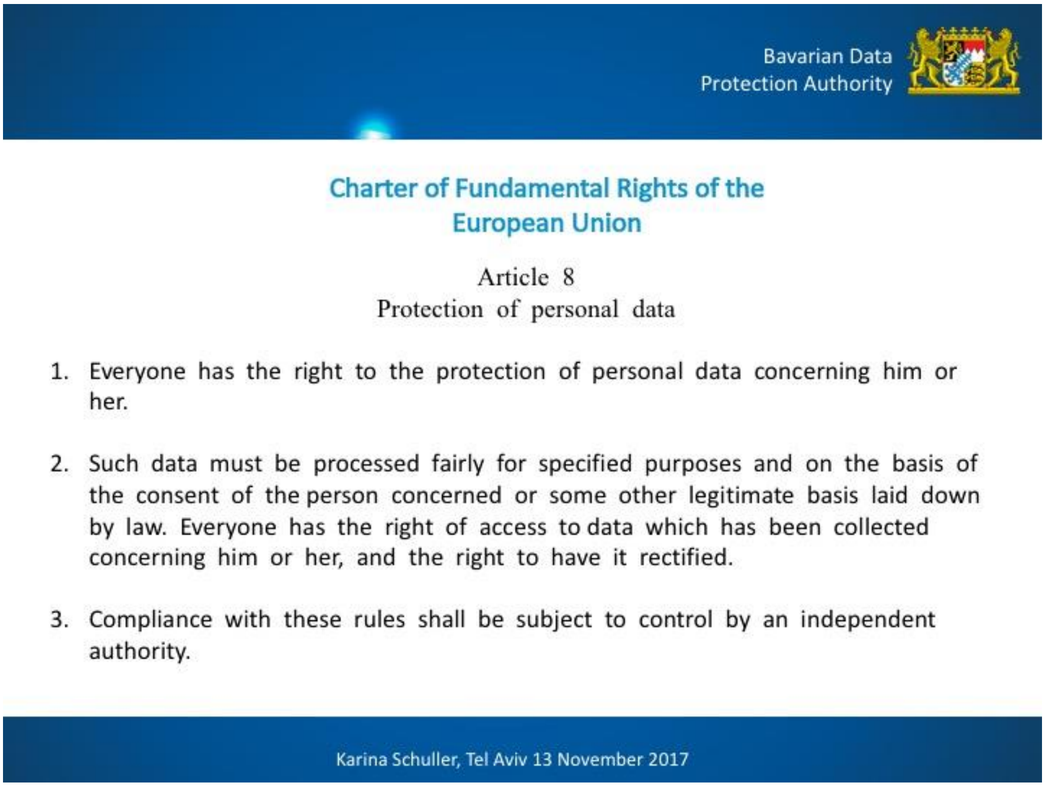
Facts about DPAs:

- 27 EU DPAs + 18 German DPAs
- 16 Länder -> federalism
- 17 DPAs (public and private sector)
- 1 federal authority

Facts about Bavarian DPA:

- over 700.000 companies
- 20 employees
- 6 departments

Karina Schuller, Tel Aviv 13 November 2017



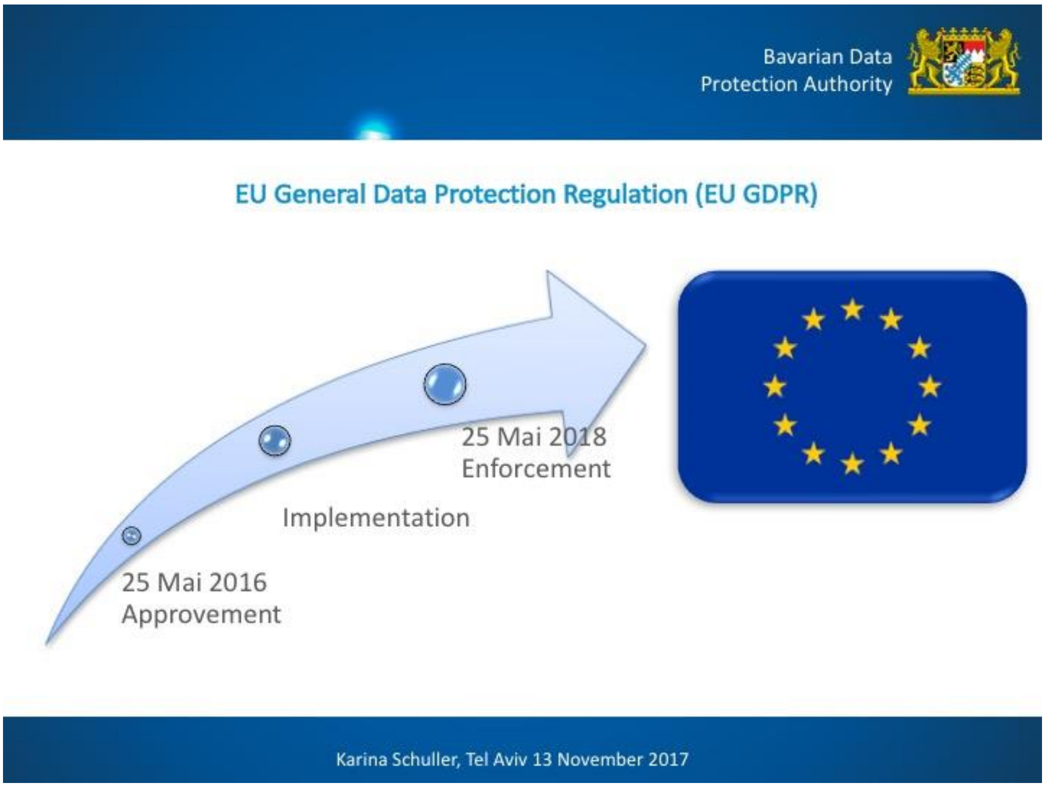
Bavarian Data Protection Authority

Charter of Fundamental Rights of the European Union

Article 8
Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

Karina Schuller, Tel Aviv 13 November 2017



Bavarian Data
Protection Authority

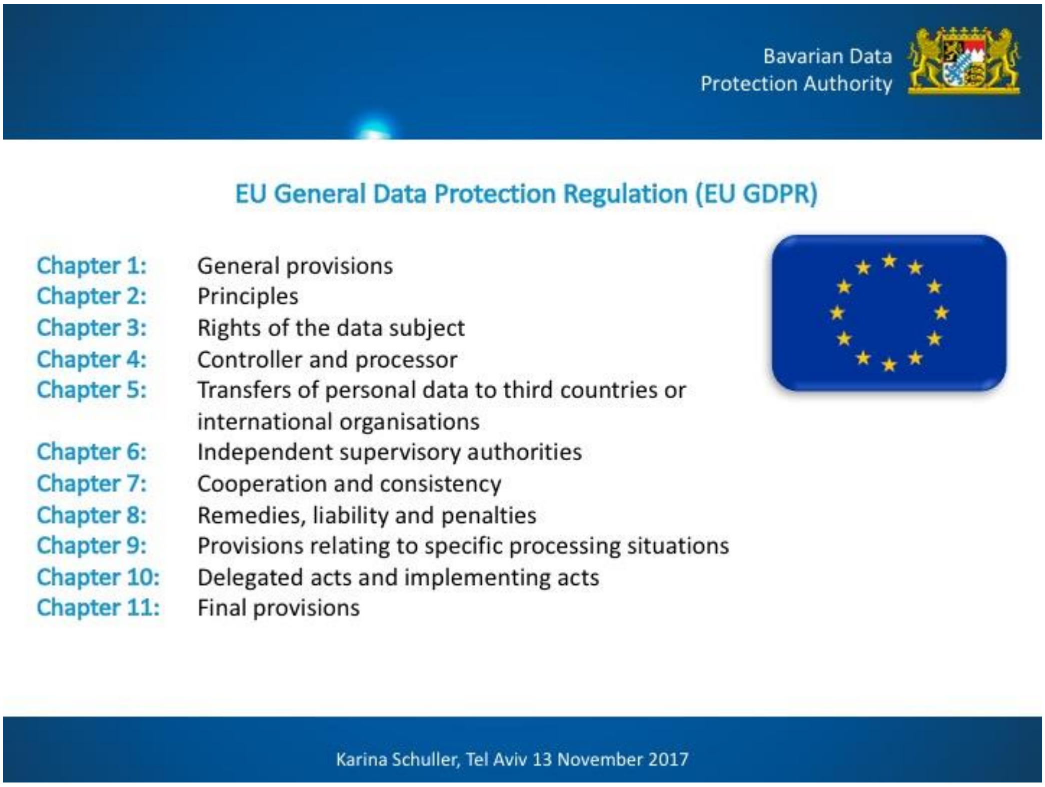
EU General Data Protection Regulation (EU GDPR)

25 Mai 2016
Approvement

Implementation

25 Mai 2018
Enforcement

Karina Schuller, Tel Aviv 13 November 2017

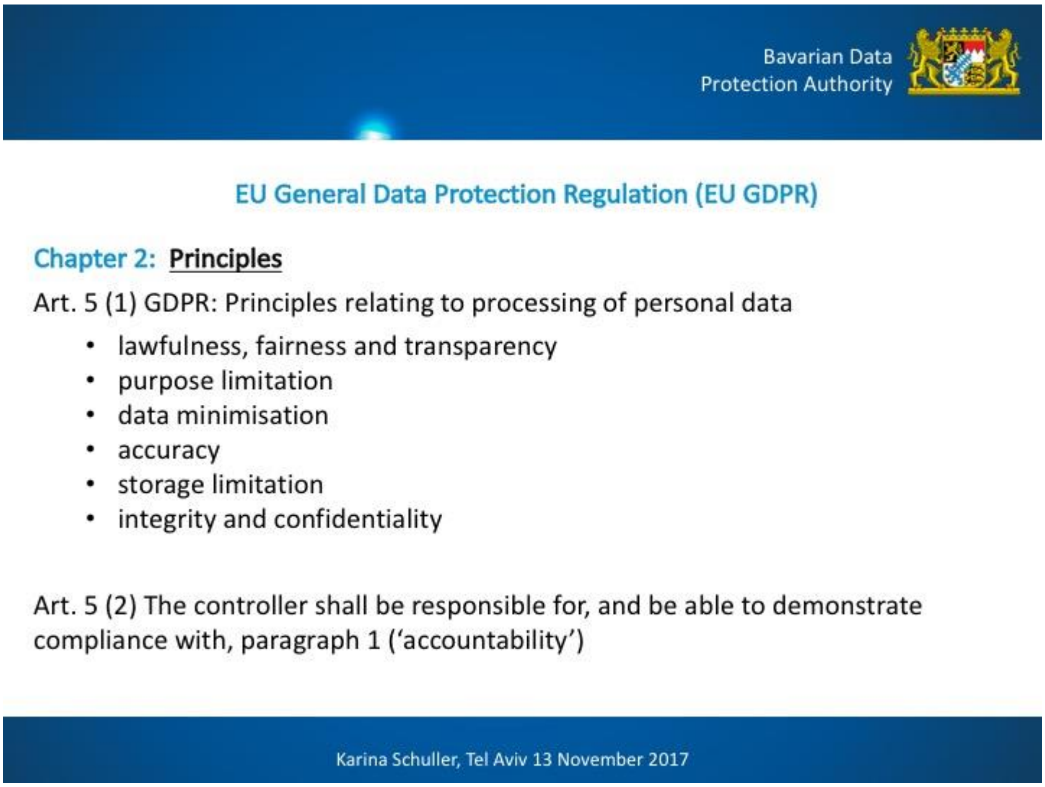


Bavarian Data
Protection Authority

EU General Data Protection Regulation (EU GDPR)

Chapter 1:	General provisions
Chapter 2:	Principles
Chapter 3:	Rights of the data subject
Chapter 4:	Controller and processor
Chapter 5:	Transfers of personal data to third countries or international organisations
Chapter 6:	Independent supervisory authorities
Chapter 7:	Cooperation and consistency
Chapter 8:	Remedies, liability and penalties
Chapter 9:	Provisions relating to specific processing situations
Chapter 10:	Delegated acts and implementing acts
Chapter 11:	Final provisions

Karina Schuller, Tel Aviv 13 November 2017



Bavarian Data
Protection Authority

EU General Data Protection Regulation (EU GDPR)

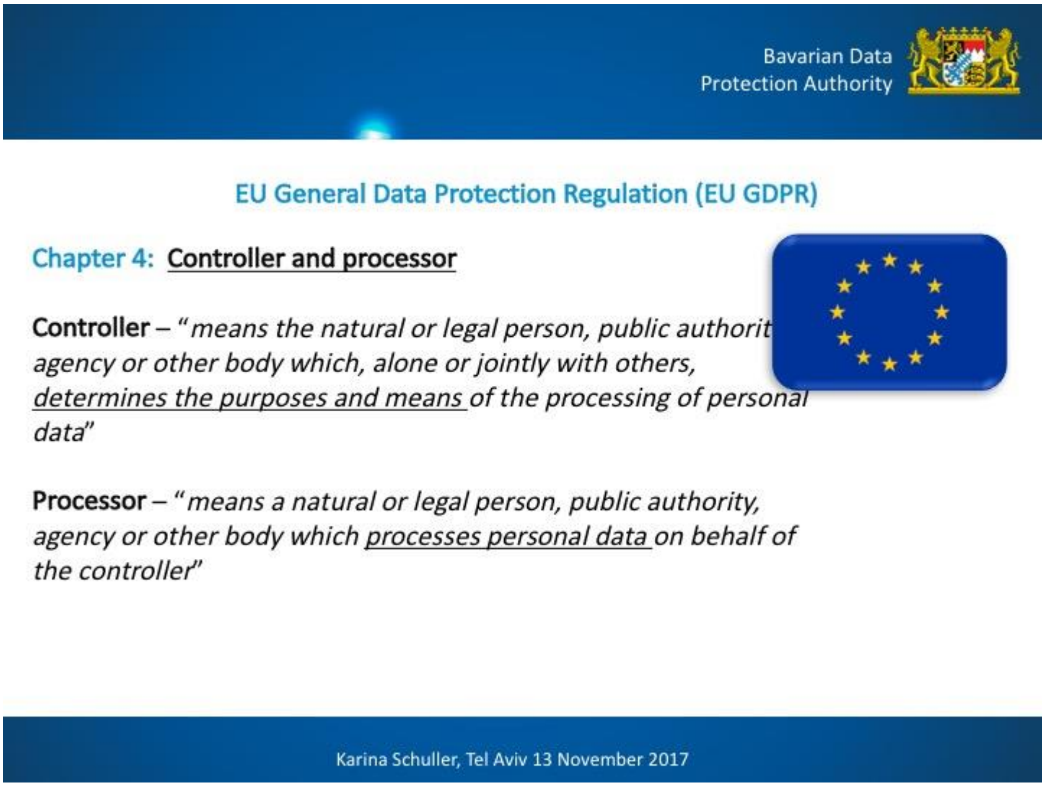
Chapter 2: Principles

Art. 5 (1) GDPR: Principles relating to processing of personal data

- lawfulness, fairness and transparency
- purpose limitation
- data minimisation
- accuracy
- storage limitation
- integrity and confidentiality

Art. 5 (2) The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')

Karina Schuller, Tel Aviv 13 November 2017



Bavarian Data
Protection Authority

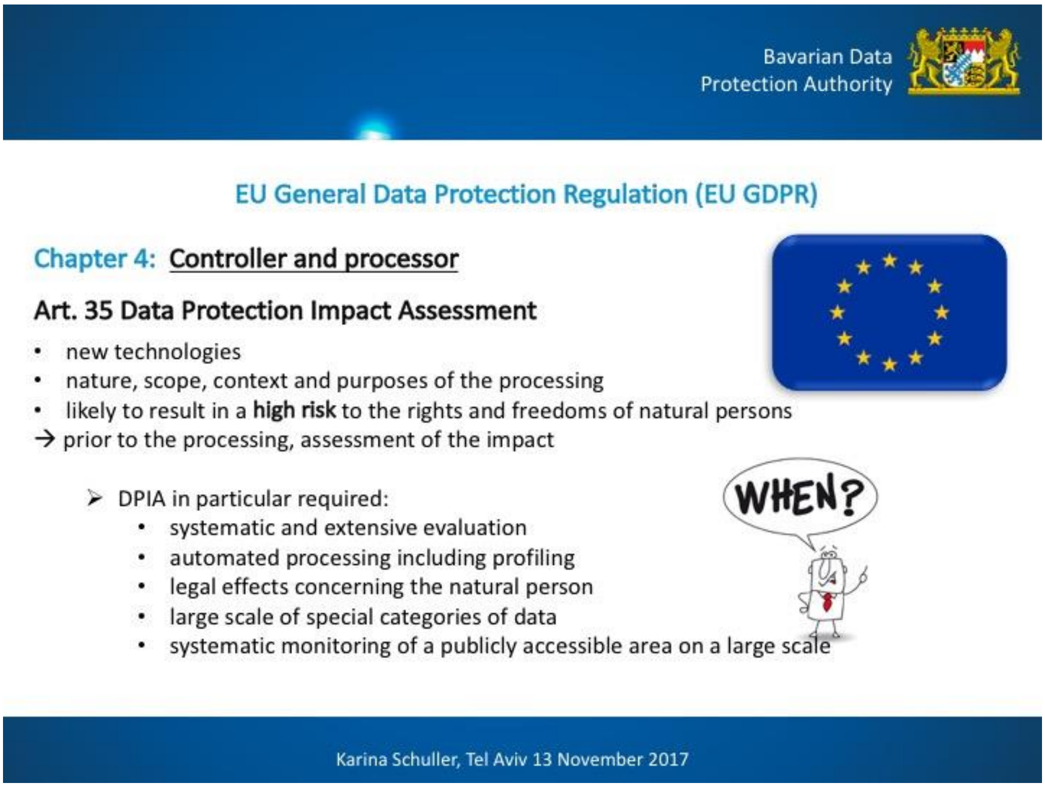
EU General Data Protection Regulation (EU GDPR)

Chapter 4: Controller and processor

Controller – "*means the natural or legal person, public authorit agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data*"

Processor – "*means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*"

Karina Schuller, Tel Aviv 13 November 2017



Bavarian Data
Protection Authority

EU General Data Protection Regulation (EU GDPR)

Chapter 4: Controller and processor

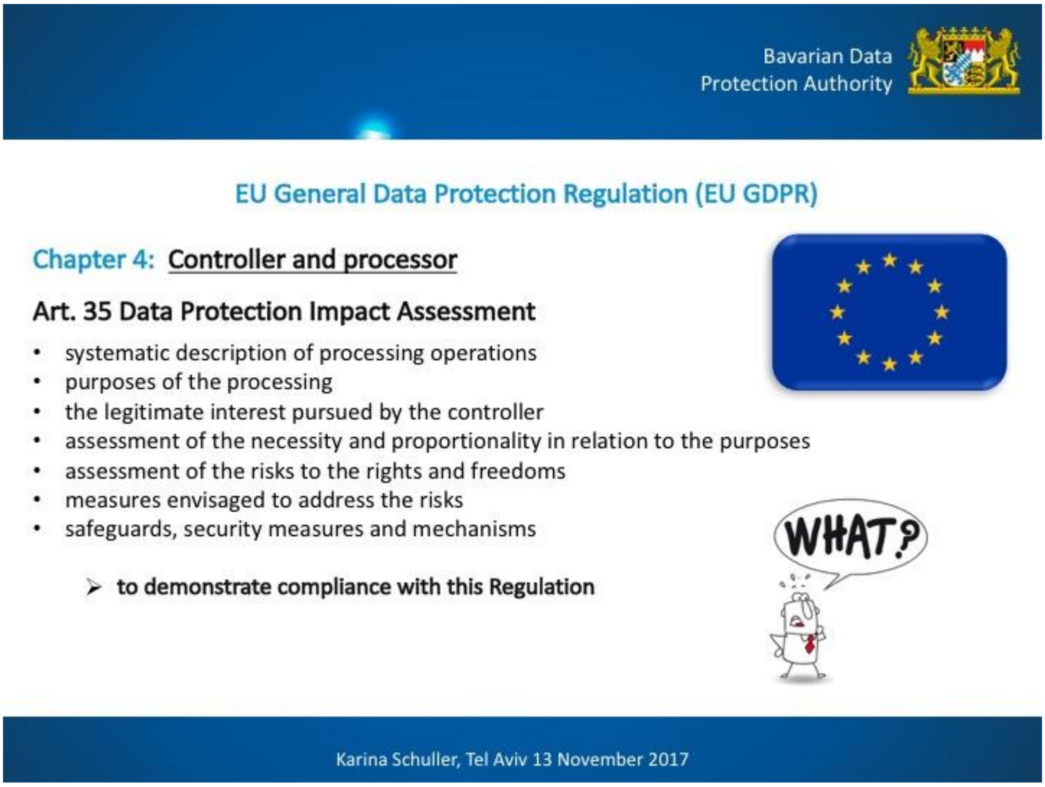
Art. 35 Data Protection Impact Assessment

- new technologies
- nature, scope, context and purposes of the processing
- likely to result in a **high risk** to the rights and freedoms of natural persons

→ prior to the processing, assessment of the impact

- ➢ DPIA in particular required:
  - systematic and extensive evaluation
  - automated processing including profiling
  - legal effects concerning the natural person
  - large scale of special categories of data
  - systematic monitoring of a publicly accessible area on a large scale

Karina Schuller, Tel Aviv 13 November 2017



Bavarian Data
Protection Authority

EU General Data Protection Regulation (EU GDPR)

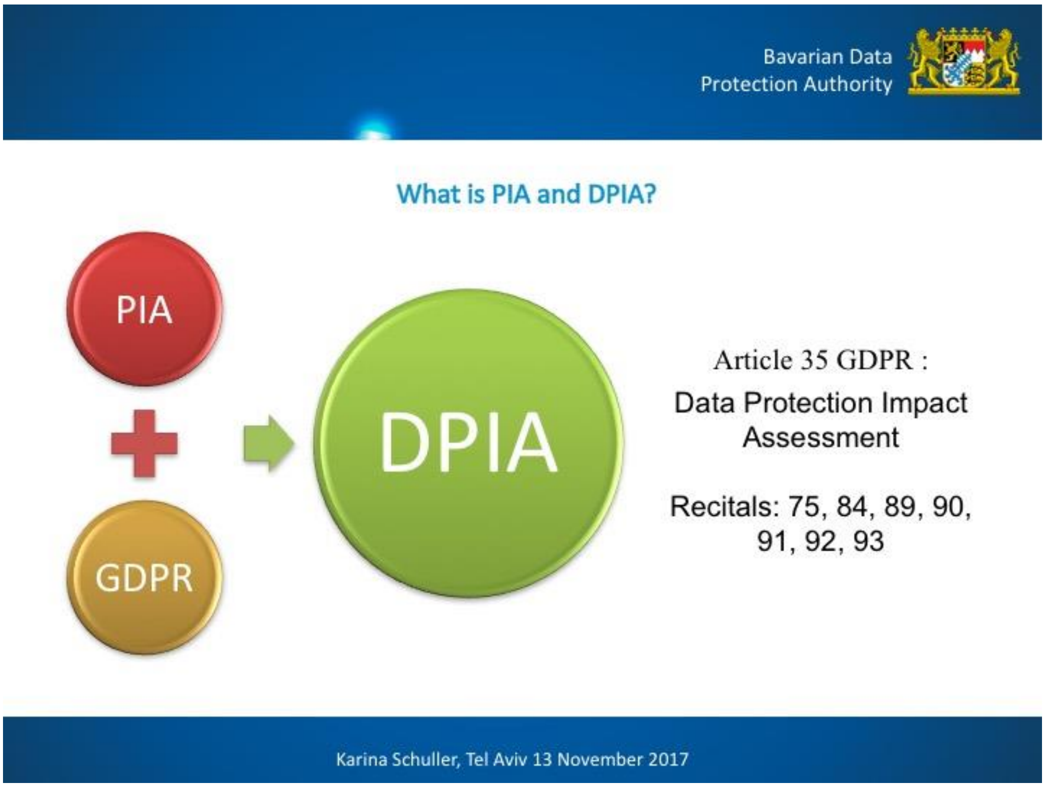
Chapter 4: Controller and processor

Art. 35 Data Protection Impact Assessment

- systematic description of processing operations
- purposes of the processing
- the legitimate interest pursued by the controller
- assessment of the necessity and proportionality in relation to the purposes
- assessment of the risks to the rights and freedoms
- measures envisaged to address the risks
- safeguards, security measures and mechanisms

➢ **to demonstrate compliance with this Regulation**

Karina Schuller, Tel Aviv 13 November 2017



Bavarian Data Protection Authority

What is PIA and DPIA?

PIA

GDPR

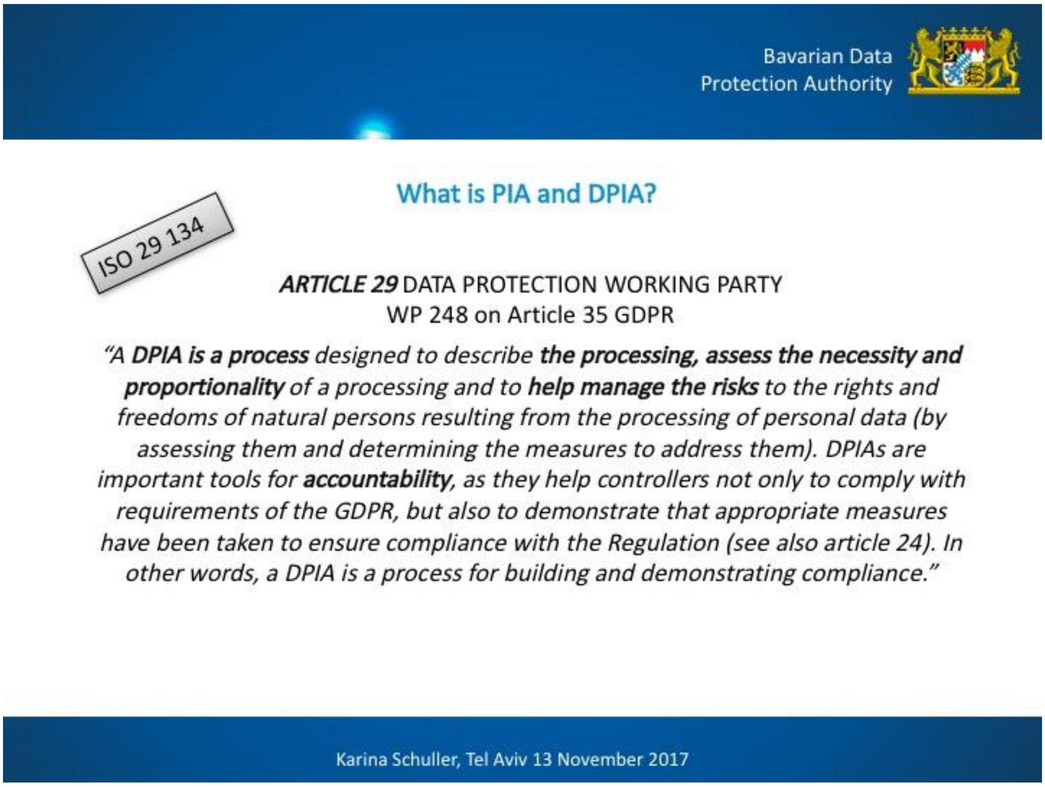
DPIA

Article 35 GDPR :

Data Protection Impact Assessment

Recitals: 75, 84, 89, 90, 91, 92, 93

Karina Schuller, Tel Aviv 13 November 2017



Bavarian Data Protection Authority

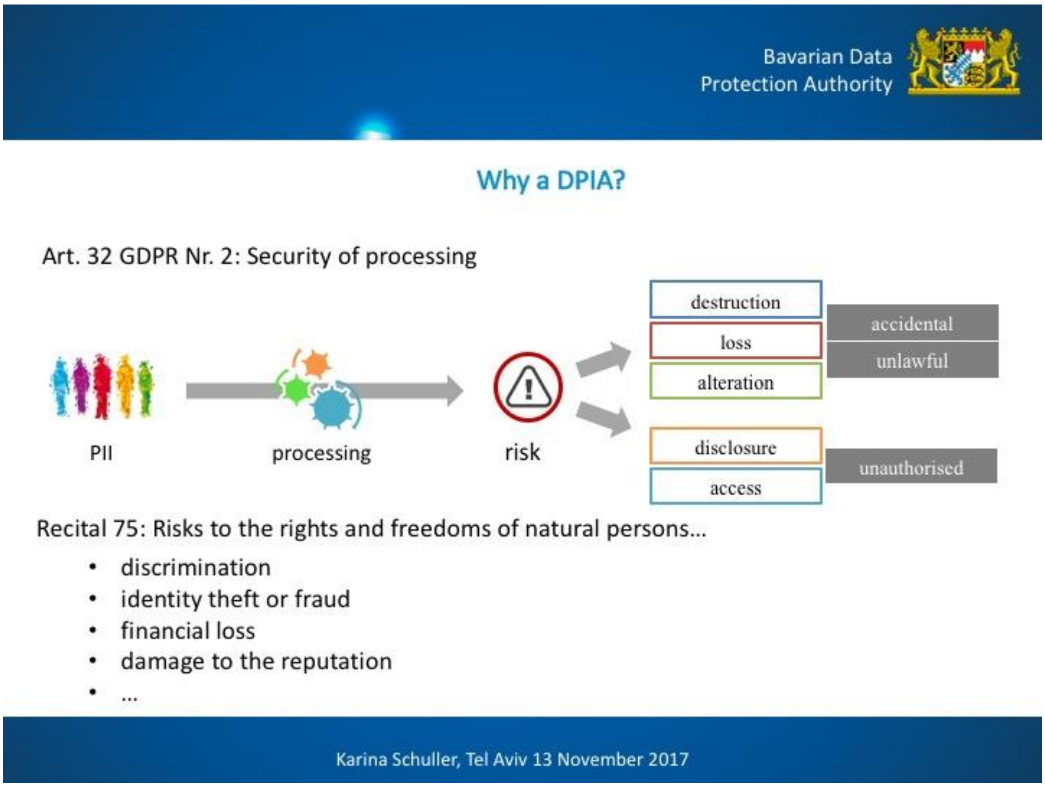
What is PIA and DPIA?

ISO 29 134

ARTICLE 29 DATA PROTECTION WORKING PARTY
WP 248 on Article 35 GDPR

*"A **DPIA is a process** designed to describe **the processing, assess the necessity and proportionality** of a processing and to **help manage the risks** to the rights and freedoms of natural persons resulting from the processing of personal data (by assessing them and determining the measures to address them). DPIAs are important tools for **accountability**, as they help controllers not only to comply with requirements of the GDPR, but also to demonstrate that appropriate measures have been taken to ensure compliance with the Regulation (see also article 24). In other words, a DPIA is a process for building and demonstrating compliance."*

Karina Schuller, Tel Aviv 13 November 2017



Bavarian Data Protection Authority

Why a DPIA?

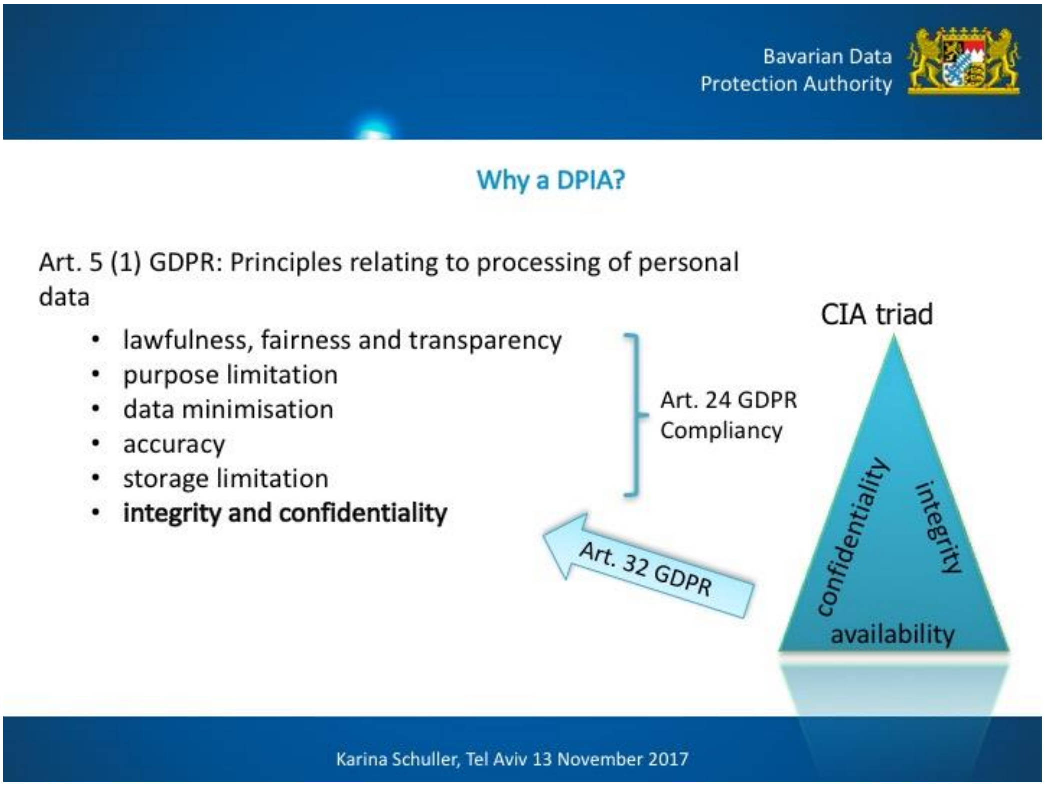
Art. 32 GDPR Nr. 2: Security of processing

PII
processing
risk
destruction
loss
alteration
disclosure
access
accidental
unlawful
unauthorised

Recital 75: Risks to the rights and freedoms of natural persons…

- discrimination
- identity theft or fraud
- financial loss
- damage to the reputation
- …

Karina Schuller, Tel Aviv 13 November 2017



Bavarian Data Protection Authority

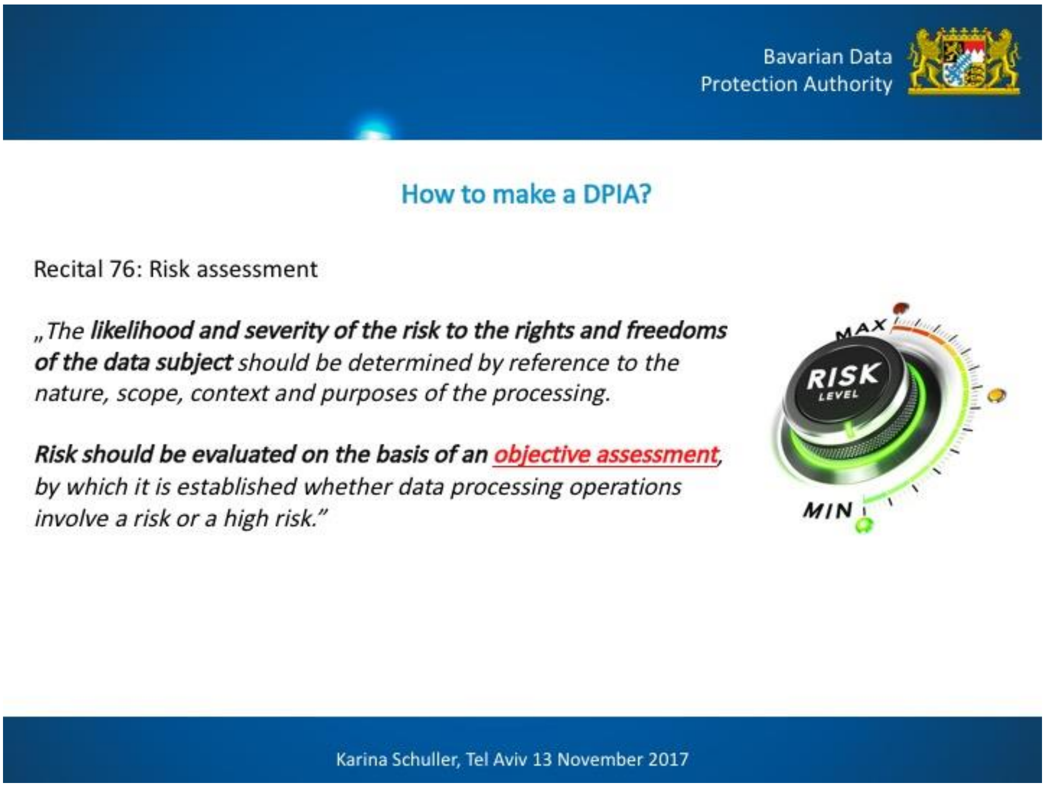
Why a DPIA?

Art. 5 (1) GDPR: Principles relating to processing of personal data

- lawfulness, fairness and transparency
- purpose limitation
- data minimisation
- accuracy
- storage limitation
- **integrity and confidentiality**

Art. 24 GDPR
Compliancy
CIA triad
confidentiality
integrity
availability
Art. 32 GDPR

Karina Schuller, Tel Aviv 13 November 2017



Bavarian Data
Protection Authority

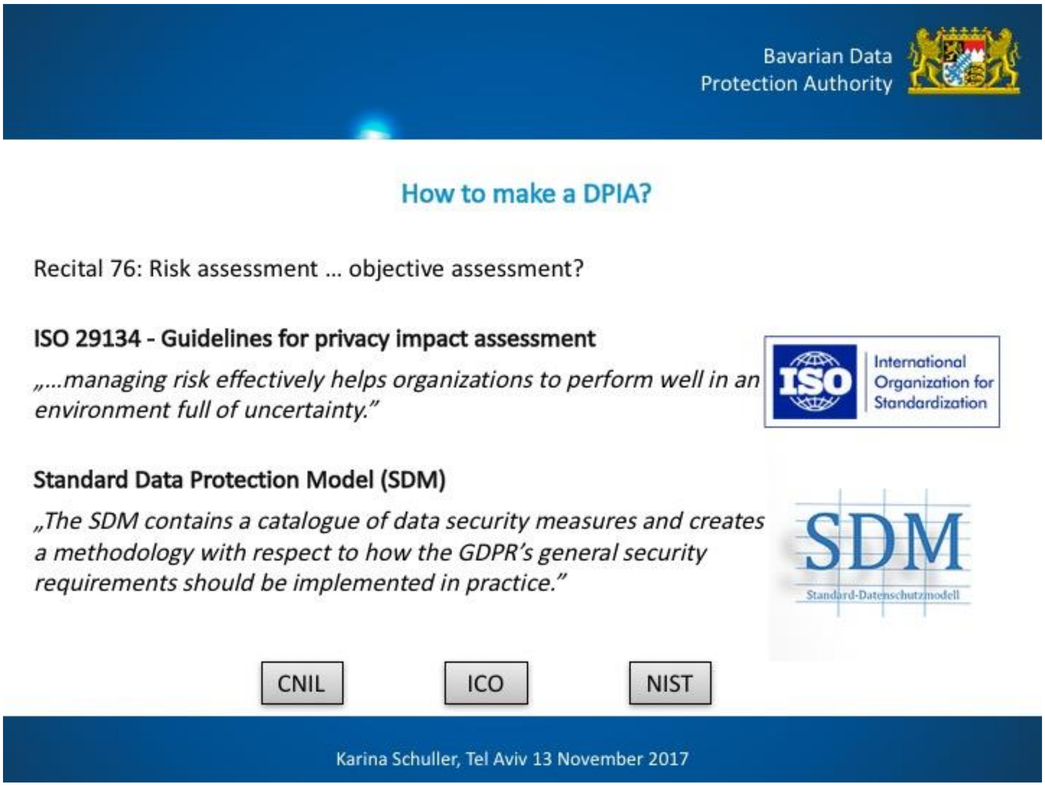
How to make a DPIA?

Recital 76: Risk assessment

*„The **likelihood and severity of the risk to the rights and freedoms of the data subject** should be determined by reference to the nature, scope, context and purposes of the processing.*

***Risk should be evaluated on the basis of an objective assessment,** by which it is established whether data processing operations involve a risk or a high risk."*

Karina Schuller, Tel Aviv 13 November 2017



Bavarian Data
Protection Authority

How to make a DPIA?

Recital 76: Risk assessment … objective assessment?

ISO 29134 - Guidelines for privacy impact assessment

„…managing risk effectively helps organizations to perform well in an environment full of uncertainty."

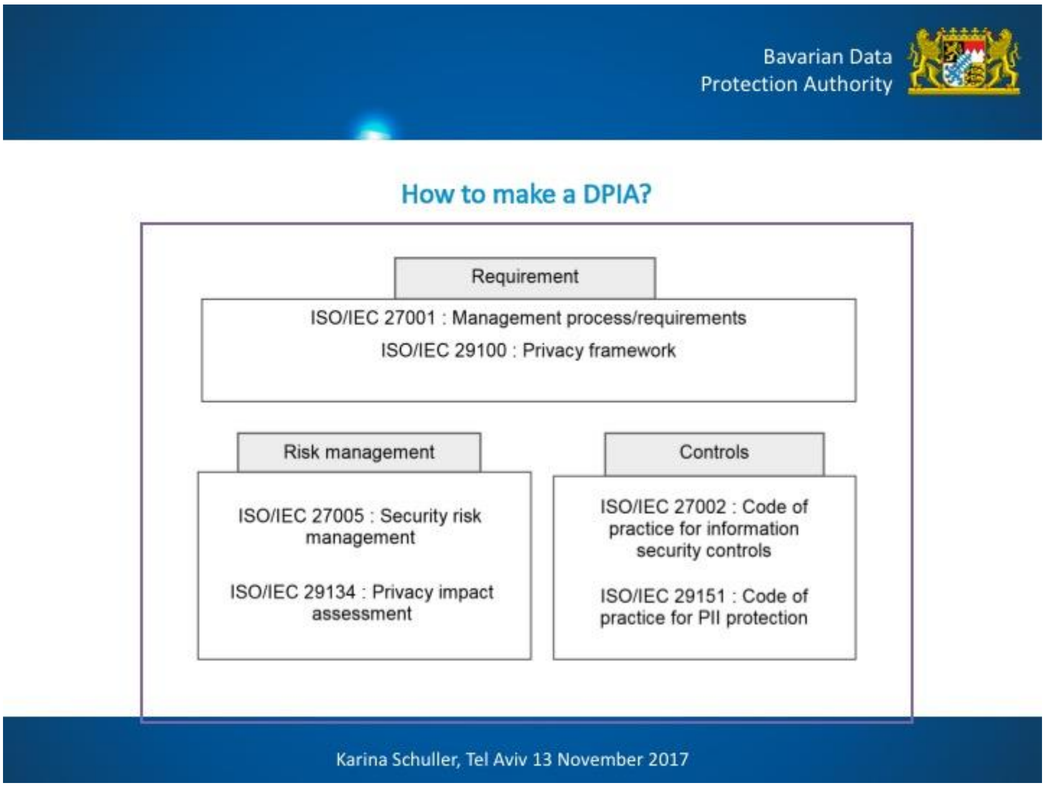
ISO
International Organization for Standardization

Standard Data Protection Model (SDM)

„The SDM contains a catalogue of data security measures and creates a methodology with respect to how the GDPR's general security requirements should be implemented in practice."

CNIL ICO NIST

Karina Schuller, Tel Aviv 13 November 2017



Bavarian Data
Protection Authority

How to make a DPIA?

Requirement

ISO/IEC 27001 : Management process/requirements
ISO/IEC 29100 : Privacy framework

Risk management

ISO/IEC 27005 : Security risk management

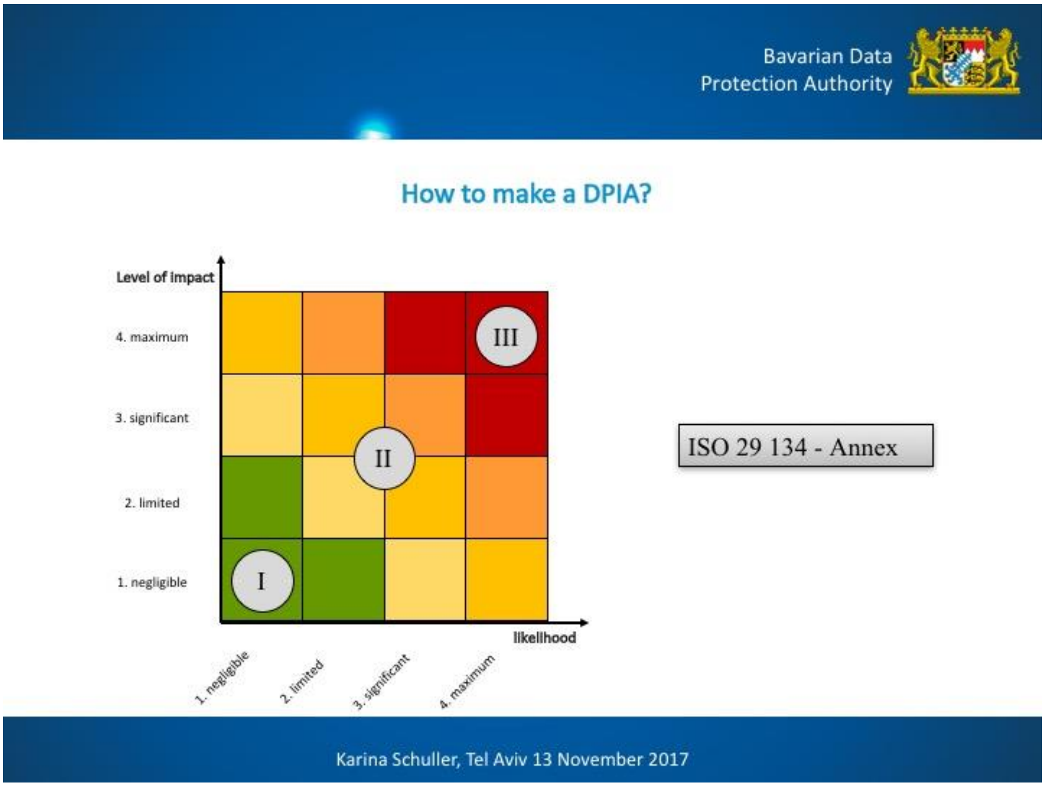
ISO/IEC 29134 : Privacy impact assessment

Controls

ISO/IEC 27002 : Code of practice for information security controls

ISO/IEC 29151 : Code of practice for PII protection

Karina Schuller, Tel Aviv 13 November 2017

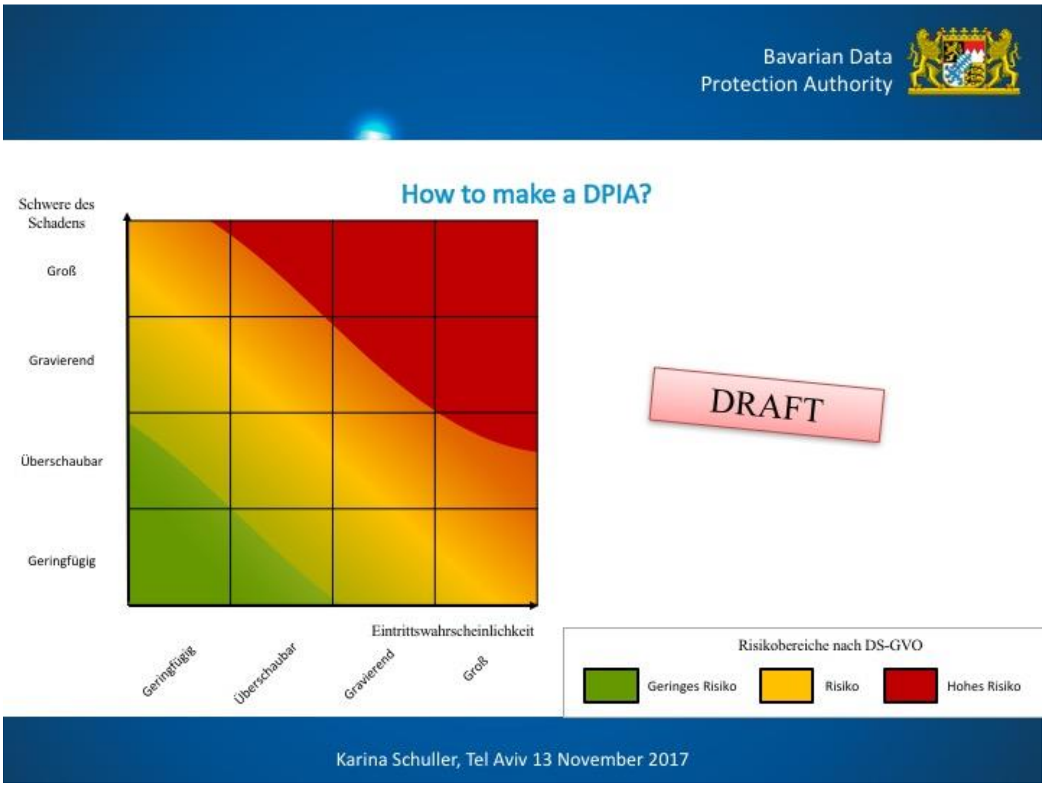


Bavarian Data
Protection Authority

How to make a DPIA?

ISO 29 134 - Annex

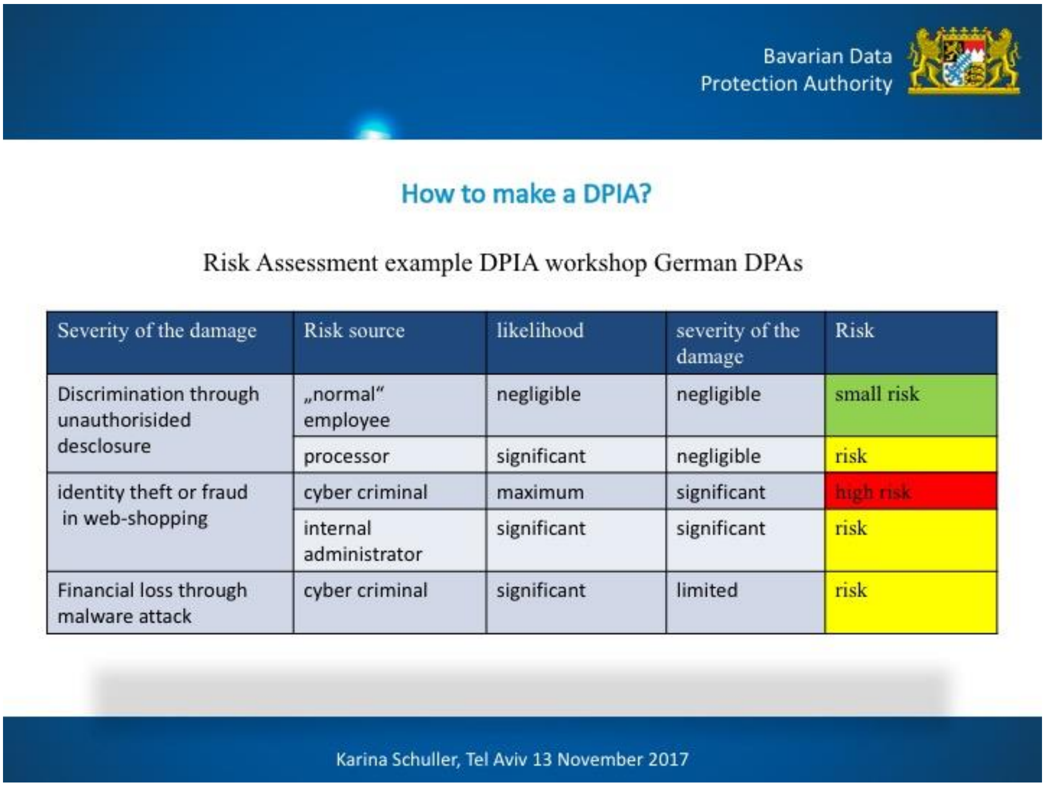
Karina Schuller, Tel Aviv 13 November 2017



Bavarian Data
Protection Authority

How to make a DPIA?

Karina Schuller, Tel Aviv 13 November 2017



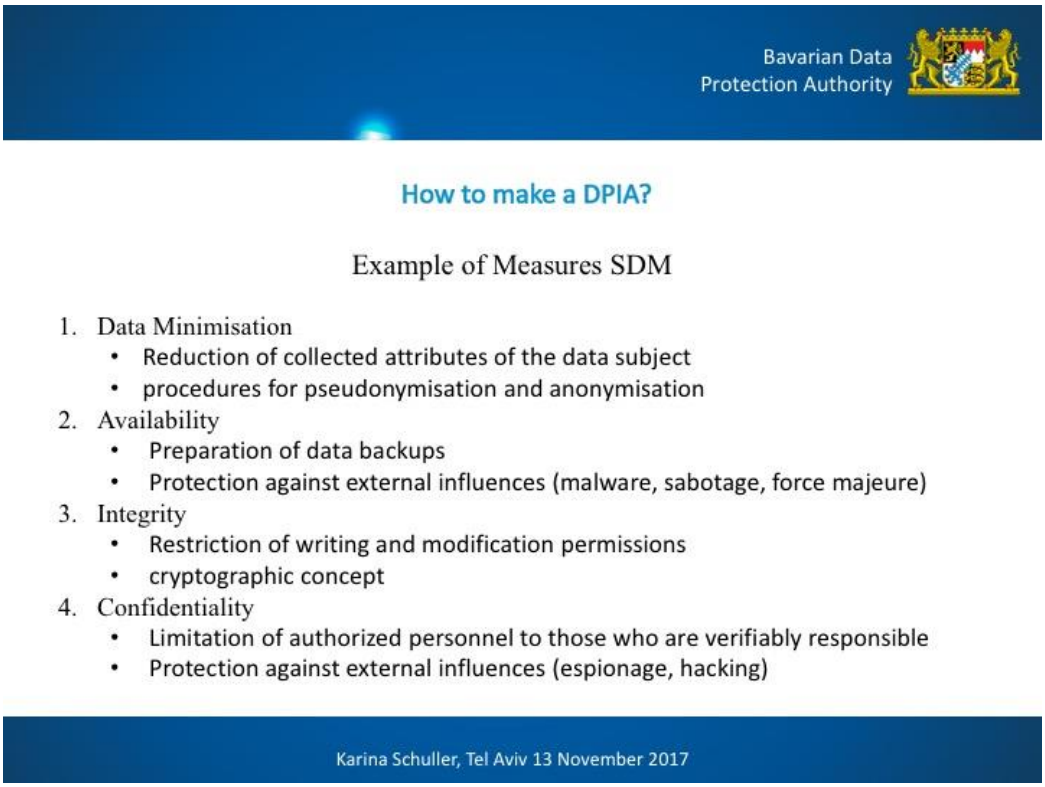
Bavarian Data
Protection Authority

How to make a DPIA?

Risk Assessment example DPIA workshop German DPAs

Severity of the damage	Risk source	likelihood	severity of the damage	Risk
Discrimination through unauthorisided desclosure	„normal“ employee	negligible	negligible	small risk
	processor	significant	negligible	risk
identity theft or fraud in web-shopping	cyber criminal	maximum	significant	high risk
	internal administrator	significant	significant	risk
Financial loss through malware attack	cyber criminal	significant	limited	risk

Karina Schuller, Tel Aviv 13 November 2017



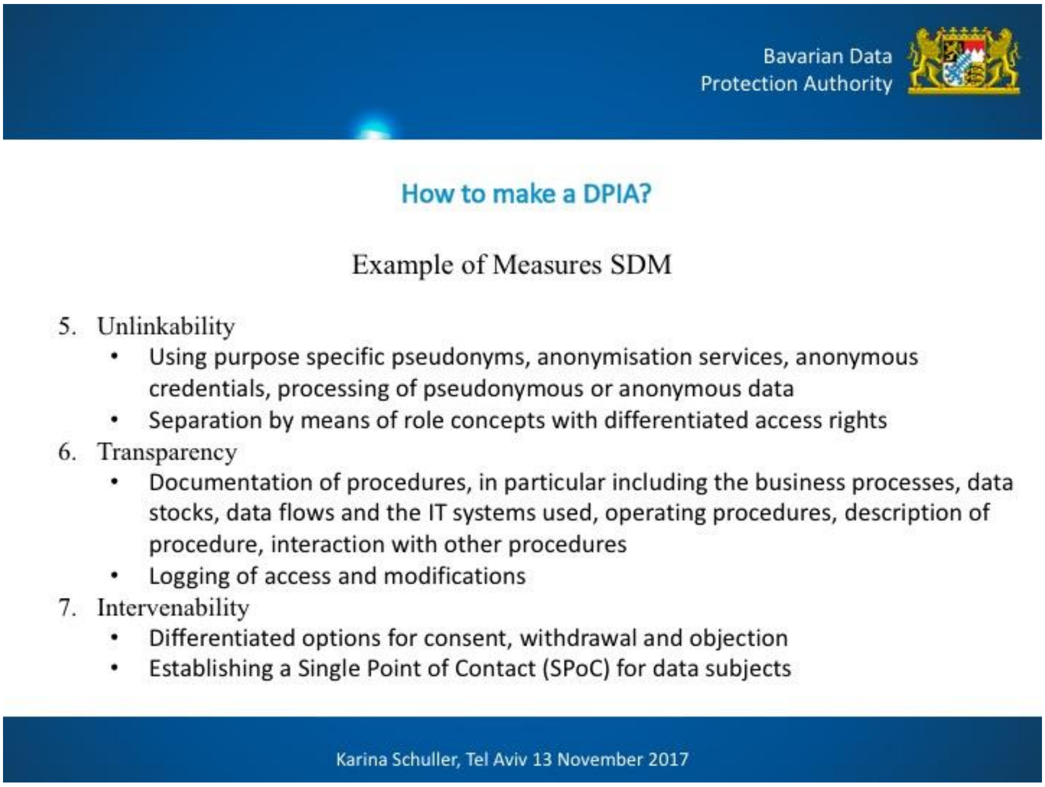
Bavarian Data
Protection Authority

How to make a DPIA?

Example of Measures SDM

1. Data Minimisation
   - Reduction of collected attributes of the data subject
   - procedures for pseudonymisation and anonymisation
2. Availability
   - Preparation of data backups
   - Protection against external influences (malware, sabotage, force majeure)
3. Integrity
   - Restriction of writing and modification permissions
   - cryptographic concept
4. Confidentiality
   - Limitation of authorized personnel to those who are verifiably responsible
   - Protection against external influences (espionage, hacking)

Karina Schuller, Tel Aviv 13 November 2017



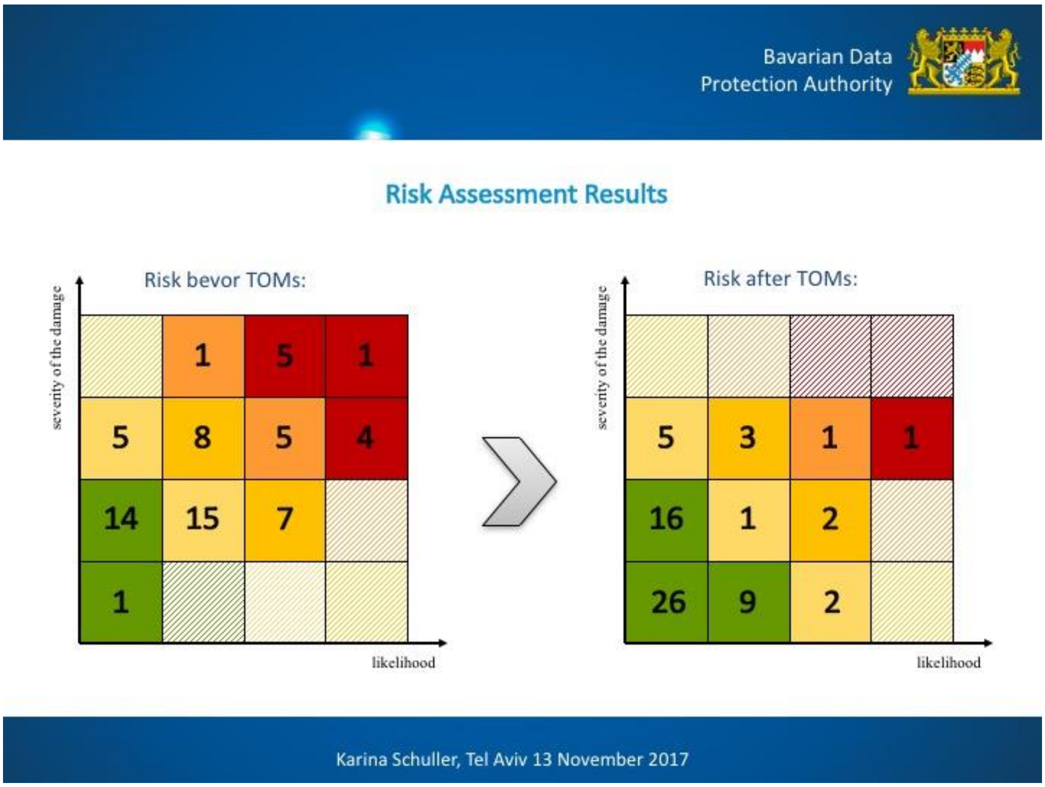
Bavarian Data
Protection Authority

How to make a DPIA?

Example of Measures SDM

5. Unlinkability
   - Using purpose specific pseudonyms, anonymisation services, anonymous credentials, processing of pseudonymous or anonymous data
   - Separation by means of role concepts with differentiated access rights
6. Transparency
   - Documentation of procedures, in particular including the business processes, data stocks, data flows and the IT systems used, operating procedures, description of procedure, interaction with other procedures
   - Logging of access and modifications
7. Intervenability
   - Differentiated options for consent, withdrawal and objection
   - Establishing a Single Point of Contact (SPoC) for data subjects

Karina Schuller, Tel Aviv 13 November 2017



Bavarian Data
Protection Authority

Risk Assessment Results

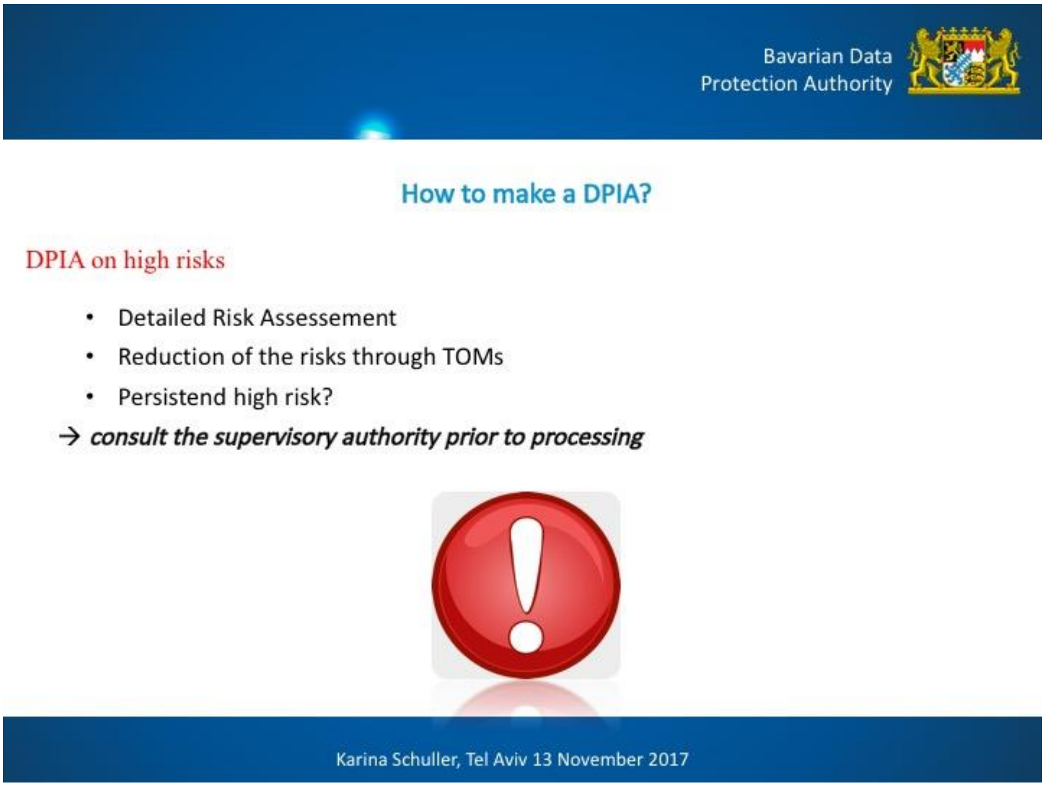
Risk bevor TOMs:

	1	5	1
5	8	5	4
14	15	7	
1			

Risk after TOMs:

5	3	1	1
16	1	2	
26	9	2	

Karina Schuller, Tel Aviv 13 November 2017



Bavarian Data
Protection Authority

How to make a DPIA?

DPIA on high risks

- Detailed Risk Assessement
- Reduction of the risks through TOMs
- Persistend high risk?

→ *consult the supervisory authority prior to processing*

Karina Schuller, Tel Aviv 13 November 2017

Bavarian Data Protection Authority

Thank you for your attention!

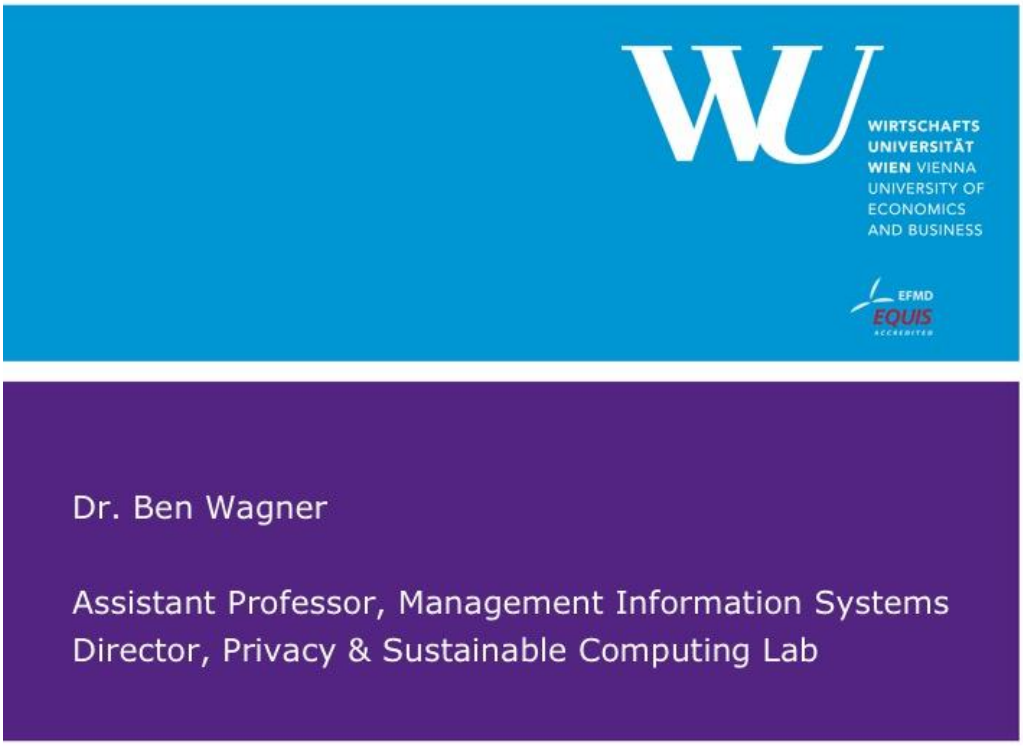
www.lda.bayern.de

BayLDA - Official Website

Welcome to the Bavarian Data Protection Authority (BayLDA)

Our website provides a large number of information about privacy, mostly even in English. You are invited to read our articles and publications. If you have any question, feel free to contact us.

Karina Schuller, Tel Aviv 13 November 2017

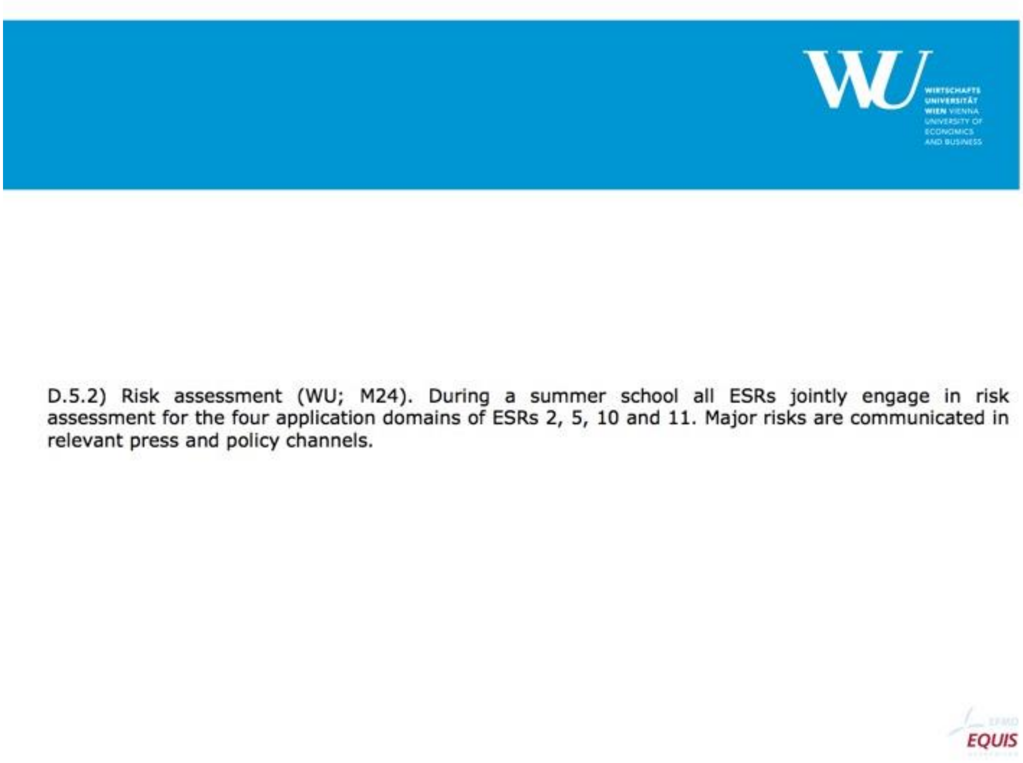


WIRTSCHAFTS UNIVERSITÄT WIEN VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS

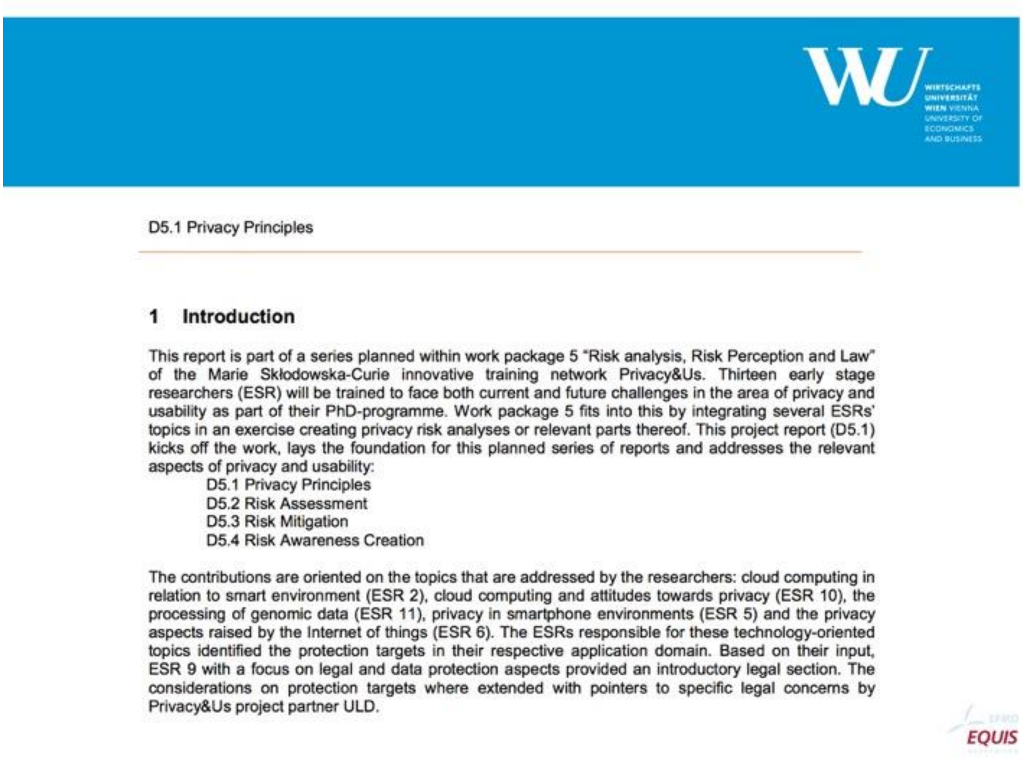
EFMD
EQUIS
ACCREDITED

Dr. Ben Wagner

Assistant Professor, Management Information Systems
Director, Privacy & Sustainable Computing Lab



D.5.2) Risk assessment (WU; M24). During a summer school all ESRs jointly engage in risk assessment for the four application domains of ESRs 2, 5, 10 and 11. Major risks are communicated in relevant press and policy channels.



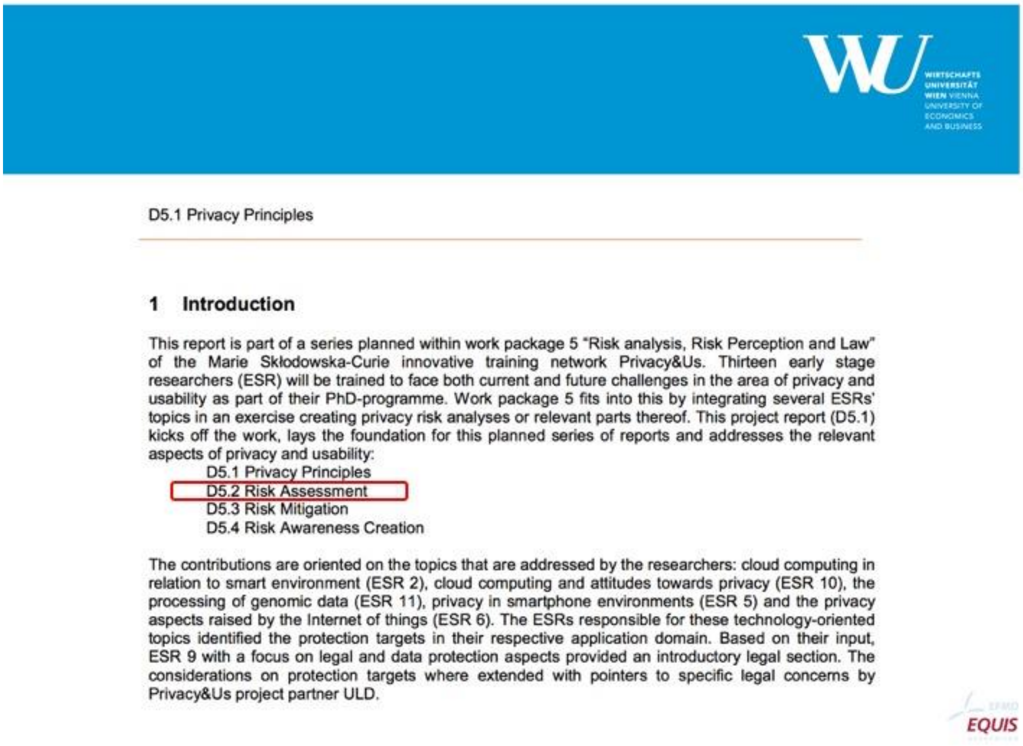
D5.1 Privacy Principles

1 Introduction

This report is part of a series planned within work package 5 "Risk analysis, Risk Perception and Law" of the Marie Skłodowska-Curie innovative training network Privacy&Us. Thirteen early stage researchers (ESR) will be trained to face both current and future challenges in the area of privacy and usability as part of their PhD-programme. Work package 5 fits into this by integrating several ESRs' topics in an exercise creating privacy risk analyses or relevant parts thereof. This project report (D5.1) kicks off the work, lays the foundation for this planned series of reports and addresses the relevant aspects of privacy and usability:

D5.1 Privacy Principles
D5.2 Risk Assessment
D5.3 Risk Mitigation
D5.4 Risk Awareness Creation

The contributions are oriented on the topics that are addressed by the researchers: cloud computing in relation to smart environment (ESR 2), cloud computing and attitudes towards privacy (ESR 10), the processing of genomic data (ESR 11), privacy in smartphone environments (ESR 5) and the privacy aspects raised by the Internet of things (ESR 6). The ESRs responsible for these technology-oriented topics identified the protection targets in their respective application domain. Based on their input, ESR 9 with a focus on legal and data protection aspects provided an introductory legal section. The considerations on protection targets where extended with pointers to specific legal concerns by Privacy&Us project partner ULD.



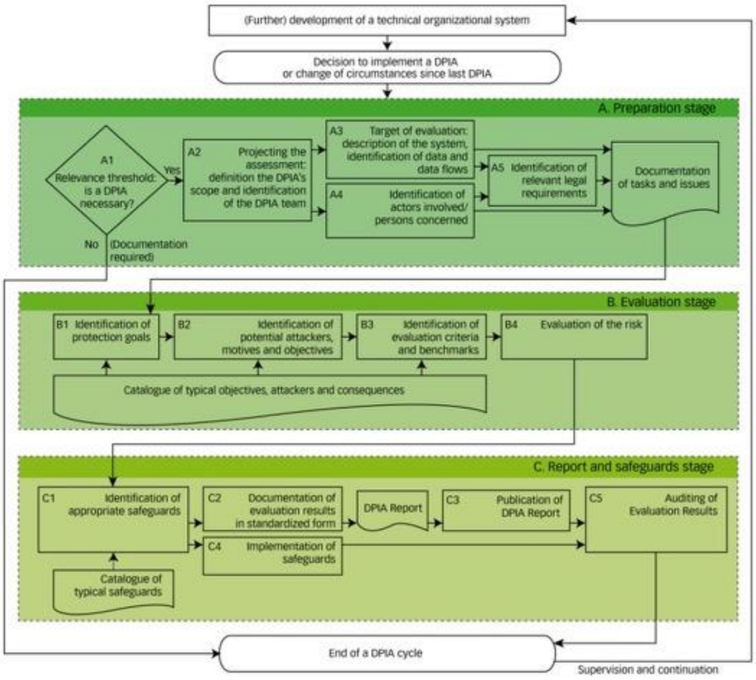
D5.1 Privacy Principles

1 Introduction

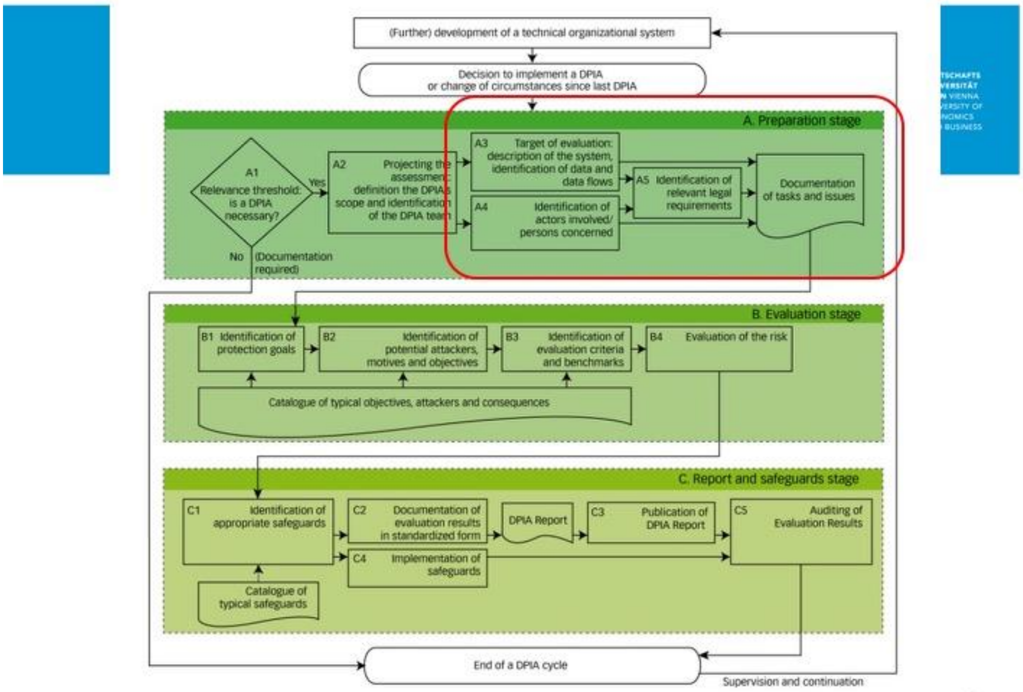
This report is part of a series planned within work package 5 "Risk analysis, Risk Perception and Law" of the Marie Skłodowska-Curie innovative training network Privacy&Us. Thirteen early stage researchers (ESR) will be trained to face both current and future challenges in the area of privacy and usability as part of their PhD-programme. Work package 5 fits into this by integrating several ESRs' topics in an exercise creating privacy risk analyses or relevant parts thereof. This project report (D5.1) kicks off the work, lays the foundation for this planned series of reports and addresses the relevant aspects of privacy and usability:

D5.1 Privacy Principles
D5.2 Risk Assessment
D5.3 Risk Mitigation
D5.4 Risk Awareness Creation

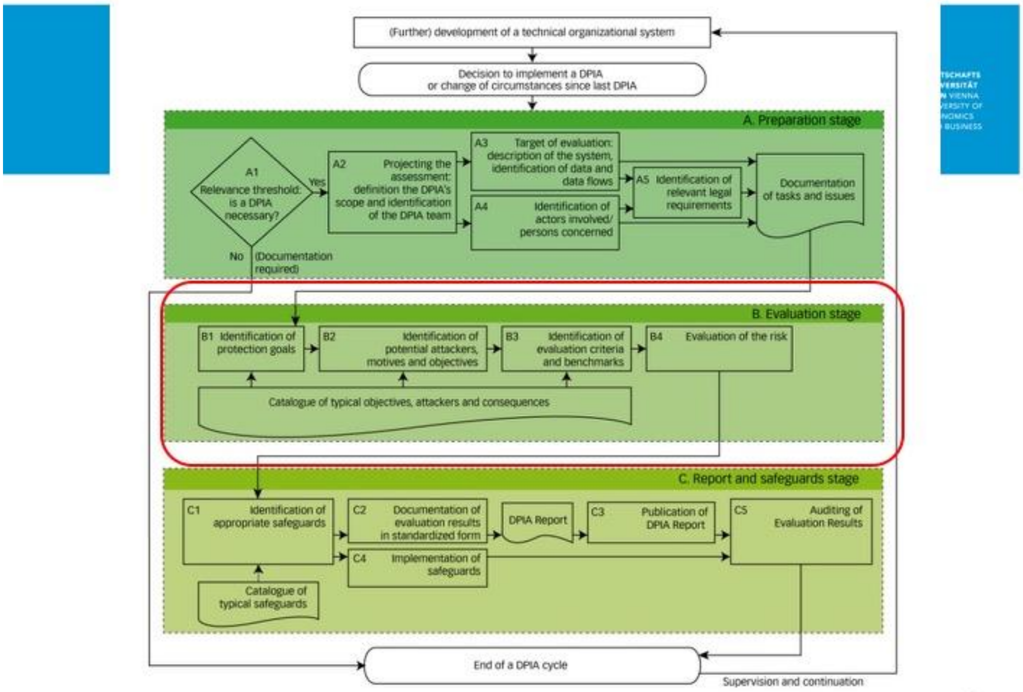
The contributions are oriented on the topics that are addressed by the researchers: cloud computing in relation to smart environment (ESR 2), cloud computing and attitudes towards privacy (ESR 10), the processing of genomic data (ESR 11), privacy in smartphone environments (ESR 5) and the privacy aspects raised by the Internet of things (ESR 6). The ESRs responsible for these technology-oriented topics identified the protection targets in their respective application domain. Based on their input, ESR 9 with a focus on legal and data protection aspects provided an introductory legal section. The considerations on protection targets where extended with pointers to specific legal concerns by Privacy&Us project partner ULD.


(Further) development of a technical organizational system
Decision to implement a DPIA or change of circumstances since last DPIA
A. Preparation stage
A1 Relevance threshold: is a DPIA necessary?
Yes
No
(Documentation required)
A2 Projecting the assessment: definition the DPIA's scope and identification of the DPIA team
A3 Target of evaluation: description of the system, identification of data and data flows
A4 Identification of actors involved/ persons concerned
A5 Identification of relevant legal requirements
Documentation of tasks and issues
B. Evaluation stage
B1 Identification of protection goals
B2 Identification of potential attackers, motives and objectives
B3 Identification of evaluation criteria and benchmarks
B4 Evaluation of the risk
Catalogue of typical objectives, attackers and consequences
C. Report and safeguards stage
C1 Identification of appropriate safeguards
C2 Documentation of evaluation results in standardized form
DPIA Report
C3 Publication of DPIA Report
C5 Auditing of Evaluation Results
C4 Implementation of safeguards
Catalogue of typical safeguards
End of a DPIA cycle
Supervision and continuation

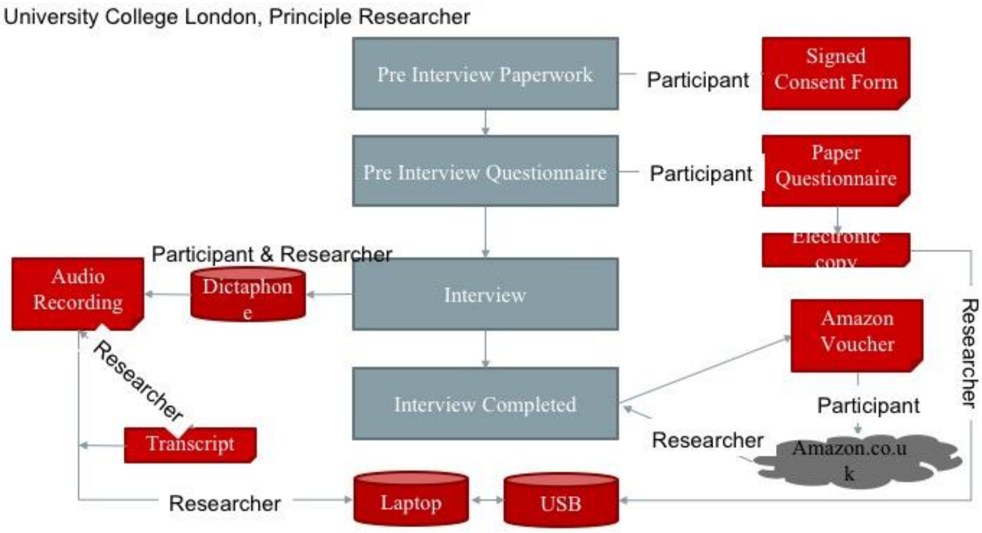
Bieker, Felix, Michael Friedewald, Marit Hansen, Hannah Obersteller, and Martin Rost. 2016. 'A Process for Data Protection Impact Assessment under the European General Data Protection Regulation'. Pp. 21–37 in *Annual Privacy Forum*. Springer.


(Further) development of a technical organizational system
Decision to implement a DPIA or change of circumstances since last DPIA
A. Preparation stage
A1 Relevance threshold: is a DPIA necessary?
Yes
No
(Documentation required)
A2 Projecting the assessment: definition the DPIA's scope and identification of the DPIA team
A3 Target of evaluation: description of the system, identification of data and data flows
A4 Identification of actors involved/ persons concerned
A5 Identification of relevant legal requirements
Documentation of tasks and issues
B. Evaluation stage
B1 Identification of protection goals
B2 Identification of potential attackers, motives and objectives
B3 Identification of evaluation criteria and benchmarks
B4 Evaluation of the risk
Catalogue of typical objectives, attackers and consequences
C. Report and safeguards stage
C1 Identification of appropriate safeguards
C2 Documentation of evaluation results in standardized form
DPIA Report
C3 Publication of DPIA Report
C5 Auditing of Evaluation Results
C4 Implementation of safeguards
Catalogue of typical safeguards
End of a DPIA cycle
Supervision and continuation

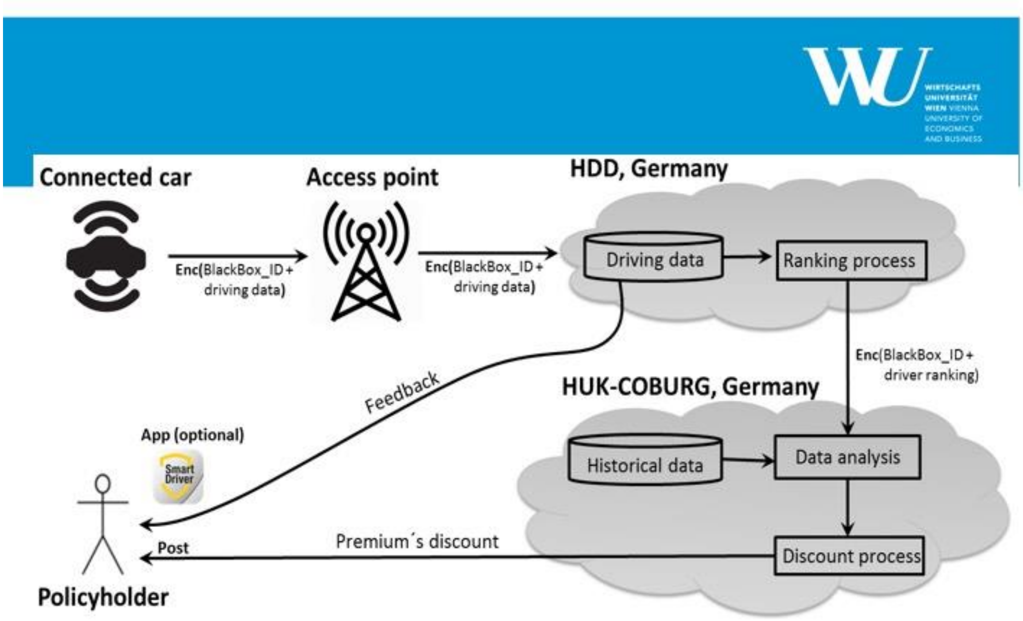
Preparation Stage – Before Tel Aviv


(Further) development of a technical organizational system
Decision to implement a DPIA or change of circumstances since last DPIA
A. Preparation stage
A1 Relevance threshold: is a DPIA necessary?
Yes
No
(Documentation required)
A2 Projecting the assessment: definition the DPIA's scope and identification of the DPIA team
A3 Target of evaluation: description of the system, identification of data and data flows
A4 Identification of actors involved/ persons concerned
A5 Identification of relevant legal requirements
Documentation of tasks and issues
B. Evaluation stage
B1 Identification of protection goals
B2 Identification of potential attackers, motives and objectives
B3 Identification of evaluation criteria and benchmarks
B4 Evaluation of the risk
Catalogue of typical objectives, attackers and consequences
C. Report and safeguards stage
C1 Identification of appropriate safeguards
C2 Documentation of evaluation results in standardized form
DPIA Report
C3 Publication of DPIA Report
C5 Auditing of Evaluation Results
C4 Implementation of safeguards
Catalogue of typical safeguards
End of a DPIA cycle
Supervision and continuation

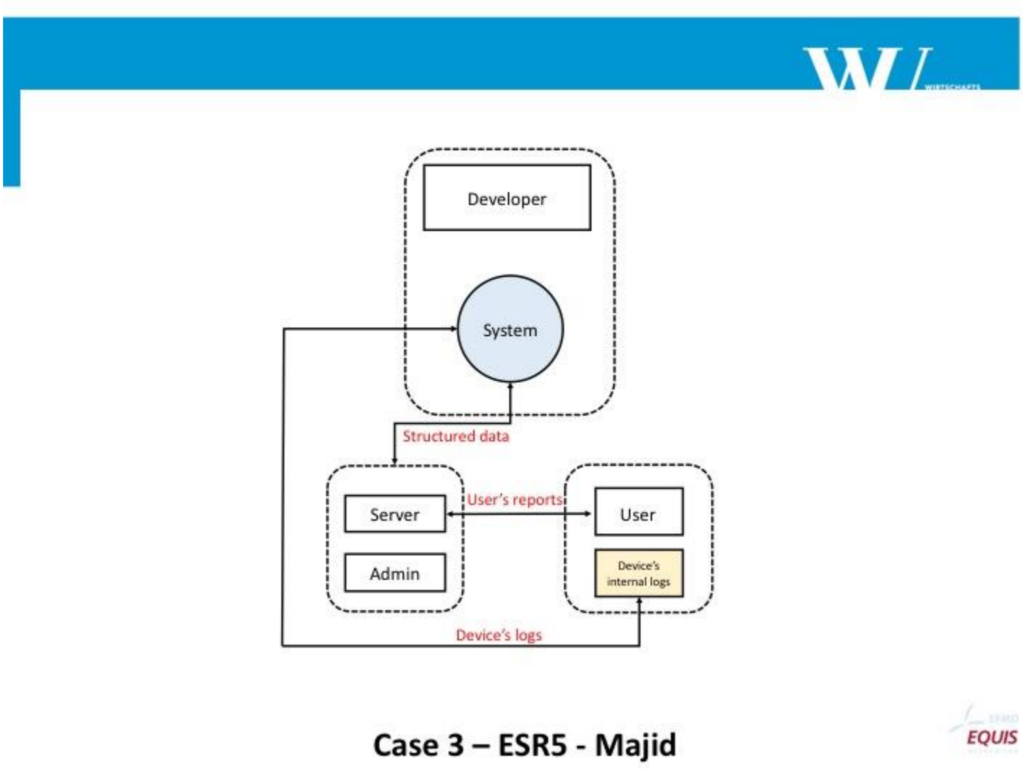
Evaluation Phase – This afternoon



Case 1 – ESR12



Case 2 – ESR7 & ESR10



Developer

System

Structured data

Server

Admin

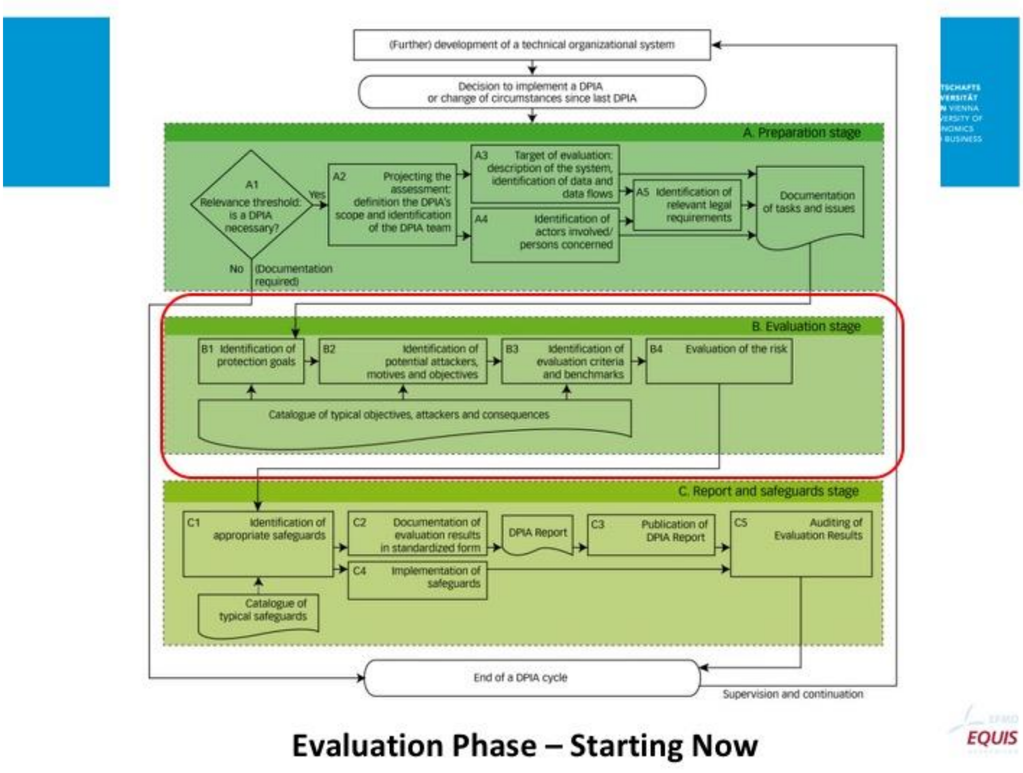
User's reports

User

Device's internal logs

Device's logs

Case 3 – ESR5 - Majid



(Further) development of a technical organizational system

Decision to implement a DPIA
or change of circumstances since last DPIA

A. Preparation stage

A1 Relevance threshold: is a DPIA necessary?

Yes

No (Documentation required)

A2 Projecting the assessment: definition the DPIA's scope and identification of the DPIA team

A3 Target of evaluation: description of the system, identification of data and data flows

A4 Identification of actors involved/ persons concerned

A5 Identification of relevant legal requirements

Documentation of tasks and issues

B. Evaluation stage

B1 Identification of protection goals

B2 Identification of potential attackers, motives and objectives

B3 Identification of evaluation criteria and benchmarks

B4 Evaluation of the risk

Catalogue of typical objectives, attackers and consequences

C. Report and safeguards stage

C1 Identification of appropriate safeguards

Catalogue of typical safeguards

C2 Documentation of evaluation results in standardized form

DPIA Report

C3 Publication of DPIA Report

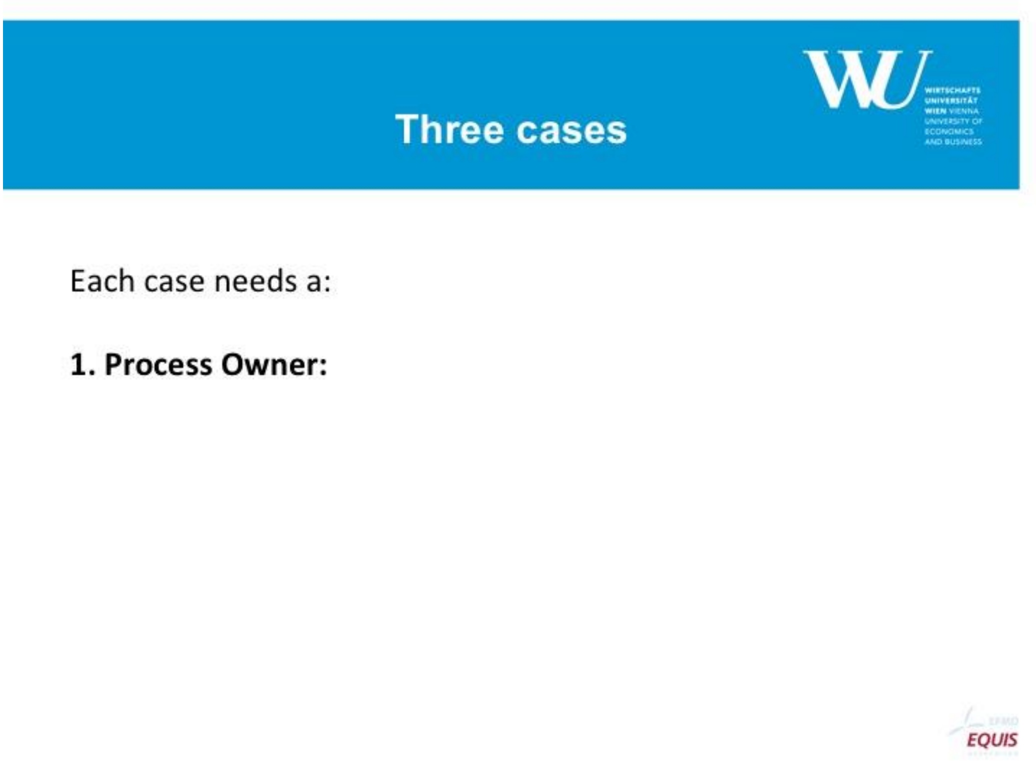
C4 Implementation of safeguards

C5 Auditing of Evaluation Results

End of a DPIA cycle

Supervision and continuation

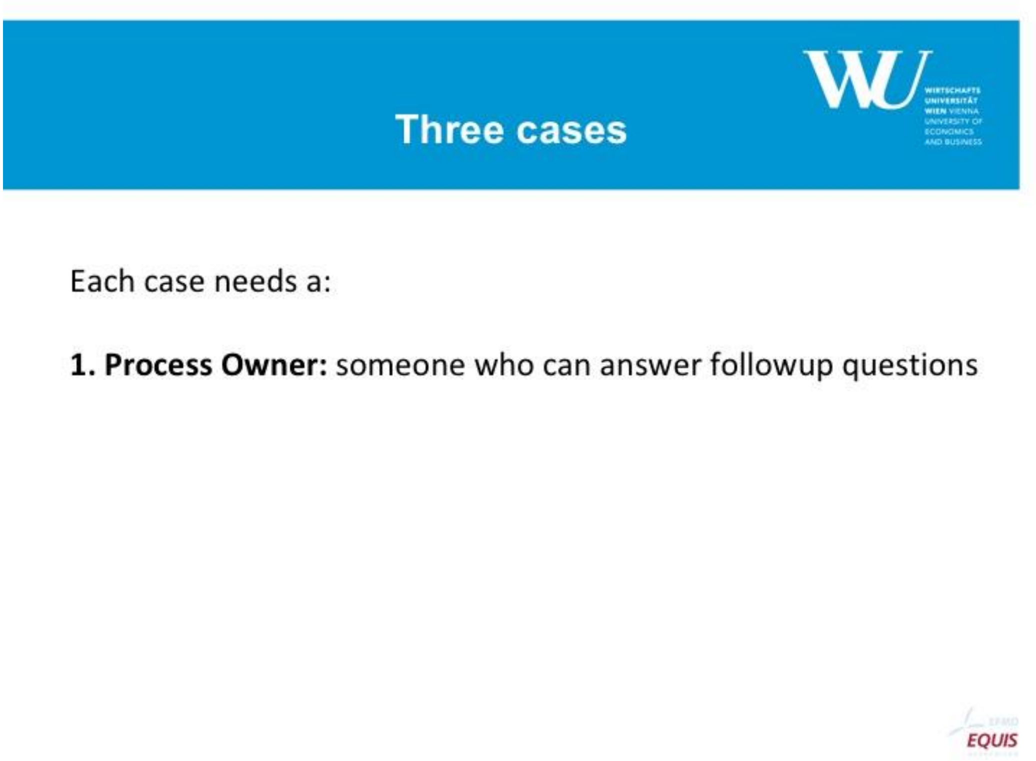
Evaluation Phase – Starting Now



Three cases

Each case needs a:

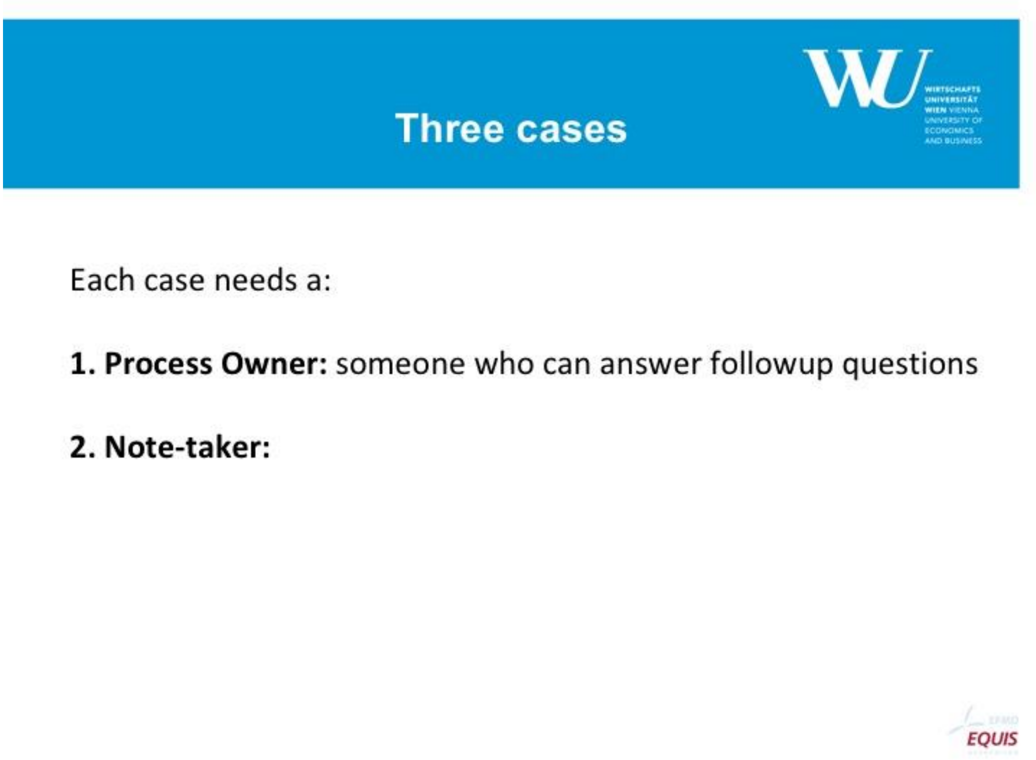
1. Process Owner:



Three cases

Each case needs a:

1. Process Owner: someone who can answer followup questions

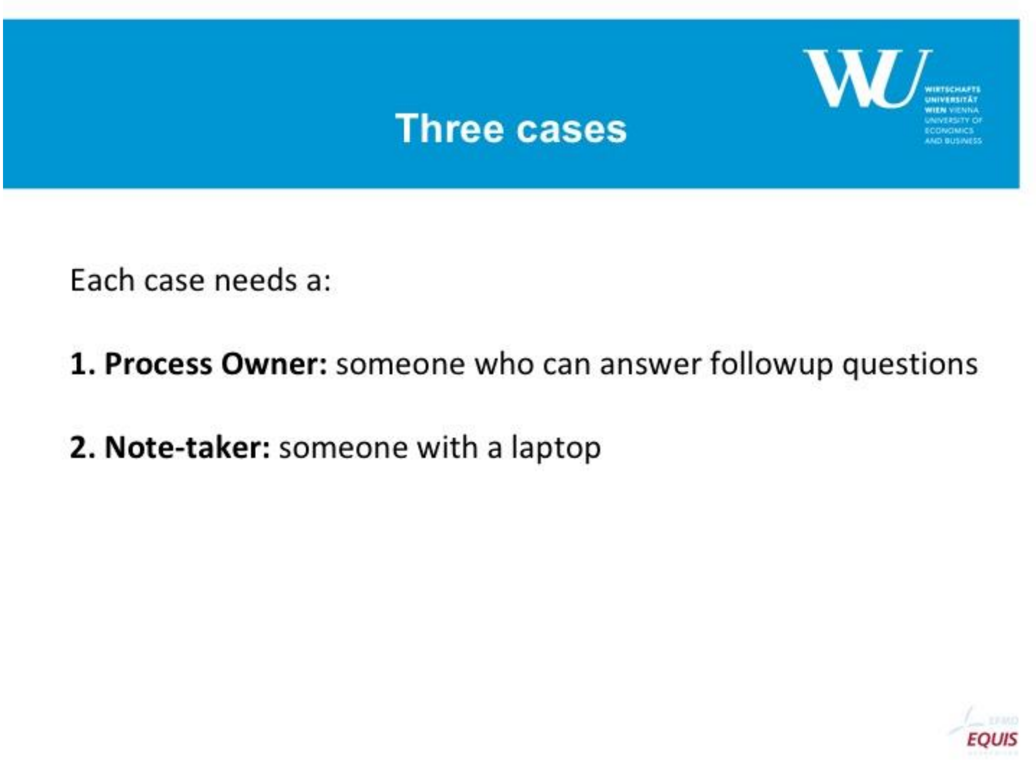


Three cases

Each case needs a:

1. **Process Owner:** someone who can answer followup questions

2. **Note-taker:**

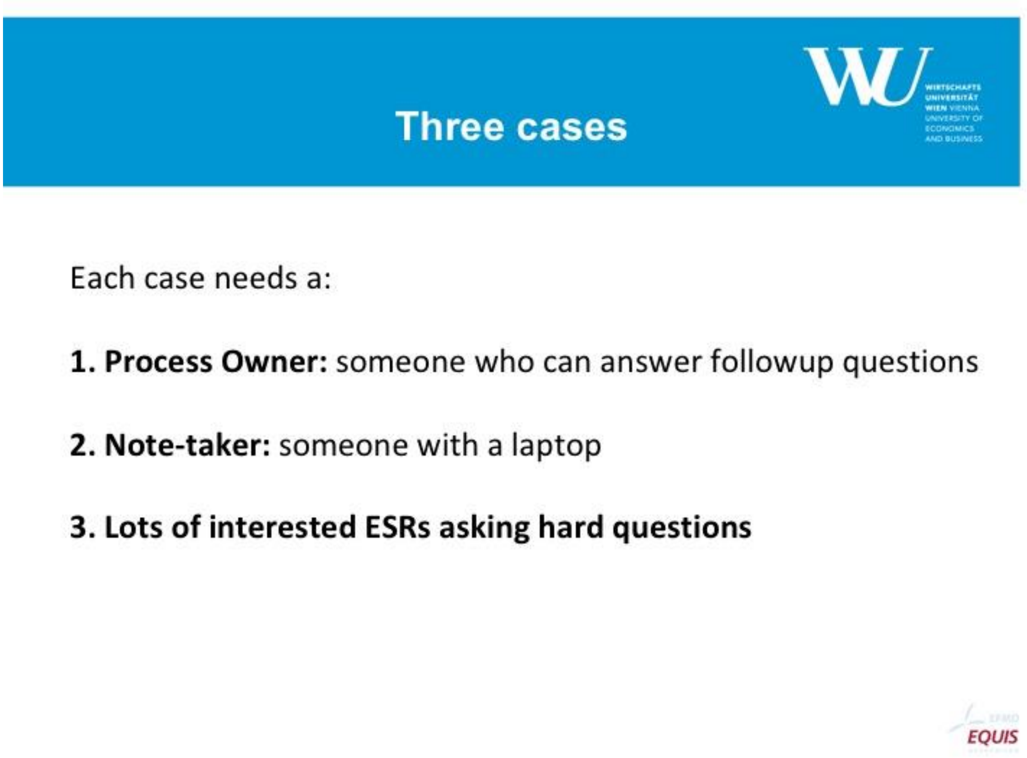


Three cases

Each case needs a:

1. **Process Owner:** someone who can answer followup questions

2. **Note-taker:** someone with a laptop



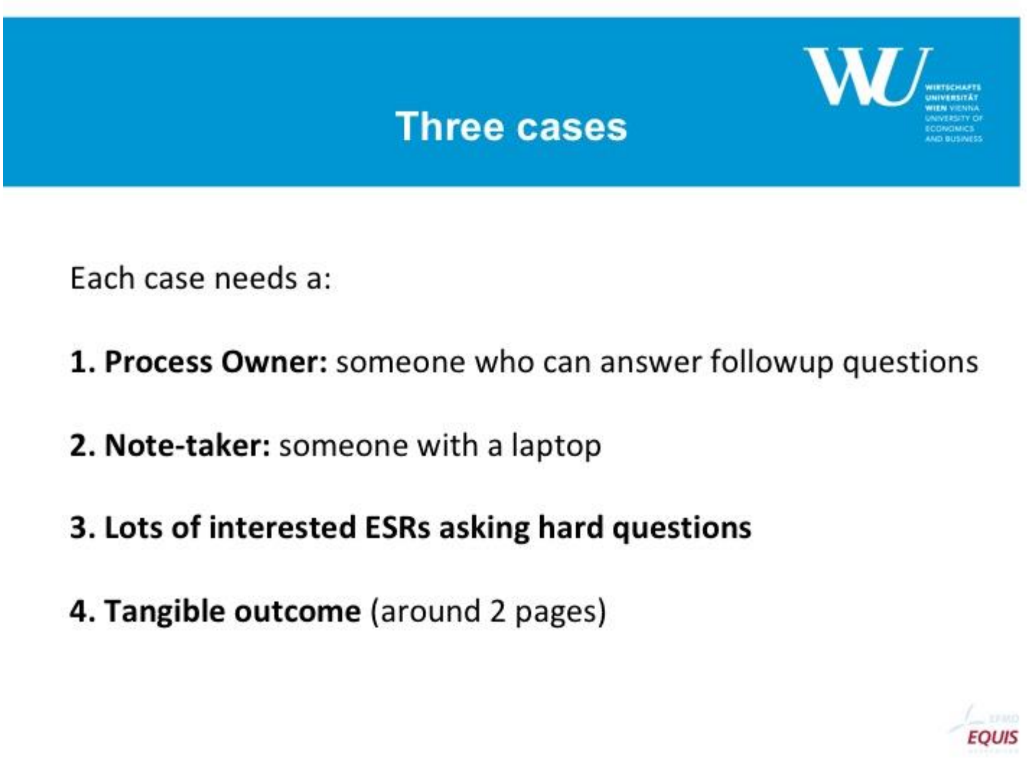
Three cases

Each case needs a:

1. **Process Owner:** someone who can answer followup questions

2. **Note-taker:** someone with a laptop

3. **Lots of interested ESRs asking hard questions**



Three cases

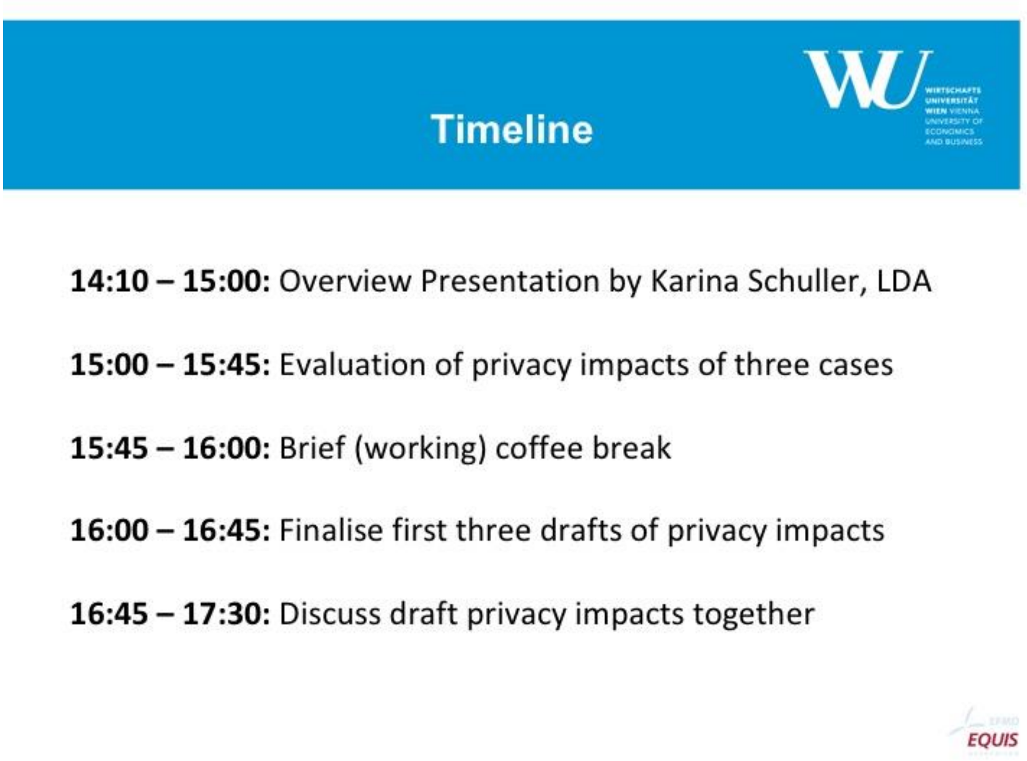
Each case needs a:

1. **Process Owner:** someone who can answer followup questions

2. **Note-taker:** someone with a laptop

3. **Lots of interested ESRs asking hard questions**

4. **Tangible outcome** (around 2 pages)



Timeline

14:10 – 15:00: Overview Presentation by Karina Schuller, LDA

15:00 – 15:45: Evaluation of privacy impacts of three cases

15:45 – 16:00: Brief (working) coffee break

16:00 – 16:45: Finalise first three drafts of privacy impacts

16:45 – 17:30: Discuss draft privacy impacts together

Thank you for listening

If you have any questions or
comments, just ask!

@benwagne_r

ben.wagner@wu.ac.at