IN5540 – Privacy by Design

Quiz questions

Tanusan Rajmohan - tanusanr@ifi.uio.no

University of Oslo

Spring 2019

Chapter 1 – Privacy-Philosophy and legislation, GDPR

Concept of Privacy

1. Privacy is a human right?
   a. **True** (See Art.8 European Convention of Human Rights)
   b. False
2. Privacy is the same as Data Protection?
   a. True
   b. **False** (No, because privacy has also the dimensions of bodily privacy, territorial and spatial privacy that do not fall under data protection)
3. Privacy is a concept that became only relevant with the upcoming of information technology in the 20th century?
   a. True
   b. **False** (Privacy as a concept is already known since ancient times)
4. The first definition of privacy by lawyers was influenced by technical developments?
   a. **True** (yes, by photography)
   b. False
5. Privacy is a fundamental and human right, but not essential for a modern democratic society?
   a. True
   b. **False** (No, as the German Constitutional court discussed in its census decision, it is a pre-requisite for a democratic society, which depends on the participation in political debates by individuals.)

Basic Privacy Principles

1. Purpose binding means that data may be used for one purpose only?
   a. True
   b. **False** (no, it may be used for several purposes, if they were specified in advanced and are needed for the fulfillment of the task.)
2. There are no non-sensitive data?
   a. **True** (yes, as the sensitivity of data depends on the purpose and context of use.)
   b. False
3. Consent is always needed as a lawful basis?
   a. True
   b. **False** (no, there are also other possible lawful bases for legitimizing data processing.)
4. Measures providing appropriate security, and not necessarily the maximum security that is possible, have to be taken to protect the confidentiality and integrity of personal data?
   a. **True** (yes, measures have to be appropriate to the risk.)
   b. False
5. You want to conduct a survey and state that the purpose of your survey is the analysis of customer preferences for different age groups. In the survey, you ask for the participants' birth date. You think that you comply with basic privacy principles of the OECD. Is that true?
   a. True
   b. **False** (No, as you do not comply with the data minimization principle. For conducting the survey, it would be sufficient to only ask for the age or age group, but the exact

age is more detailed information than needed. Hence, the principle of data minimization of data collection is breached.)

Privacy Laws

1. The OECD Guidelines are legally binding for its member states?
    a. True
    b. **False** (No, it is only a recommendation.)
2. The Privacy Shield Agreement is relevant for the processing of personal data of Swedish users by Facebook?
    a. **True** (yes, as usually these data will be transferred from Sweden to the USA.)
    b. False
3. The processing of location data will in future be regulated by the ePrivacy Regulation, which has precedence in relation to the GDPR?
    a. **True** (yes, the ePrivacy regulation regulates the electronic communication section and is lex specialis.)
    b. False
4. Video surveillance will in future only be regulated by the GDPR in Sweden?
    a. True
    b. **False** (No, Camera Surveillance Act also applies - even though camera surveillance will in many ways be considered as any other handling of personal data, i.e. rules of the GDPR needs to be met.)
5. The GDPR replaces the Swedish Freedom of the Press Act?
    a. True
    b. **False** (No, personal data in official documents may be disclosed (art 86 GDPR). But: The Public Access to Information and Secrecy Act states that secrecy shall apply to personal data, if it can be assumed that disclosure would cause the data to be processed in violation of GDPR.)

Mobile Computing & Smart Metering

1. Location data can reveal health information?
    a. **True** (Yes, if for instance someone is regularly visiting a cancer treatment center, the location data of this person can reveal that this person is likely getting a cancer treatment.)
    b. False
2. The Electronic Product Codes on RFID tags attached to items that can be purchased are not and cannot become personal data?
    a. True
    b. **False** (In contrast to a bar code that is only unique for a product group, the Electronic Product Code is unique for each product item and can become a unique identifier for a person carrying that item around.)
3. Smart Metering introduces privacy issues that can only be handled sufficiently well by privacy and data protection laws - no adequate privacy enhancing technologies have been developed yet?
    a. True
    b. **False** (In addition to laws, also efficient privacy-enhancing technologies exist for anonymizing smart metering readings from individual households.)

Social Networks, Big Data & Cloud Computing

1. Information about my personality and intelligence can be derived from what I am publishing on social networks by social network analysis?
    a. **True** (see course literature.)
    b. False
2. Discrimination by algorithms can be prevented if they are carefully designed and made transparent?
    a. True
    b. **False** (No, also the quality of the input data training the algorithms may contribute to discrimination.)
3. For a Cloud service that is offered in Sweden, different service sub providers in different jurisdictions can be involved?
    a. **True** (Yes, the cloud chain may involve different sub-providers in different countries along a cloud chain. Those countries may have different data protection laws/rules or even no data protection legislation at all.)
    b. False

Introduction to the GDPR

1. If I order items from a webshop in Brazil, the shop will have to follow the GDPR when processing my personal data?
    a. **True** (Yes, the GDPR also applies outside Europe for service providers that offer services to European citizens.)
    b. False
2. If I store contact details of my friends on my mobile phone, I have to follow the rules of the GDPR?
    a. True
    b. **False** (No, as the household exemption applies, i.e. this data processing is out of scope of the GDPR.)
3. If you publish photos on Flickr about your friends to an unrestricted audience, is Flickr the only data controller responsible for the data processing?
    a. True
    b. **False** (No, you would also be the data controller, as the household exemption will not apply (cf. Bodil Lindqvist case).)
4. An IP address classifies as personal data?
    a. **True** (Yes, an IP address can often directly identify a person or provide information that make the person at least more likely to be identifiable.)
    b. False
5. Technical security is outside the scope of the GDPR?
    a. True
    b. **False** (No, according to Art. 5 (I) f., appropriate security measures need to be guaranteed for personal data that are processed.)

Lawfulness & Consent

1. Personal data may only be processed with the consent of the data subject?
    a. True

    b. **False** (No, there are 5 other legal bases defined in for making data processing legitimate.)

2. During my lectures, I am allowed to ask my students to participate in a survey which also involves disclosing some demographic data, if the students provide their consent?
    a. True
    b. **False** (No, as there is an imbalance of power between the students and me as teacher of the course, the consent would not be considered as freely given if it is part of a course that my students have to take.)
3. Is the following statement valid for a consent? [] I agree that my address may be used for the purposes of shipping the purchased items and for sending me information about special offers.
    a. True
    b. **False** (No, "bundling" of purposes is not allowed for freely given purposes.)
4. If the conference department at Karlstad University collects data about dietary requirements of conference participants, the data may only be collected with a legal basis pursuant to Art. 6 GDPR?
    a. True
    b. **False** (No, data about dietary requirements are "special categories" of data, as they may reveal information about the health or religion of the conference participants. Hence, Art. 9 GDPR applies.)
5. As a data subject, I will be responsible to prove that I have not given my consent to a service provider in case of a dispute?
    a. True
    b. **False** (No, the data controller has the burden of proof that he obtained a valid consent.)

Data Subject Rights

1. The right to be forgotten applies only after the data are at least 20 years old?
    a. True
    b. **False** (No, the GDPR gives no fixed time period - the question whether data are outdated and no longer needed can therefore be answered differently from case to case.)
2. I have only the right to object to automatic decision making if the decisions are made without any human interactions?
    a. **True** (Yes, the decision making must be based solely on automatic processing)
    b. False
3. The right to data portability also applies for data, such as reputation scores, that a service provider received about me from third parties (e.g., my reputation as a seller in eBay)?
    a. True
    b. **False** (No, the right to data portability only applies for data disclosed by the data subject.)
4. The right of access by the data subject includes the right to get an electronic copy of his/her personal data, including personal data that were provided by third parties (such as reputation scores)?

    a. **True** (Yes, the right of access applies to disclosed data, derived data and also to data that the service provider received about the data subject from third parties.)
    b. False
5. Standardized policy icons can replace the written policy information in privacy policy notices?
    a. True
    b. **False** (No, the GDPR only says in Art. 12 (7) that the information to be provided to data subjects may be combined with standardized icons (which means that it should not replace it).)

Responsibilities & Rules

1. The obligation to assign a DPO applies to both data controllers and data processors?
    a. **True** (Yes, see art. 38 GDPR.)
    b. False
2. In case of disputes, a multinational company will only have to deal with the lead supervisory authority in the country, where the company has its main or single establishment?
    a. **True** (Yes, according to the so-called "one-stop-shop" principle.)
    b. False
3. According to Art. 25 GDPR, the Data Protection by Design and Default principle is a legal obligation for the producer of IT systems?
    a. True
    b. **False** (No, Art. 25 only applies to data controllers, who are responsible for achieving Data Protection by Design and Default.)
4. For all projects that involve the processing of personal data, the data controller has to first conduct a Data Protection Impact Assessment (DPIA)?
    a. True
    b. **False** (No, a DPIA only needs to be conducted for high-risk data.)
5. Pseudonymized data are personal data?
    a. **True** (Yes, they still classify as personal data, as the identity of the data subjects could usually still be determined. Only anonymized data do not classify as personal data.)
    b. False

ePrivacy Regulation

1. The ePrivacy Regulation will have priority over the GDPR?
    a. **True** (The ePrivacy Regulation will be lex specialis to the GDPR and thus overrides the GDPR.)
    b. False
2. According to the proposed ePrivacy Regulation, consent is in general required for Cookies?
    a. True
    b. **False** (Certain types of cookies that are regarded as non-privacy sensitive are exempted.)
3. "Take it or leave it" type of services will be prohibited?
    a. True

   b. **False** (No, as criticized by the GDPR, so-called tracking walls—that is, denial of access to a website or service unless the user consents to tracking on other websites or services—is not prohibited by the proposed regulation.)

4. The proposed ePrivacy regulation forbids WiFi tracking?
   a. True
   b. **False** (No, as the Art. 29 WP criticized, the proposed ePrivacy regulation allows the collection of data emitted by users' devices, such as MAC addresses, without the user's prior opt-in consent, if the user received a clear and prominent notice that explains how individuals can minimize or stop this data collection.)
5. Marketing callers will need to display their phone number or use a special pre-fix that indicates a marketing call?
   a. **True** (Yes, this is part of the rules to protect individuals against SPAM.)
   b. False

Chapter 2 – Privacy Enhancing Technology (PET)

PETs

1. Of the following list, which ones are objectives of PETs?
   a. control over personal data
   b. data minimization / avoidance
   c. lawful processing of data
   d. data security and integrity
   e. all of the above alternatives
2. Why are PETs relevant in the context of the GDPR?
   a. The GDPR has a paragraph listing the relevant PETs
   b. The GDPR is a collection of PETs
   c. PETs are countermeasures to be included in the DPIA
   d. PETs and GDPR are basically the same thing
   e. PETs are not relevant to the GDPR
3. PETs are technical means for protecting personal data based on standards, protocols, tools and mechanisms.
   a. True b. False
4. Which of the below are arguably NOT a PET?
   a. **RFC 793 (Transmission Control Protocol, TCP)**
   b. RFC 5246 (Transport Layer Security, TLS)
   c. NoScript (a browser extension for controlling scripts)
   d. Tor (an anonymous communication system)
   e. All of the above are PETs

Terminology

1. An anonymity set is:
   a. the set of all possible subjects (or "suspects")
   b. a set in which all elements cannot be identified
   c. a set of subjects with the same identification tag
   d. the set of pseudonyms of a given subject
   e. the set of anonymous credentials of a given subject

2. Pseudonyms are:
    a. distinct nicknames for each communication partner
    b. a substitute for the holder's name which is regarded as representation for the holder's civil identity
    c. set to specific roles, e.g., a customer pseudonym or an Internet account used for many instantiations of the same role "Internet user"
    d. **all the above are correct**
    e. none of the above is correct
3. Which of the following options best describe a transaction pseudonym?
    a. a social security number
    b. distinct nicknames for each communication partner
    c. a one-time-use pseudonym
    d. randomly generated transaction numbers for online banking
    e. the first and the fourth alternatives are correct
    f. the third and the fourth alternatives are correct
4. Undetectability of an item of interest from an attacker's perspective means that the attacker cannot sufficiently distinguish whether it exists or not.
    a. True
    b. False
5. Undetectability implies unobservability.
    a. True
    b. **False** (Unobservability implies undetectability)

PGP

1. What does PGP offer in terms of security:
    a. confidentiality
    b. integrity
    c. availability
    d. authentication
    e. the first, second and third alternatives are correct
    f. the first, second and fourth alternatives are correct
2. PGP was designed for encrypting, decrypting and signing
    a. text
    b. email
    c. files
    d. all of the above
    e. none of the above
3. Concerning the public and private key-pair:
    a. Bob (and everyone else) knows Alice's public key
    b. only Bob knows Alice's public key
    c. only Bob knows Alice's private key
    d. only Alice knows Alice's private key
    e. the first and third alternatives are correct
    f. the first and fourth alternatives are correct
4. What is the Web of Trust?
    a. a network of secure Internet relays
    b. a set of routers that communicate using PGP
    c. **a decentralized trust model**
    d. an IETF RFC
    e. a public key infrastructure based on certificate authorities

TLS and Certificate Authorities

1. TLS provides a secure channel over an untrusted network.
    a. **True** (Yes, and the channel provides confidentiality, integrity, server authentication (normally), and optional client authentication.)
    b. False
2. TLS is the same as SSL.
    a. True
    b. **False** (SSL is the 20+ years predecessor of TLS.)
3. Considering the performance overhead of TLS is important.
    a. True
    b. **False** (No, performance is not an important consideration anymore when it comes to TLS:
       - https://istlsfastyet.com/
       - https://blog.cloudflare.com/how-expensive-is-crypto-anyway/).
4. TLS is used in HTTPS to transport HTTP over TLS.
    a. **True**
    b. False
5. Getting a valid certificate costs money.
    a. True
    b. **False** (Nope, not a DV certificate, due to Let's Encrypt.)
6. Certificate Transparency prevents man-in-the-middle attacks.
    a. True
    b. **False** (Not directly: CT is a detective measure, not a preventive one, enabling us to find out about misused certificates after the fact. (Of course, this may indirectly prevent attacks that otherwise would have occurred.))

Secure Messaging

1. A messaging app that encrypt messages between user-and-server using TLS is a secure messaging app.
    a. True
    b. **False** (No, one characteristic of secure messaging apps is that they're end-to-end secure, that is, from user-to-user.)
2. Which of the following secure messaging apps are end-to-end secure by default for one-to-one communication?
    a. Facebook Messenger
    b. **WhatsApp**
    c. Google Allo
    d. Signal
3. Secure messaging apps are about as usable as PGP.
    a. True
    b. **False** (They're significantly more usable.)
4. Which technology is most widely deployed and used today?
    a. PGP
    b. WhatsApp
5. Secure messaging apps will hide who is communicating with whom.
    a. True
    b. **False** (Not in general. Some might, but it's not the default for any of the widely used secure messaging apps. The community is working on usable alternatives.)

Mixnets

1. Mixnets can protect against a global passive adversary that sees all network traffic.
    a. **True** (Yes, in general, if properly designed and implemented. (The protection is not perfect though, see, e.g., Statistical Disclosure Attacks: Traffic Confirmation in Open Environments).)
    b. False
2. Messages are not encrypted when sent through mixes.
    a. True
    b. **False** (They are encrypted, and the encryption (or mix) format is surprisingly advanced in modern designs.)
3. It's possible to provide strong anonymity against a powerful adversary and have both low latency and bandwidth overhead.
    a. True
    b. **False** (No, the current view in the research community is that this is not possible.)
4. There are many mature mixnets that are deployed and used by many today.
    a. True
    b. **False** (Nope, unfortunately mixnets have not received nearly the same attention in terms of deployment as Tor. Maybe this is changing though.)
5. Mixnets are low latency.
    a. True
    b. **False** (In general, no, latency is used to gain strong anonymity together with bandwidth.)

Tor

1. Tor is designed to protect against a global passive adversary that can see all network traffic.
    a. True
    b. **False** (No, Tor can only protect against limited compromise of its network.)
2. Onion services are only useful for hiding the location and identity of the service.
    a. True
    b. **False** (No, they're also self-authenticated, end-to-end encrypted, NAT punching, and expose a limited attack surface of the service.)
3. Which of the below are use-cases of Tor?
    a. Encryption
    b. **Anonymous browsing**
    c. Censoring Internet access
    d. **Censorship circumvention**
    e. **Onion services**
    f. Unobservable service hosting
    g. Single onion services
4. The .onion addresses used to access onion services rely on the certificate authority ecosystem.
    a. True
    b. **False** (No, but .onion is a special-use domain nameLinks to an external site. that you can get an extended validation certificate for, like Facebook has, for facebookcorewwwi.onion.)
5. Anyone can run a Tor relay or bridge.
    a. **True** (Yes, The Tor Project has more information on how.)
    b. False

k-anonymity

1. What of the following alternatives better describes the goal of k-anonymity?
    a. **to prevent the re-identification of individuals when releasing a data set by checking if an individual is indistinguishable from at least k-1 other individuals.**
    b. to construct data sets that with mathematically defined k-filters that can enforce a data protection framework, including the GDPR.
    c. to formally define the concept of anonymity using first-order logic and set theory.
    d. to define a scale of anonymity that extends and supersedes the Pfitzmann-Hansen terminology with the definition of k-scales and quasi-identifiers.
    e. to theoretically define the concepts of quasi-identifiers using Ricoeur's theory of the distinction of the self.
2. k-anonymity differentiate between explicit and quasi-identifiers. Of the following, which alternative contains only quasi-identifiers?
    a. nationality, profession, IP address
    b. gender, address, social security number
    c. phone number, ethnicity, nationality
    d. **profession, gender, spoken languages**
    e. full name, address, phone number
3. In k-anonymity, what is the minimum allowed k for preventing the re-identification of individuals when publishing a data set?
    a. 0
    b. 4
    c. 3
    d. 1
    e. 2
4. k-anonymity removes explicit identifier attributes, such as names, from the data set. It also uses two methods to deal with quasi-identifiers. They are:
    a. deletion and compartmentalization
    b. minimization and compliance
    c. confusion and sifting
    d. oppression and garbling
    e. suppression and generalization
5. What alternative better describe l-diversity:
    a. it addresses attribute disclosure attacks on t-closeness.
    b. it is the first instantiation of k-anonymity.
    c. it is a privacy metric that is unrelated to k-anonymity.
    d. **it addresses the homogeneity and background knowledge attacks over k-anonymity. Its own limitations are addressed by t-closeness.**
    e. it addresses part of the t-closeness limitations. The metric it uses is the attacker's information gain.

Differential privacy

1. Differential privacy looks into data releases from:
    a. hierarchical databases
    b. operational databases
    c. relational databases
    d. distributed databases
    e. statistical databases

2. Differential privacy:

   a. **quantifies the difference what might be learned about any individual from a database with or without said individual.**
   b. extends k-anonymity, l-diversity and t-closeness.
   c. is a construct for quantifying the socio-economic value of personal information stored in a statistical database.
   d. quantifies the contents of a database using a complex mathematical definition for measuring the privacy value of quasi-identifiers.
   e. quantifies the level data protection of individuals in a database by comparing it with other individuals in the same database.

3. The privacy budget:
   a. is voted every February. It may result in a government shutdown.
   b. is the statistical upper bound privacy cost allowed for a query.
   c. **defines the maximum privacy release allowable for all queries.**
   d. defines a monetary function for the cost of queries to a database.
   e. defines the information difference between two data releases.
4. Concerning differential privacy, which of the following is correct:
   a. differential privacy provides a rigorous framework with a set of theoretical bounds for releasing data.
   b. the privacy budget defines how much noise is to be added.
   c. how to add noise depends on the type of data and mechanism design.
   d. the Laplace mechanism is used for numerical data.
   e. all alternatives are correct.
5. Concerning differential privacy and data utility, which of the following is NOT correct:
   a. all alternatives are incorrect.
   b. the epsilon of two data releases, one with Alice and the other without Alice, is equal to Alice's contribution to the dataset. It means that Alice data is exposed.
   c. **a tiny privacy budget would result in no data utility.**
   d. the epsilon of two data releases, one with Alice and the other without Alice, is zero. It means that Alice data utility is also zero.
   e. a tiny privacy budget has no effect on the data utility.

Blockchains

1. Blockchains are designed for trusted writers to agree on the state of the data structure that changes over time.
   a. True
   b. **False** (No, blockchains are made for mutually untrusted writers. If writers trust each other (or have to), then a blockchain is not needed.)
2. We have efficient algorithms for establishing consensus in permissionless blockchains.
   a. True
   b. **False** (No, the energy consumption of PoW algorithms are a significant sustainability concern.)
3. Data stored in a blockchain must be public.
   a. True
   b. **False** (No, there are private permissioned blockchains, and further, some blockchains encrypt the data.)

4. Blockchains are a mature technology that are easy to use in practice.
   a. True
   b. **False** (Far from it.)
5. The bitcoin white paper, despite the pedigree of many of its ideas, was more novel than most academic research.
   a. True
   b. False

Anonymous credentials

1. What does X.509 public key certificates and anonymous credentials have in common?
   a. **they are used to authenticate users.**
   b. they establish secure communication channels.
   c. they are based on blind signatures.
   d. they are patented by IBM.
   e. they are included in the design of Tor.
2. Anonymous credentials are used:
   a. to establish secure HTTPS connections.
   b. by Tor relays to anonymize data.
   c. **to verify an identity without revealing it.**
   d. by anonymous access control mechanisms.
   e. to authorize bitcoin transactions.
3. Anonymous credentials can be constructed to offer:
   a. selective attribute disclosure.
   b. authentication
   c. unlinkability between multiple uses
   d. unforgeability
   e. all alternatives are correct
4. Idemix basic cryptographic building block is:
   a. blind signatures.
   b. **zero knowledge proofs.**
   c. Pedersen commitments.
   d. oblivious transfers.
   e. the Caesar cipher.

TETs

1. Transparency is a basic legal data protection principle?
   a. **True** (Yes, see for instance Art. 5 I (a) GDPR.)
   b. False
2. Transparency can also endanger the rights of others?
   a. **True** (Yes, it can for instance endanger or restrict business secrets or privacy rights of others.)
   b. False
3. TETs can be divided into ex ante TETs, ex post TETs and intervenability tools?
   a. True
   b. **False** (No - transparency is usually a prerequisite for intervenability and some ex post TETs (such as the Data Track) also provide intervenability functions. However, there can also be intervenability tools that go beyond transparency and offer data subjects to exercise their intervenability rights to delete, correct data or to revoke consent.)
4. Lightbeam is a trusted third-party TET?

   a. True
   b. **False** (No, lightbeam is a Firefox add-on and runs the user side.)

5. The Data Track is a user side TET that allows to visualize data exports?
   a. **True** (Yes, the stand-alone version of the Data Track can visualize data exports that users may obtain by exercising the right of data portability.)
   b. False

Chapter 3 – Designing for Privacy / Data Protection impact assessment

The GDPR

1. The GDPR is a new directive.
   a. True
   b. **False** (No, it's a regulation. The Data Protection Directive is from 1995.)
2. One of the goals of the GDPR is to harmonize the data protection legislation across Europe.
   a. **True** b. False
3. Law enforcement activities are covered by the GDPR.
   a. True
   b. **False** (No, see Directive (EU) 2016/680.)
4. Data processors processes data on behalf of data controllers.
   a. **True** b. False
5. Data processing of personal data of European data subjects must meet the requirements of the GDPR.
   a. **True** (Yes, as long as they want access to the European market.)
   b. False
6. The definition of personal data in the GDPR is narrow and limited, only covering specific types of data about persons.
   a. True
   b. **False** (No, the definition is very broad.)

Privacy and Data Protection

1. Data protection is a human right.
   a. True **b. False**
2. Privacy is explicitly a human right in the Universal Declaration of Human Rights.
   a. **True** b. False
3. Privacy is implicitly a human right in the European Convention on Human Rights.
   a. **True** b. False
4. Data protection is a human right in the European Convention on Human Rights.
   a. True **b. False**
5. Data protection is a fundamental right in the European Charter of Fundamental Rights.
   a. **True** b. False
6. Privacy is implicitly a fundamental right in the European Charter of Fundamental Rights.
   a. **True** b. False
7. Privacy is explicitly a fundamental right in the European Charter of Fundamental Rights.
   a. True **b. False**

Seven Principles

1. On the left are seven bad principles stating roughly the inverse of the seven principles of Privacy by Design. Match each bad principle to its original corresponding principle.
    a. We'll cross that bridge when we get to it – **Proactive not Reactive**
    b. Click here to opt-in for privacy – **Privacy as the Default**
    c. We'll add privacy later as an add-on – **Privacy Embedded into Design**
    d. Privacy vs. security – **Full Functionally**
    e. HTTPS ought to be enough for anyone – **End-to-End Security**
    f. Security through obscurity – **Visibility and Transparency**
    g. Organization-centric – **Respect for User Privacy**

Privacy Paradigms

1. Match the privacy paradigm with the description that best fits.
    a. Once disclosed all is lost – **Privacy as confidentiality**
    b. Data protection – **Privacy as control**
    c. Negotiable boundaries – **Privacy as practice**
2. Match the privacy paradigm with the description that best fits when it comes to dealing with social networks (based on an example made by Seda Gürses in https://www.youtube.com/watch?v=y7fGVSO2lEg)
    a. "Before uploading a picture, I encrypt it so that only my intended friends can see it." – **Privacy as confidentiality**
    b. "When posting a picture, I use the settings provided by the provider to ensure my parents can't see it." – **Privacy as control**
    c. "I always remove friends tagged automatically in photos before posting, it would be rude not to." – **Privacy as practice**
3. Match the privacy paradigm with the description that best fits.
    a. The purpose of processing is really important - **Privacy as control**
    b. Without open source and verifiable builds software cannot be really trusted - **Privacy as confidentiality**
    c. Privacy nudges in the right context gives people better control - **Privacy as practice**

Technology in Hostile States

1. Tor is a good example of the privacy-as-control paradigm.
    a. True **b. False**
2. Laws can be relied upon to protect users.
    a. True **b. False**
3. Policy commentary, for example around encryption and the "need for backdoors", should be prepared in advance.
    a. True b. False
4. Keep as much user data as possible.
    a. True **b. False**
5. Give nobody control over data: data wants to be free!
    a. True **b. False**
6. Require users to reveal their real-world identities to prevent abuse.
    a. True **b. False**
7. Encrypt data only in transit, not at rest.
    a. True **b. False**

8. Focus on building a single system that's trustworthy and strongly protected, then bootstrap the rest from there.
    a. True
    b. False
9. Open source and user freedoms are at odds.
    a. True
    b. False
10. Keep systems and designs a secret to make them harder to attack.
    a. True
    b. False

Common Mistakes

1. Mistake 1 is storage as default. Which of the following is a primary reason behind the mistake?
    a. **"You never know when you're going to need it. So better keep it." (**Together with the low cost of storage, these are the main reasons behind storage of the default.)
    b. The need for swapping out RAM to disk.
    c. Misconfiguration.
    d. The prevalence of logfiles.
2. Linking data together by identifiers across tables, databases, and systems is a common occurrence that is, in general, good for privacy.
    a. True
    b. **False** (Massive linkable data is a nightmare from a privacy perspective. As soon as one piece of data is linked to an individual, then all data by definition is linked.)
3. Why could relying on social login services like Facebook be a problem for account management in a service?
    a. Social networks can be hard to use.
    b. **Many social networks enforce real-name policies, preventing users from being pseudonymous.**
    c. Social login implies that the social login provider can profile users.
4. Function creep, in the sense of processing data beyond the original purpose or context, is allowed in the GDPR.
    a. True
    b. **False** (purpose binding is a core concept in data protection that is often problematic for technologies to deal.)
5. Information provided to users (data subjects) are often fuzzy and/or incomplete. Which of the following is not a relevant example of this mistake?
    a. A data controller not sharing the identities of data processors.
    b. A privacy policy not provided in plain language.
    c. A generic description of a purpose.
    d. Lack of TLS by default.
6. The location where data processing takes place is less important today thanks to cloud computing.
    a. True
    b. **False** (Location of data processing is an important legal consideration.)

7. Considering the full lifecycle of data, an organization, or a system itself is important. Which of the following is a likely reason behind neglecting lifecycle assessment?
    a. No demand for long-term thinking.
    b. **A focus on quick and dirty functionality.**
    c. Team maturity.
    d. Developer education.
8. When assumptions made during the design of a system are later violated, for example due to new functionality being implemented, privacy may be negatively impacted.
    a. **True** (This is especially true for stronger privacy goals, such as anonymity or unlinkability.)
    b. False
9. Systems are commonly designed with data subject intervenability in mind.
    a. True
    b. **False** (Hopefully the GDPR will lead to this being true.)
10. When personal data is processed on the basis of informed consent having been provided by the data subjects, the GDPR specifies a number of criteria. Which of the following is not a criterion from the GDPR?
    a. The consent is not valid if the data subject has no real choice.
    b. The consent must be freely given.
    c. **The consent is provided after processing.**
    d. The consent must be informed.

DPbD and by Default

1. All possible measures need to be taken to be compliant with Data Protection by Design as in the GDPR.
    a. True
    b. **False** (Only reasonable measures need to be taken, whatever that ends up meaning.)
2. Reasonable technical and organizational measures should be taken to protect data subjects to be compliant with Data Protection by Design as in the GDPR.
    a. **True** b. False
3. Data Protection by Design as in the GDPR is identical to Ann Cavoukian's Privacy by Design.
    a. True **b. False**
4. Data processors are directly responsible for Data Protection by Default.
    a. True
    b. **False** (Data controllers are responsible.)
5. Enabling all functionality and features by default in a service is compliant with Data Protection by Default in the GDPR.
    a. True **b. False**
6. Strong privacy protection should be enabled by default to be compliant with Data Protection by Default in the GDPR.
    a. **True** b. False

From DPbD and by Default to DPIAs

1. It's clear what the impact of the GDPR will be.
    a. True **b. False**

2. Understanding privacy risks are fundamental to designing for privacy.
    - a. **True**
    - b. False
3. DPIAs/PIAs are useful to have done when dealing with personal data breaches.
    - a. **True**
    - b. False
4. It's possible to leave everything concerning personal data breaches and the obligation to notify supervisory authorities to consultants that can be hired when a breach is detected.
    - a. True
    - **b. False**

PIA as a Process

1. What is the condition to carry out a Data Protection Impact Assessment according to Art 35 GDPR?
    - a. Where the deployment of a new technology may have any impact on data subject's privacy.
    - b. **Where a type of processing is likely to result in a high risk to rights and freedoms of natural persons.**
    - c. There is no such condition for DPIAs.
    - d. Where there is collection and processing of personal data.
    - e. Where a particular new technology is being developed and deployed.
2. Based on the description of a DPIA in Art 35 and the definition of a PIA in the ISO 29134, we can state that they are unequivocally identical.
    - a. True
    - **b. False**
3. Who benefits the most from PIAs?
    - a. Organization
    - b. **Data subjects and general public**
    - c. Regulators
    - d. Project managers and upper management staff
    - e. Employees
4. Which of the following steps is not traditionally part of a PIA process?
    - a. Identify and consult with stakeholders
    - b. Map personal information flow
    - c. Conduct a threshold analysis
    - d. Identify privacy issues
    - **e. Implement countermeasures in the system**

PIA Frameworks

1. Choose the correct answer. Regarding PIA Frameworks, it is right to say that:
    - a. Most of the PIA Frameworks work best for 'Data Privacy' but not really for 'Privacy' in its broader dimension.
    - b. The PIA frameworks proposed by CNIL (France) and ICO (UK) are recommended only for their jurisdictions.
    - c. The PIA RFID framework is only suitable for this specific kind of applications (i.e., RFIDs).
    - **d. Many researchers and DPAs have been articulating and systematizing PIA Frameworks to the point that today we have many suitable methodologies to carry out PIAs.**
2. Choose the correct answer. Regarding PIA Frameworks, it is right to say that:

    a. **PIA frameworks have already achieved a level of maturity that allows researchers and DPAs to agree upon many of the used methods (e.g., system documentation, threat analysis and controls, and reporting).**
    b. Existing PIA frameworks are significantly different from each other, so that organization have to carefully choose only the one that works for them specifically.
    c. In general, organization do not need a PIA framework because the GDPR only requires DPIAs which tend to be much simpler.
    d. There is a lack of methodologies for DPIAs, although many PIA frameworks have already been published.

3. Match the PIA framework with its right comment.
    a. PIA RFID – **Considered as a sector-specific PIA methodology**
    b. ICO's PIA – **A streamlined version of its previous PIA handbook**
    c. ISO 29134 – **Recently published new standard for PIAs**
    d. CNIL's PIA – **Composed by a set of manuals published by the French DPA**

DPIAs Threshold Analysis

1. What is the main purpose of Guidelines on DPIAs provided by WP29?
    a. To establish a criterion for an acceptable DPIA.
    b. **To provide a consistent interpretation and criteria on whether a DPIA is required.**
    c. To provide a consistent list of existing EU DPIA Frameworks.
    d. To establish which processing operations are subjects to a DPIA.
2. Match the following examples of processing with their possible relevant criteria.
    a. Use personal data from users in a social network platform for targeted advertising. – **Evaluating and scoring**
    b. Collection and processing of health data of patients. – **Sensitive data**
    c. Employers requesting access to employees' professional social networks (e.g., LinkedIn, ResearchGate) in order to improve their HR's records. – **Data concerning vulnerable data subjects**
    d. Use of drones for sending letters and parcels to the customer's home. – **Innovative use of applying technological or organizational solutions**
3. During the threshold analysis, a project matches only one of the items in the established criteria. Would it be mandatory to carry out a DPIA?
    a. Absolutely
    b. Not necessarily

PIA RFID

1. Which of the following items is not part of the PIA methodology proposed by Oetzel & Spiekermann (2014)?
    a. System Characterization
    b. Threshold analysis
    c. Definition of Privacy Targets
    d. Identification of Threats
    e. Documentation of Residual Risks
2. Match each step of the PIA methodology with its respective output (i.e., part of the PIA Documentation).
    a. Characterization of the System – **System Documentation**
    b. Definition of Privacy Targets – **List of Privacy Targets**

    c. Evaluation of Degree of Protection Demand – **List of Privacy Targets & Their Impact Degree**
    d. Identification of Threats for each Privacy Target – **List of Threats & Their Likelihood**
    e. Identification and Recommendation of Controls against Threats – **List of Controls**
    f. Assessment and Documentation of Residual Risk – **Residual Risks & Control Implementation Plan**
    g. Documentation of PIA Process – **PIA Report**
3. In the PIA methodology, all the Privacy Principles and Privacy Targets are derived from the GDPR. However, the authors (Oetzel & Spiekermann) explained that these principles and targets can be also mapped in a more complete list of privacy threats. Where does this list come from?
    a. Cavoukian, A., 2009. Privacy by design: The 7 foundational principles. implementation and mapping of fair information practices. Information and Privacy Commissioner of Ontario, Canada.
    b. Westin, A.F., 1968. Privacy and freedom. Washington and Lee Law Review, 25(1), p.166.
    c. **Solove, D.J., 2005. A taxonomy of privacy. U. Pa. L. Rev., 154, p.477.**
    d. EC (European Parliament and Council of the European Union). (1995) Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal of the European Communities L 281/31: 31–50.
    e. OECD (Organization for Economic Cooperation and Development). (1980) Guidelines on the protection of privacy and transborder flows of personal data.
4. According to the PIA methodology, if a threat is likely to exist a control MUST be determined to mitigate it; no matter the associated level of impact.
    a. **True**
    b. False
5. Given that a threat is likely, and it is associated to a Privacy Target that demands 'medium' level of protection. What is the level of rigor for its relevant control measure?
    a. **Strong**
    b. Very strong
    c. Satisfactory
6. Controls to minimize, mitigate and eliminate threats usually fall into two categories:
    a. Privacy and security
    b. Technical and non-technical
    c. Technical and organizational
    d. Prevention and detection
    e. Privacy and Data Protection
7. The final PIA Report should always be made available to the public with easy and accessible writing.
    a. True
    b. False

PIAs in Practice

1. DPIAs are always mandatory in the GDPR.
    a. True
    b. False
2. The more PIAs that are performed the better.
    a. True
    b. **False** (While practice makes perfect, too many PIAs may lead to PIA fatigue.)
3. How data processing is assessed in a PIA should be adopted to the target of evaluation.

a. **True**
b. False

4. PIAs should be user-centric, not organization-centric.
   a. **True**
   b. False
5. A PIA is a one-time task.
   a. True
   b. **False** (A PIA is a process)
6. By making the mistake of focusing on organizational risks instead of users' privacy risks, we may avoid risks instead of mitigating them.
   a. True
   b. **False** (An organizational focus leads to risk mitigation, not risk avoidance, which is preferable for users.)
7. Research shows that, in general, PIAs lead to privacy-friendly systems.
   a. True
   b. **False** (Research shows that PIAs, at best, lead to data protection compliant systems, not privacy-friendly systems.)

Chapter 4 – Privacy risk assessment

PIA and risk assessment

1. Which of the following elements are part of the privacy risk management process?
   a. revise privacy policy
   b. production of a report for management
   c. **communications and consultation with stakeholders** (Only through communication with stakeholders, privacy risk and impact can be understood correctly.)
   d. **establishing the context** (First, the context of PII processing has to get established!)
   e. creating a PII logfile for debugging
   f. education of end users
   g. publish privacy breaches
   h. **monitoring and reviewing risks and controls** (Continuous monitoring of risks is part of risk assessment!)
   i. **treating risks** (Risk treatment is the main reason for running risk assessment processes!)
   j. assessing risks
2. Which input data is used to assess privacy risk?
   a. legal violation of data protection legislation
   b. **magnitude (cost and impact) of an occurring risk** (The damage done by a realized risk is an important input to risk assessment!)
   c. identity theft statistics
   d. end user privacy attitudes
   e. **likelihood/probability that a privacy risk occurs** (The actual or expected occurrence of the risk is an important input parameter!)
   f. cost of system administration
3. Which of the following types of privacy shall be considered during a Privacy Impact Analysis (PIA)?
   a. privacy of the CIO
   b. privacy of business networks
   c. privacy of service provider transactions

   d. **privacy of personal communications**
   e. **privacy of the person**
   f. privacy of business transactions
   g. **privacy of personal behavior** (Personal profiling may impact privacy!)
   h. **privacy of personal information**

4. What does best characterize Privacy Impact Assessment (PIA)?
   A Privacy Impact Assessment (PIA) is __________________ for identifying and addressing privacy issues in an information system that considers the future consequences for privacy of a current or proposed action.
   a. **a permanent process**
   b. a regular process
   c. an on-going process
   d. a cyclic process
5. What does the term "duality of privacy risks" refer to?
   a. Dual risks emerge from compliance risks and privacy regulation.
   b. Privacy risk is realized as systemic risks and personal risks.
   c. **Privacy risk is realized as business risks and user risks.**
6. Which of the following alternatives best describes the core process of an Information Security Management System (ISMS)?
   a. **An ISMS is a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process characterized by PLAN, DO, CHECK, ACT phases.**
   b. An ISMS is a software platform that enable Chief Information Officers and their security staff to automatically monitor, configure and protect network security through PLAN, DO, CHECK, ACT.
   c. An ISMS is technology to automatically classify new risks, to quantify them, produce ontologies describing them, plans to protect against them (PLAN), defend against then (DO), check for collateral damage (CHECK) and to used applied calculus transfer (ACT) to improve system policy.
   d. ISMS refer to a set of procedures defined by the International Society of Military Sciences (ISMS), an international military research organization defining PLAN-DO-CHECK-ACT tactics in cyber warfare.

Privacy controls quiz

1. Privacy controls are used for various purposes and under various contexts. Please complete the text below by choosing the correct alternative!
   a. _____ are used to prevent a threat from being realized in a damage.
      i. **Preventative controls**
      ii. Preventive controls
   b. _____ help recognizing that a threat has affected a system.
      i. Detective controls
      ii. Detection controls
   c. _____ reduce the effect of a threat by reducing the damage realized.
      i. Corrective controls
      ii. Correction controls
   d. _____ are used to mitigate or lessen damage by providing alternative
      i. Compensatory controls
      ii. Compensation controls

2. Which of the following statements about when a privacy control is used, is true?
   Detective controls mitigate privacy risks when...
   a. No answer text provided.
   b. ... risk impact has changed after a data protection impact assessment.
   c. ... new vulnerabilities get known with vulnerability databases.
   d. … a risk has been realized that should get acted upon immediately.

3. Please chose the eight privacy strategies proposed by Colesky, Hoepman, and Hillen from the list below.
   a. Change
   b. **Enforce**
   c. Share
   d. **Minimize**
   e. Operate
   f. **Control**
   g. **Inform**
   h. **Abstract**
   i. Retain
   j. Store
   k. Breach
   l. **Hide**
   m. **Demonstrate**
   n. **Separate**
   o. Collect

4. Which of the following criteria are used to select privacy controls?
   a. Mobile phone models
   b. CEO qualification
   c. **Goal conflicts**
   d. **Procedural feasibility**
   e. **Budget limitations**
   f. Machine learning
   g. Churn rate

Chapter 5 – Privacy Management

Quiz 1

1. How are the four phases of IT management called?
   a. Check, Action, Procure, Act
   b. **Plan, Do, Check, Act**
   c. Plan, Outsource, Audit, Implement
   d. Check, Manage, Implement, Run

2. How many principles has "Privacy by Design"?
   a. 9
   b. 12
   c. **7**
   d. 3

3. What is the privacy-violating actions described by Dan Solove?
   a. Data accumulation, De-anonymization, Surveillance, Oppression
   b. Profiling, Spying, Spam Mail, Data Breach
   c. Identification, Authentication, Accumulation, Dissemination
   d. **Information collection, Information processing, Information dissemination, Invasions**

4. What are the stakeholders that are referred to in data protection regulation?
   a. **data subject, data controller, data processor**
   b. big data, machine learning, consumer advocacy groups
   c. Programmers, data bases, consumers
   d. Telecom industry, computer industry, governments

5. Why is the C-I-A (confidentiality, integrity, availability) approach not sufficient to comply with data protection legislation?
    a. No answer text provided.
    b. **Because it does not provide any means for data flow control, handling data subject consent, or minimizing consumption of personal data.**
    c. The C-I-A approach complicates system development and performance with too much cryptographic complexity.
    d. The CIA should not handle citizen's personal data at all!
6. Which types of pseudonyms can, according to Pfitzmann/Hansen, get used in online interactions?
    a. e-mail addresses, social media profiles, mobile phone numbers, credit card numbers
    b. self-chosen pseudonyms, self-signed pseudonyms, imposed identities, government identities
    c. **person pseudonyms, role pseudonyms, relationship pseudonyms, role relationship pseudonyms, transaction pseudonyms**
    d. citizen numbers, social security numbers, digital certificates

Chapter 6 – Privacy engineering & privacy patterns

Privacy foundations

1. Below you will find several statements about the GDPR. Please tick all correct statements.
    a. Data controllers process data on behalf of data processors.
    b. Processing of personal data of European data subjects must meet the requirements of the GDPR if and only if the data processor is based in Europe.
    c. Law enforcement activities are covered by the GDPR.
    d. One of the goals of the GDPR is to harmonize the data protection legislation across Europe.
    e. **Processing of personal data of European data subjects must meet the requirements of the GDPR.**
2. Below, you will find seven phrases, stating bad examples regarding designing privacy. Map each phrase to its "inverse" principle of the group of the seven privacy-by-design-principles that it violates.
    a. "We'll deal with that potential privacy issues if it really shows up." – **Proactive not reactive**
    b. "Click here to opt-in for improved privacy." – **Privacy as the default**
    c. "Let's first deal with the core functionality of the system. We integrate a privacy component later." – **Privacy Embedded Into**
    d. "We can either have privacy or full functionality - not both. Your choice!" – **Full Functionality**
    e. "Our webservice is accessible via HTTPS only - that's enough privacy." – **End-to-end security**
    f. "Don't tell anyone how we protect our data. That's best for privacy!" – **Visibility and transparency**
    g. "Hide the privacy policy behind this tiny button in the bottom right. Users won't read it anyway." – **Respect for user privacy**

3. Which of the following statements describes the need for a PIA according to the GDPR best? You must perform a PIA of a system if...
    a. The GDPR does not state any requirements for PIAs.
    b. ...the system deals with personal data.
    c. ...the system involves deployment of a new technology potentially impacting users' privacy.
    d. ...the system is supposed to process personal data of EU citizens.
    e. ...its processing of data is likely to result in a high risk to rights and freedoms of natural persons.
4. Which of the following is ***not*** a typical step in PIAs?
    a. Conduct a threshold analysis.
    b. Map the flow of personal information.
    c. **Implement countermeasures into the system.**
    d. Identify and consult with stakeholders.
    e. Identify privacy issues.
5. Of the following list, which ones are objectives of PETs?
    a. Control over personal data
    b. Data security and integrity
    c. Lawful processing of data
    d. Data minimization / avoidance
6. Why are PETs important in the context of the GDPR?
    a. The GDPR is a collection of PETs.
    b. The GDPR has a paragraph listing the relevant PETs.
    c. PETs are not relevant to the GDPR.
    d. PETs and GDPR are basically the same thing.
    e. **PETs are countermeasures to be included in the DPIA.**

Software Architecture Concepts

1. Below you find several statements about software architecture and the concepts introduced in this module. Check the correct statements in order to pass this question. Group of answer choices
    a. A software system's architecture must contain all details of the system structure and behavior.
    b. Software architecting integrates analyzing what software system needs to be built and how it should be built.
    c. An architectural tactic is a reusable decision that describes how (a part of) a system might address a desired quality attribute.
    d. Creating a software architecture means do a “big design up front”, this means, first a complete design of the system has to be created before the implementation can start.
    e. Software system developed in an agile way usually do not have and do not need a software architecture.
    f. As a software architect, you do not need to understand the requirements of a system.

   g. **Software architecture involves making principle design decisions from a set of alternatives that determine macro-structures aiming to adhere to a given set of requirements.**
   h. **Understanding the desired quality attributes for a software system is of particular importance for the software architect.**
2. Below you will find a few fictitious requirements that could be defined for health information system. Identify for each of these requirements, whether it constitutes a functional requirement, a quality attributes requirement, or a constraint.
   a. The health information system will provide output from all commands within 1 second – **Quality attribute requirement**.
   b. The system shall automatically generate reports for printing after 17.30 on the last working day of the month – **Functional requirement**.
   c. The system shall implement patient privacy provisions as set out in the national health systems standard for patience privacy i.e. HStan-03-2006-priv – **Constraint**.
   d. Users of the system shall authenticate themselves using their health authority identity card – **Functional requirement**.
   e. The manager responsible for the development team insists that the system must use 128-bit encryption for all transactions – **Constraint**.
   f. Java will be used as the development language because this is the common expertise of the development team – **Constraint**.
   g. The system shall be available to all clinics during normal working hours (Mon–Fri, 08.30–17.30). Downtime within normal working hours shall not exceed five seconds in any one day – **Quality attribute requirement**.
3. Here you find several requirements. Match each of these requirements with the quality attribute that it addresses. There is one requirement for each of the possible answers which are seven different quality attributes and the option "Not a quality attribute".
   a. The system should be able to run without modification on any operating system for which a Java Runtime Environment (JRE) version 7 or higher is available. - **Portability**
   b. The new library system needs to be able to interchange book data according to the format defined by the national library. - **Compatibility**
   c. At 50% load and below the system should be able to respond to user search queries within 1 second. - **Performance**
   d. No part of the system should be accessible without authenticating a user. - **Security**
   e. The system should not be down for more than 5% in a year. - **Reliability**
   f. It should not take more than 4.5 person days to fix a category 2 defect in the system including regression testing and documentation updating. - **Maintainability**
   g. Staff and students should be able to use 75% of the system's functionality after 2 hours of training. - **Usability**
   h. The eLearning system shall generate monthly management reports showing the number of students that logged into the platform each month – **Not a quality attribute**

Privacy design strategies

1. <u>Ticketing system</u>

A public transport company provides a mobile app via which customers can buy electronic tickets for their busses, trams, etc. Beside other functionality, customers can enter the start and final destination of a trip they wish to make and buy a ticket for this trip. The ticket is electronic and loaded onto the customers mobile phone, ready for use.

For user convenience, the system stores information about the routes that customers search and buy tickets for on central servers; this way, users travelling the same route frequently can simply select entries from a "purchase history" in their app instead of having to manually enter the same start and destination for each travel again and again.

The software architect decides to change two things. Firstly, users shall be able to switch off the function of storing a purchase history. Secondly, the purchase history, if activated, shall be stored on the user's device not on central servers.
Which privacy design strategies does the software architect plan to follow?

a. Demonstrate
b. Hide
c. Inform
d. **Separate** (That's right. Storing personal data separately, the purchase history on the user's device in this example, is an example of the Separate strategy.)
e. **Control** (Exactly! Having the option to switch of the purchase history gives the user some control over the processing of his personal data!)
f. Aggregate/Abstract
g. Enforce
h. Minimize

2. A Webshop example

Recently, the webshop system that the software architect was working on, has been re-deployed "to the cloud", using the services of a commercial cloud service provider. This migration also included all databases including those storing customer data.

In this context, the software architect decided to extend the registration process for new users: they are now informed that data is stored at a third-party including all personal data such as contact information, data about the user's orders, etc. They are also informed about another change introduced with the migration: all personal data is stored in encrypted form.

Which privacy strategies were implemented?

a. Aggregate/Abstract
b. Inform (That's right. At least new users are informed about the way their personal data is processed.)
c. Enforce
d. Control
e. Hide (Yes! Encryption is a common way to implement the Hide strategy)
f. Minimize
g. Demonstrate
h. Separate

3. E-learning platform

In this example, the software architect wants to change the way how students are internally identified on a e-learning platform (such as Canvas).

Currently, student is assigned an identifier when they register with the platform. The identifier is constructed based on the birthday of the person encoded as YYMMDD (e.g. 850523 for someone born on May 23, 1985) followed by random sequence of 8 digits (e.g., 850523-75983261).

The software architect decides that the format shall be changed as it unnecessarily reveals personal data and shall consist of a random sequence of digits only.

Which privacy design strategies does he/she plan to follow?

a. Demonstrate
b. Minimize (Yes! Instead of "day of birth" + "random number", only a random number shall be used. The number of data field used is reduced.)
c. Enforce
d. Separate
e. Hide
f. Inform
g. Control
h. Aggregate/Abstract

4. Legacy system

The software architecture has recently become responsible for a legacy system without documentation of the architecture. As part of the reconstruction of the architecture, she wants to document how personal data is processed and stored. She also requests to have a demo of the system available at all times which shows how data is processed in case potentially new customers want to know.

Which privacy design strategies does she plan to implement this way?

a. Control
b. Aggregate/Abstract
c. Hide
d. Enforce
e. Separate
f. Demonstrate (Correct! Both actions, updating the documentation and preparing a demo trail so they explain privacy protection measures are examples of the Demonstrate strategy.)
g. Minimize
h. Inform

5. Messaging system

The software architect is responsible for modifying an instant messaging system. The way messages shall be stored needs to be changed. Among other things,

- all messages between any users of the messaging service shall be stored in encrypted form,
- messages shall be stored in an independent database from any other data; references to sender and receiver are stored in encrypted form
- IP addresses of senders and receivers will not be stored unless requested by law. So far IP addresses have been stored for 10 years.

Which privacy design strategies does he plan to implement this way?

a. Inform
b. **Hide** (Perfect! Again, this refers to encryption for hiding personal data from plain view!)

c. **Separate** (Yes! Messages are stored separately and links to sender and receiver are encrypted.)

d. **Minimize** (Correct! This refers to the IP addresses not being stored longer than necessary.)

e. Aggregate/Abstract

f. Control

g. Enforce

h. Demonstrate

6. <u>Another webshop</u>

A webshop system includes a recommendation system that suggests products to customers based on what they bought previously. This is based on the assumption that users might be interested in similar articles, complementary accessory, etc. For this purpose, the purchase history of users is analyzed including information about products bought, time of purchase, and more.

The software architect thinks that this violates the users' privacy. She suggests the following changes:

- Enable users to switch off automatic recommendations - information about previous purchases is only stored for the purpose of billing and (re-) shipment.
- For the purpose of automatic recommendations, only the product category of a purchased good is stored and analyzed instead of the exact product.
- Additionally, only the year of purchase is stored and analyzed instead of the exact date.

Which privacy design strategies does she implement this way?

a. Demonstrate

b. Separate

c. Hide

d. **Control** (Yes. Again, it is the possibility to switch of the functionality completely that gives users some control.)

e. Inform

f. **Aggregate/Abstract** (Correct! Information about purchases are made more abstract: product categories instead of product, year of purchase instead of day of purchase!)

g. Enforce

h. Minimize

Privacy Patterns

1. Look up the pattern "Onion Routing" in the pattern catalogues linked in this module (feel free to research other resources in case you would like to have more detailed information about the pattern).

Which of the following statements about the pattern are true? Please tick the correct statements. Group of answer choices

a. Onion routing consumes more bandwith and might lead to higher latency compared to "plain" networks.

b. The content of messages (e.g. login information for your online banking account) sent via an onion routing network are automatically encrypted and hence protected.

c. The main motivating problem for this pattern is the question of how to hide the information contained in messages sent over a network.

d. In onion routing, messages are usually encrypted several times.

    e. **The problem that the pattern addresses is essentially the problem of how to obfuscate senders and receivers of messages.**

2. Imagine a web-based health information system where users can search for all kinds of health-related information, e.g. about symptoms and treatments of diseases.

   The system uses third-party services to analyze the traffic on the website. An unfortunate implementation causes user searches to be transferred to these third parties as well, such that the third party can, for example, analyze what diseases users are looking up.

   The implementation cannot be changed easily. However, which of the following patterns might help in the meantime? Select the most useful and easiest-to-implement one.
    a. "Protection Against Tracking"
    b. "Pseudonymous identity"
    c. **"Use of dummies"** (Exactly, "dummy" generated actions could come from fake searches on the website, possibly auto-generated by a small "confuse the analysis tool" plugin.)
    d. "Added-noise measurement obfuscation"
3. Which of the following cases are instances of applying the "Strip Invisible Metadata" pattern?
    a. A health information system blackens diagnosis information when generating sick leave reports to be handed in to the employer.
    b. **Before uploading, a blog platform removes EXIF information from photos (such as date of picture, location, etc.).**
    c. During user registration, a social network offers users to hide certain personal data (e.g., data of birth) from other users.
    d. **A browser plugin removes information about the browser version from requests to servers.**
4. Look up the pattern "Handling unusual account activities with multiple factors" in the pattern catalogues linked in this module (feel free to research other resources in case you would like to have more detailed information about the pattern).
   Which of the following statements about the pattern are true? Please tick the correct statements.
    a. In case a suspicious login attempt via a mobile is registered, sending a text message with one-time password is a secure second authentication factor.
    b. **In case of unusual activities, the account holder should be informed as soon as possible.**
    c. **The pattern tries to balance usability and privacy protection.**
    d. The pattern suggests that a hardware token should always be used as second authentication.
    e. The pattern essentially suggests to always authenticate users through multiple factors.

1. Please tick the true statements about privacy dark patterns!
    a. Privacy Zuckering is about not allowing users to modify privacy settings.
    b. Privacy dark patterns work because they often take advantage of psychological properties of human beings.
    c. "Shadow User Profiles" may only affect users that explicitly registered for a service.
    d. Terms and conditions formulated in an unclear or complicated way are known dark privacy pattern.
    e. The terms "privacy anti-patterns" and "privacy dark patterns" can be used synonymously.
    f. A privacy dark pattern is a privacy pattern that has not been proven useful to protect privacy.
    g. The privacy dark pattern implements the "Maximize" strategy.