Guest Lecture
Data Privacy & GDPR

TDT4237

Presentasjon:
Knut Soelberg

Dato:
24.03.2025

Aboveit

Background

In a world of rapid development of new technology, which is used in ever-changing contexts, we face several challenges. A key challenge is how to safeguard privacy in digital products and services while maintaining accessibility and user-friendliness.

The EU General Data Protection Regulation (GDPR) has been part of the Norwegian Personal Data Act for almost 7 years. However, the GDPR is often experienced as complex and not very accessible. Furthermore, many experience that it is unclear what is a necessary level of privacy assessments and associated documentation.,

My experience shows that it is possible to establish a structured, "easily" accessible and transparent approach to how to ensure that digital services comply with the Personal Data Act.

The guest lecture focuses on raising awareness of what should be done by privacy assessments with associated documentation and what their role should typically be in this context. The workshop also focuses on good examples and the use of simple templates for privacy assessments.

About Me

- Master's degree in computer science – University of Oslo
- I have most of my carrier been a consultant, but also been a researcher at the Norwegian Computing Center (NR)
- Project management, agile digital product development, change management and data privacy are my special areas
- I have been a Project manager and advisor (government contractor) in major development projects in the public sector
- I have had several Data privacy assignments in a 3-year period starting in 2018
  - Based on that experience, I started lecturing data privacy courses
- For the last 5 years (2020-2024), I have been a project manager (government contractor) at the Norwegian Digitalisation Agency (Digdir) helping them to modernize Id-porten and their digital joint solutions (fellesløsningene)

Aboveit - Key numbers

2023
NOK 160 million in revenue

135 +
Employees

34
Average age

28%
Women

75+ diferent customers

Consultancy services

Architecture & Cloud Services

Usabillity & Design

Project Management & Testing and Test Management

System Development & Integrations

Practical information

- Guest Lecture: 10-12 including 1 break
- Workshop: 14-16 including 1 break

- The slides used in this lecure and the workshop is distributed
- Questions are welcome any time

The presentation is quite comprehensive so that it can be used as a reference later

Vocabulary (English - Norwegian):
https://www.datatilsynet.no/en/regulations-and-tools/vocabulary/

Agenda

Lecture

- Data Privacy and GDPR Basics
- How to Describe the processing of Personal Data
- How to Assess compliance with the privacy principles
- Product Teams and Privacy by design

Workshop (14h-16h)

- Examples and case

Objectives: Lecture and workshop

- Understand and be able to apply GDPR's basic concepts and principles
- Understand what must be described and assessed when a projects/teams develops a product that processes personal data
    - Examples and exercises (workshop)
- **Be aware of that privacy is an interdisciplinary discipline**
- Be able to identify issues related to privacy that must be raised by the customer/product owner for further (legal) clarification and authorization

Data Privacy and GDPR Basics

Introduction: Data Privacy and GDPR

- What is Data Privacy about?
  - **Privacy is about the right to privacy and the right to decide when someone can use your own personal data**
- In EU/ECC, Data privacy is Regulated by the General Data Protection Regulation (GDPR) as well as relevant special laws related to the various applications / domains
- Do you think that
  - Privacy is basically only about security?
  - It is almost impossible to write a formal DPIA document?
  - A product team automatically develops products supporting “privacy by design”?
- **Data Privacy is interdisciplinary and can be made understandable**
  - Privacy by design can become an inherent part of the product development without too much effort
- Today's lecture and workshop will address the following
  - How the descriptions and assessments necessary regarding data privacy can be made “simple”
  - The product team is key to ensure “privacy by design” as a native part of digital products

Personal data – What is important?

To handle personal data as part of the business' services and processes correctly in accordance with the law

The law does not distinguish between
what is processed by IT systems
and
what is processed manually

The goal is
not to avoid using personal data,
but to use personal data correctly
in the correct context

Challenge

- Data Privacy is regulated by the Personal Data Protection Act / GDPR
  - Requires that the business and its suppliers have
    - employees who understand and can apply the basic concepts and privacy principles defined in the GDPR
- **To secure high quality privacy assessments, you need relevant domain expertise!**
- Insufficient understanding of how to comply with the Personal Data Act results in
  - Unilateral focus on IT systems and IT security
  - Insufficient focus on the business domain
  - Insufficient authorization by relevant "business areas"

Lack of understanding of how to ensure good Data Privacy results in **false safety and lack of compliance** with the Personal Data Act

The Personal Data Act (Personopplysningsloven)

Available from Lovdata

- https://lovdata.no/dokument/NL/lov/2018-06-15-38 (in Norwegian)
- https://lovdata.no/dokument/NLE/lov/2018-06-15-38 (in English)
- GDPR in English: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

Consists of 2 parts

- GDPR - General Data Protection Regulation
- Norwegian clarifications and additions

Most important parts of the EU regulation (in order of priority) when developing digital products

- I (definitions), II
- IV, III
- V

GDPR (EU regulation) - Chapter structur

I. General provisions

II. Principles

III. Rights of the data subject

IV. Controller and processor

V. Transfers of personal data to third countries or international organisations

VI. Independent supervisory authorities

VII. Cooperation and consistency

VIII. Remedies, liability and penalties

IX. Provisions relating to specific processing situations

X. Delegated acts and implementing acts

XI. Final provisions

Important Definitions and Principles

Correct understanding of important concepts and principles is crucial to ensure correct assessments of Data Privacy

Important Definitions

GDPR article 4

- Personal Data (Personopplysning)
- Processing (Behandling)
- Special categories of personal data (Særlige kategorier opplysninger)
- Controller (Behandlingsansvarlig)
- Processor (Databehandler)
- Recipient (Mottaker utlevering)
- The Data Subject (den registrerte)

Principles relating to processing of personal data (Personvernprinsipper)

GDPR article 5

- Lawfulness, Fairness and Transparency (Lovlighet, rettferdighet og åpenhet)
- Purpose Limitation (Formålsbegrensing)
- Data Minimisation (Dataminimering)
- Accuracy (Riktighet)
- Storage Limitation (Lagringsbegrensing)
- Integrity & Confidentiality (Integritet/konfidensialitet
- Accountability (Ansvarlighet)

Important Definitions GDPR – Personal Data

GDPR Article 4. Definitions

For the purposes of this Regulation:

1. *‘**personal data**’ means any information relating to an identified or identifiable natural person (‘data subject’); **an identifiable natural person is one who can be identified, directly or indirectly**, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or **to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person***

In other words:

Personal Data includes for example

Social Security Number (fnr) og contact information (adress, phone, email)

Important! Personal Data also includes all kind of information relatet to a person (data subjects). Personal data incudes behavioral patern, facts, results and health information

If you put together enough indirect personal data, you will be able to find the relevant natural person

Who (which IT-systems that) has the total overview and the link to the natural person does not matte

Flights: the following is also personal data for a passenger on a given flight

3 pieces of luggage checked in, security checked and loaded on board flight xx at yy.zz

Student loans: the following is also personal data for a given borrower/applicant

Application xx rejected <date>

Loan balance as of <date>: kr: yyyy

Important Definitions GDPR - Processing

GDPR Article 4. Definitions

For the purposes of this Regulation:

2. '**processing**' means any ***operation or set of operations*** which is performed on personal data or on sets of personal data, whether or not by automated means, such as ***collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction***

Processing - What does it mean?
The Personal Data Act applies to any form of processing of personal data

Processing includes manual paper-based handling as well as processing using IT IT-systems

Remember, storage is one of a large number of different types of processing (ref. definition of processing)

Processing - example:

Air travel: check in passengers and baggage, verify baggage before loading onto flight, onboard passengers onto flight
Student loans: Process loan application, request loan installments for given loan customer

Important Definitions GDPR - Special Categories of Personal Data

From GDPR Article 9.1

These categories of personal Data is defined as “special categories of personal data”

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person
- data concerning health
- data concerning a natural person’s sex life or sexual orientation

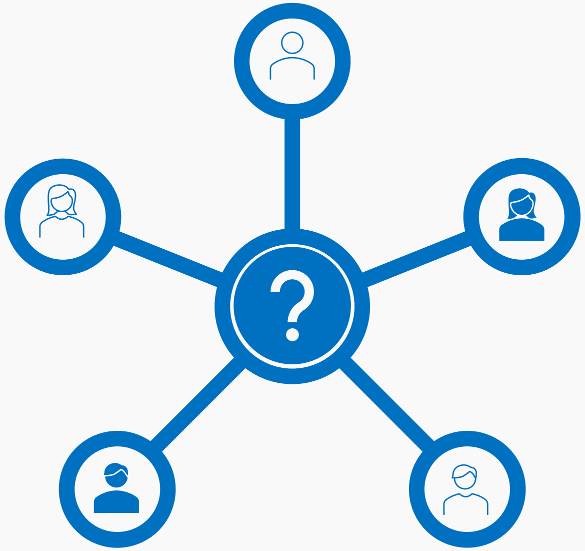
Important!

GDPR article 9.1 concludes that processing of Special Categories of Personal Data shall be prohibited

However, GDPR article 9.2 defines when article 9.1 shall not apply
These are strict exceptions (we will briefly walk through these exceptions later)

Important Definitions GDPR – Rolles

Roles is an important topic, however in this lecture we will not elaborate further



The controller
means the natural or legal person, public authority, agency or other body which*, **alone or jointly with others determines the purposes of the processing of personal data and the means to be used***

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

Recipient
means a natural or legal person, public authority, agency or another body, to **which the personal data are disclosed, whether a third party or not**

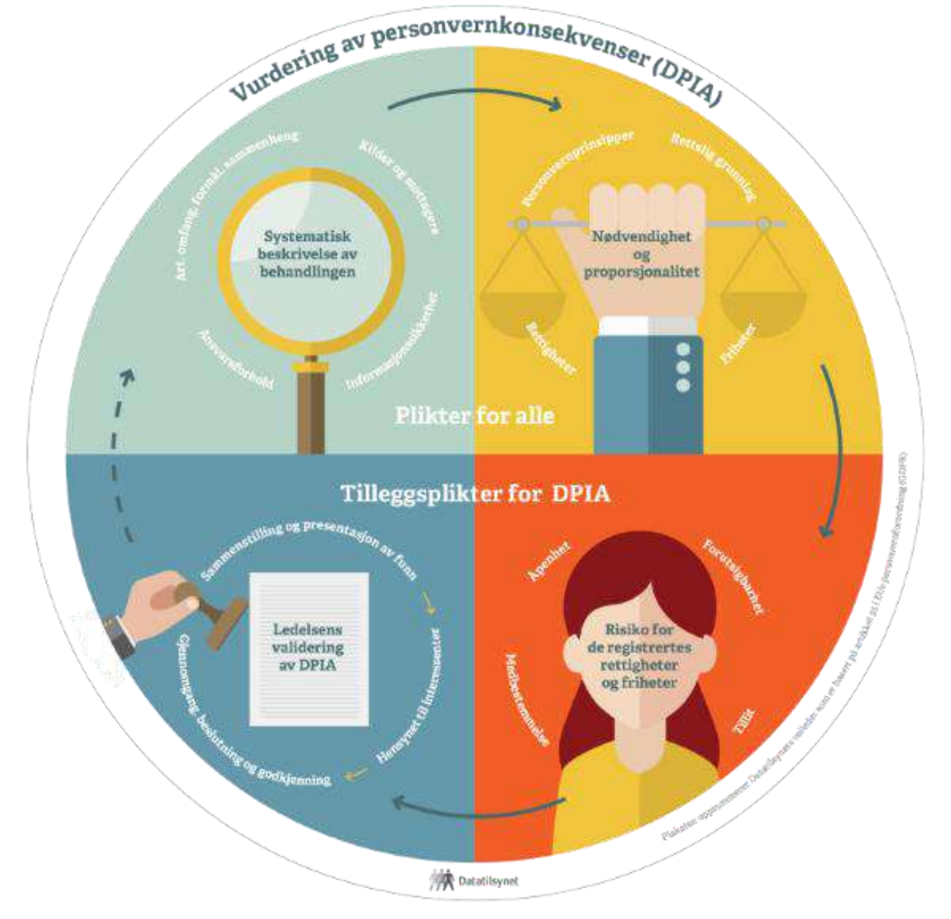
necessary

Data Protection Impact Assessment (DPIA)

- GDPR Article 35 describes when a DPIA must be prepared and what it must contain
  - A DPIA is a formal document, but GDPR places few requirements on such a document beyond its overall content
- Many businesses find that preparing a DPIA is a big job that is demanding to complete
  - A DPIA can be done short and simple – review real examples in the workshop
  - Too many businesses probably do not prepare a DPIA when necessary
- **Important!**
  - Assessing compliance with the privacy principles is always necessary according to GDPR
    - Not only when a formal DPIA document is needed!

We will walk through how to do assessment of compliance with the privacy principles as part the workshop this afternoon (examples and exercise)

Data Privacy assessments:
Iterative process as part of product development


Vurdering av personvernkonsekvenser (DPIA)
Art, omfang, formål, sammenheng
Kilder og mottagere
Systematisk beskrivelse av behandlingen
Informasjonssikkerhet
Ansvarsforhold
Personvernprinsipper
Rettslig grunnlag
Nødvendighet og proporsjonalitet
Rettigheter
Friheter
Plikter for alle
Tilleggsplikter for DPIA
Sammenstilling og presentasjon av funn
Ledelsens validering av DPIA
Hensynet til interessenter
Gjennomgang, beslutning og godkjenning
Åpenhet
Forutsigbarhet
Risiko for de registrertes rettigheter og friheter
Medbestemmelse
Tillit
Plakaten oppsummerer Datatilsynets veileder, som er basert på artikkel 35 i EUs personvernforordning (GDPR)
Datatilsynet

The Norwegian Data Protection Authority highlights the following 4 steps in an overall process for DPIA

1. Describe the processing of Personal Data
2. Assess compliance with the privacy principles
3. Assess the risk to the data subjects' rights and freedoms
4. Authorization

Remember this is an **iterative process!**

Always performed: Step 1 and 2 apply to all processing of personal data

Challenge

GDPR is “cryptic” for those who develop digital products

- Demanding to "translate" GDPR requirements into process and solution when developing digital products
- The regulation itself does not say anything about how to do this "translation"
- Current documentation available from the Norwegian Data Protection Authority are not very specific
- Both GDPR and the documentation available needs to be more specific about what privacy-by-design means and to enable privacy-by-design in a digital product

This lecture and workshop will guide you through the steps and documentation needed for this “translation”

How to Describe the processing of Personal Data
Focus: The products of an autonomous product team

Description of the processing of Personal Data - Topics

New or changed service / product – what needs to be identified and described?

Topics

- o The purpose of the processing of Personal Data
- o The nature and context of processing (High level functional description)
- o The scope of the processing
- o Sources for the collection of personal data
- o Recipients of personal data
- o Responsibilities (Who is Controller and processors?)
- o High level technical description

- An important **success criterion** is to ensure short, precise descriptions at an appropriate level of detail, at least initially
  - The descriptions should be understandable to 3. parties
  - The descriptions should be gradually elaborated over several iterations
- **NB! The description of the processing will be the basis for assessing compliance with the privacy principles and risk.**

The Purpose of processing of personal data

Purpose = end-user-oriented service

A purpose is typically a (sub)process or service that uses personal data

- Can consist of one or more processings (process steps)
- Should have a business focus
- Start by defining "coarse-grained" purposes
- Based on increased insight, split into smaller and more specific purposes during the development cycle if needed

Identifying appropriate* purposes *is a very important success criterion for good privacy protection

  - **Domain expertise** is required to identify a “good” purpose
  - Purpose is not the same as an IT system
  - An IT system can support multiple purposes

***During the workshop this afternoon, we will discuss several examples of* appropriate purposes**

Example: The description of the processing – Registration for internal event

To be discussed as part of the workshop

Purpose	The nature and context of processing (High level functional description)	Categories of personal data per category data subjects
Registration for internal events within Bouvet	Participants can search for upcoming internal events by category or follow a link. ***Participants register for an event that is open for registration.*** If the event serves food, the participant can "check the box for have food allergies". The participant will then receive a dialog to give explicit consent to state food allergies and then which food allergies. It is also possible to "centrally" give express consent to state food allergies and which food allergies apply. If this has been done and the participant is to register for an event with food, the participant can choose to check the box for "show registered food allergies to organizer" so that the organizer takes your dietary needs into account. ***Managers and other employees can create an event.*** Only the organizer can see what food allergies have been registered. Only the individual organizer can change the event information for their events. Everyone in the company can see who has registered for the various events, as this is, among other things, a means of increasing participation in the various events.	**Event participant (employee):** • Contact information (retrieved from internal IT-systems including master data) • Organizational information (organizational unit, employee number - retrieved from internal IT-systems including master data) • Registration information (event name, event time, registered/not registered, comments regarding registration, any food orders) • Food allergies (if relevant) **Event manager/organizer (employee):** • Contact information (retrieved from internal solutions with master data) • The events he/she manages incl status information

Testdata	The scope of the processing	Responsibilities	Sources for the collection of personal data
The product team members uses their own personal data as a basis for test data – food allergies are syntetic. Routines for the scope and deletion of test data have been established.	Event registration for an established event applies to all organizational units and their employees. Bouvet has over 2,000 employees, spread across several units throughout the country. In one year, the employees make more than 10.000 sign-ups	Bouvet is the data controller (and data processor). Microsoft (Norway) is sub data processor (Microsoft Azure).	No personal data is collected from external parties, only from internal systems (master employee data).

Recipients	High level technical description
No personal data is disclosed to external parties other than Microsoft Azure which is being used to run applications and store data in a data center in Norway. Regarding food orders, only the number of people with the various food allergies registered with the food supplier is disclosed.	IT systems and infrastructure: The solution is web-based and internally developed using .net and runs in the company's tenant in Microsoft Azure (data center in Norway) using SQL-db and Azure AD for authentication, authorization. Comment: This description should ideally be expanded with some more detailed information.

When do we need a complete DPIA?

How to validate if “High Risk”?

Assessments if "high risk" and the need to do a complete DPIA

Certain types of processing of personal data are considered to involve a more serious interference with privacy than others because

- The personal data processed are of a particularly sensitive nature
- How the personal data are processed constitutes a particular interference with the rights and freedoms of data subjects

If “high risk”, GDPR sets requirements for formal documentation as well as risk assessments

- Important to early consider whether "high risk" or not
- There is a list of criteria's used to evaluate ift “high risk” or not

Check list – “high risk” or not

A Complete formal DPIA is needed if 2 or more criteria's are met

Does the processing of Personal data include

1. Evaluation or scoring
2. Automated-decision making with legal or similar significant effect
3. Systematic monitoring of the data subjects
4. Sensitive data or data of a highly personal nature
5. Data processed on a large scale
6. Matching or combining datasets
7. Data concerning vulnerable data subjects
8. Innovative use or applying new technological or organizational solutions
9. Prevent data subjects from exercising a right or using a service or a contract

Source: Guidelines on Data Protection Impact Assessment (DPIA)

How to Assess compliance with the privacy principles?

Data privacy principles - Overview

Understanding these principles is essential for complying with GDPR

1. Lawfulness, fairness and transparency

2. Purpose limitation

3. Data minimization

4. Accuracy

5. Storage limitation

6. Information security

Ansvarlighet – overall management responcibillity

Data protection by design and by default

What does that mean?

The product team must ensure

- Compliance with privacy principles as an inherent part of the digital product development
  - Identify and implement the necessary technical and organizational measures to comply with each of the principles
  - The measures are identified and specified as part of the team's specification process according to the product roadmap
  - The measures should be in accordance with the nature of the processing and the product's risk profile
  - The principles set requirements for usability and technical quality. The level of quality for this depends on the nature of the processing, i.e. the risk profile
- **The measures are described** at an appropriate level
  - ***As** a part of product's epics and user stories*

Purpose limitation – how to comply (1/2)

Important: Identify the most appropriate purposes that focus on end-user-oriented services

- Use the time and the iterations needed to ensure that you have identified purposes that are appropriate

Verify that personal data processed for the purpose is not used in any context other than what is necessary and lawful

- For example: A bank can process personal data for banking purposes, but they can not (without further ado) process the same personal data for insurance purposes
  - Nor can they without necessary lawfulness transfer the personal data to partners that have other purposes (***which is sadly too common on the Internet today***)
- Ensure that the personal data and functionality is only available to those who contribute to achieve the purpose, in other words: “to make the service work”

Purpose limitation – how to comply (2/2)

Role-based access control is a good basic measure to ensure purpose limitation

- Both in terms of end users, APIs, operational tasks, etc.
- The different user groups should only have access to the information and services that are relevant to perform their responsibilities related to the purpose
- Don't forget: This also applies to roles related to operation and management, including monitoring and logs

Verify that all processing included are necessary and lawful

- Transfers of personal data to recipients and 3. parties
- Collection of personal data(using APIs) from 3. parties
- The use of data processors including public cloud

Transferring of personal data to recipients without a **valid purpose and lawful legal basis** is probably the **most common reason** why businesses receive **fines** related to violations of the Personal Data Act.

Data minimization – how to comply

Verify that only information that is necessary for the purpose (service) is collected

- This is not always obvious
- It is important that user dialogue is well-designed and does not collect more personal data than is necessary to deliver the service
- Minimize the use of free text fields
- It is important that the APIs used do not expose more information than necessary
- If commercial APIs are used, and these expose too much information, ignore excess information, do not store this. In the long term, the API should be improved

Example: For a purpose related to processing applications and allocating municipal housing, what information is necessary for the case manger to be able to state a decision? Is it sufficient for the applicant to only state the number of children in the household, or is it necessary to provide a lot of details about each of the children?

Accuracy – how to comply

- The principle requires that **the personal data processed is correct and that the result of the processing is correct**
  - The quality of data is important; however, it is also important to ensure the quality of specifications, code, development process and testing to ensure correct processing and correct "derived" personal data
  - Collecting personal data from external sources such as the National Population Register (Folkeregisteret) is an example of an appropriate quality-enhancing measure
- The principle requires that the personal data is correct in a year or two as well
  - This will typically demand automation of a periodic verification process
  - Online banks, among other, handle this by explicitly asking you to verify and update various types of basic information, e.g. once a year.

Storage limitation – how to comply (1/2)

- Different categories of personal data processed within the same purpose may have different storage periods
  - This must be explicitly considered by the product owner/business on a case-by-case basis
  - In some cases, there will also be requirements in special laws, e.g. the Archives Act
  - Also remember different types of logs
- Don't consider storage time only for normal cases
- The storage time must also consider exceptions - e.g. complaints, mishandling, fraud attempts, etc.

Storage limitation – how to comply (2/2)

- Assessing storage time is difficult in many cases
  - Start handling this early
  - Ask for legal and/or business assistance is often a good idea
- In many cases, there is a need for different types of analyses and statistics
  - Often this does not require personal data
  - Periodically anonymize relevant personal data for analysis/statistics, and then delete relevant personal data according to the storage limitation
  - Anonymization is not necessarily easy; it might be easy to fall into an "anonymization trap"
- Link to Datatilsynets supervisor for anonymization: anonymisering av personopplysninger

Information security – how to comply

- Technical and organizational measures to ensure personal data security, i.e. confidentiality, integrity and availability, must be assessed and described
  - This includes technical measures such as authentication and authorization mechanisms, logging/traceability, integrity checks, zone models/zero-trust models, encrypted communication and/or storage, etc.
- The level of the various measures must be assessed in relation to the results of the
  - Assessment of the privacy principples
  - The risk analysis (if full DPIA)
  - Tost-benefit assessments – GDPR does not require data controllers to "shoot sparrows with cannon"
- **Also remember organizational measures** such as. routines for deliveries, use of security standards, security policy, code reviews, security tests, devsecops
- Do not forget that the GDPR is based on the premise that **the level of measures must be linked to the risk profile of the purpose**, i.e. don't "shoot sparrows with a cannon"
  - Example: For some purposes, username and password are ok, while other cases require high level electronic ID (eID)

Lawfulness, fairness and transparency - how to comply

Complying to fairness and transparency is achieved by ensuring:

Real co-determination

- The data subject must have a choice, be given information, be given access, and so on

Real transparency

- Explain complex treatments and expected results when comparing personal data with other data sets and so on

Predictable treatment

This means

- User-friendly service
- Uniform case management (where relevant)
- Easily accessible and understandable privacy policy
- Functions/procedures for fulfilling the rights of data subjects

Legality is fulfilled by the product owner by getting the necessary assistance at an early stage to assess the legal basis for the purposes

- Remember that a legal basis must be identified for both the processing of ordinary personal data and special categories of personal data
- Several legal bases also require references to relevant special laws
- ***Remember that consent is one of many legal bases, but which is currently often misused***
- Do not confuse consent as a legal basis for a specific purpose (service) with consent for Cookies

Lawfulness of processing General Personal Data

GDPR article 6

Legal basis

a)consent

b)the performance of a contract to which the data subject is party

c)compliance with a legal obligation

d)vital interests

e)public interest or in the exercise of official authority

f) legitimate interests – Requires a **balancing of interests**

c) and e) is also to be linked to relevant laws or regulations

Remember: Consent is one of many possible legal bases,

- but is in many cases abused where there are better alternatives

Lawfullnes of processing of special categories of personal data - GDPR article 9.2 (Simplified version – for overview only)

a) explicit consent

b) fulfil obligations and exercise special rights in the area of labour law, social security law and social law

c) protect the vital interests of the data subject or of another natural person;

d) foundation, association or other non-profit body whose objectives are of a political, religious or trade union nature

e) personal data that it is obvious that the data subject has made public

f) establish, exercise or defend legal claims

g) The processing is necessary for reasons of important public interest, on the basis of Union or Member State law, which must be proportionate to the objective pursued, be compatible with the essence of the right to the protection of personal data and ensure appropriate and specific measures to protect the fundamental rights and interests of the data subject

h) preventive medicine or occupational medicine to assess an employee's work capacity, in connection with medical diagnostics, the provision of health or social services, the treatment or management of health or social services and systems

i) public health considerations

j) the processing is necessary for archival purposes in the public interest, for the purposes of scientific or historical research, or for statistical purposes;

The Rights of the Data Subject

What does that mean?

- The freedoms of data subjects are assessed in relation to the ETS no 5
- The rights of data subjects are described in GDPR article 12-23 and includes
  - Simple and good information about the processing must be provided to the data subjects
  - Right of access
  - Right to rectification and deletion (be forgotten)
  - Right to restriction of processing
  - Right to data portability
  - Right to protest
  - Right not to be subject to decision based solely on automated individual decisions
    - Exceptions in relation to the implementation of agreements, e.g. allocation of student loans
- This means that treatment should not reduce these rights and freedoms
- Personal data that goes astray can reduce these rights and freedoms

European Convention on Human Rights and Fundamental Freedoms – ETS no 5

- **The right to privacy** and protection of communications
- The right not to be discriminated against
- Freedom of thought, belief and religion
- Freedom of expression and information

What does this mean for your product?

- How the rights of the data subjects are fulfilled, and which rights are relevant will vary from case to case
- Some kind of self-service might be appropriate, but in many cases, handling this by using manual routines provides the best cost/benefit

Accountability and interference with privacy

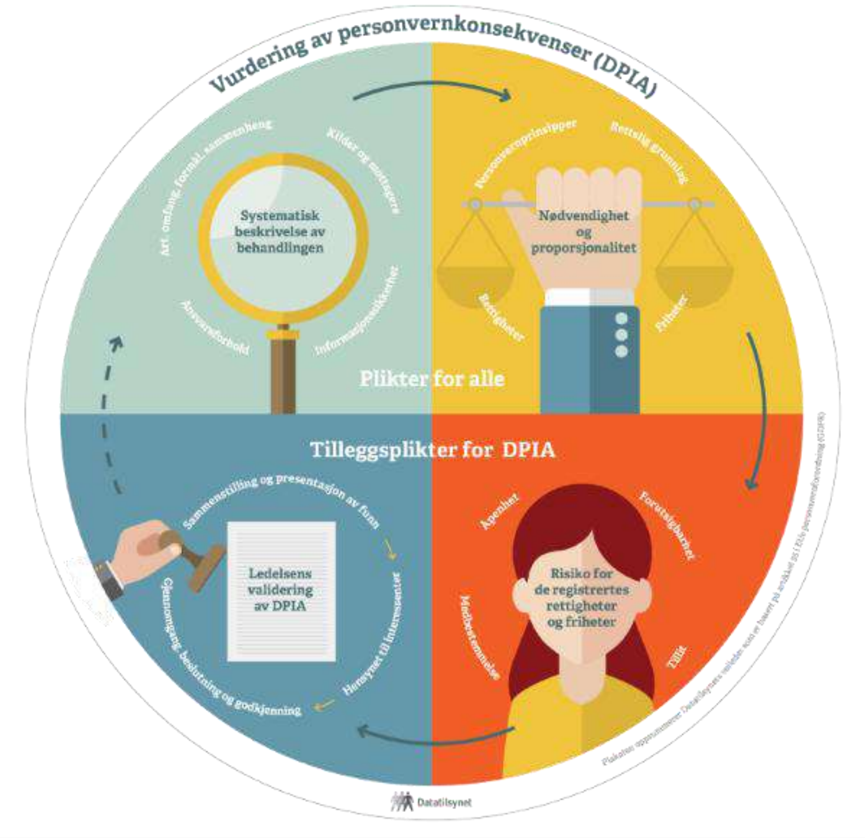
- Accountability
  - Means that the data controller and data processors, i.e. management, are responsible for ensuring that necessary privacy assessments are carried out and documentation is established
  - In practice, the team or project, typical has the operational responsibility
- Interference with privacy should match **necessity and proportionality**
  - Is the benefit for the data controller greater than the disadvantage for the data subject?
  - The greater the interference with privacy, the more important it is to explicitly consider this
  - The assessment of compliance with the privacy principles should highlight that necessity and proportionality match

Personal data as testdata

- The use of production data for testing is considered as processing of personal data
  - provided that the production data includes information about actual persons
- The use of synthetic test data is preferable from a privacy perspective if the production of synthetic test data is possible with an acceptable cost/benefit
  - Tenor testdatasøk is a tool from Digdir for finding synthetic test data across test environments in Norway
- Possible approach when production data must be used for testing
  - Justify and document why (nature of the processing and, if applicable, purpose)
  - Ensure good practices for storage time, sharing, and access control for the test data

Product Teams and Privacy by design

Data Privacy: Iterative process as part of product development


Vurdering av personvernkonsekvenser (DPIA)
Art, omfang, formål, sammenheng
Kilder og mottagere
Systematisk beskrivelse av behandlingen
Ansvarsforhold
Informasjonssikkerhet
Personvernprinsipper
Rettslig grunnlag
Nødvendighet og proporsjonalitet
Rettigheter
Friheter
Plikter for alle
Tilleggsplikter for DPIA
Sammenstilling og presentasjon av funn
Ledelsens validering av DPIA
Hensynet til interessenter
Gjennomgang, beslutning og godkjenning
Åpenhet
Forutsigbarhet
Risiko for de registrertes rettigheter og friheter
Medbestemmelse
Tillit
Datatilsynet

The Norwegian Data Protection Authority highlights the following 4 steps in an overall process for DPIA

1. Describe the processing of Personal Data
2. Assess compliance with the privacy principles
3. Assess the risk to the data subjects' rights and freedoms
4. Authorization

Remember this is an **iterative process!**

Always performed: Steps 1 and 2 apply to all processing of personal data

Data privacy assements

Who should handle this?

- Have you ever listened to someone having statements like
  - The privacy assessments done by the lawyers is an obstacle to the progress of Product Development
- Good data privacy requires knowledge of the relevant domain as well as functional and technical product development expertise
- It other words, the Product Team should be responsible for
  - A systematic description of the processing operations of the personal data for specific purposes
  - Assess compliance with the privacy principles
  - Do risk assessments when needed
- In some cases the Product Teams need to involve lawyers

  The product team needs to know when; typical cases
  - What is the legal basis for processing and who is the controller?
  - Is it any special laws that sets requirements for our product? What are these requirements?
  - Is the transfer of personal data to this 3rd country legal?

Who should be lead in the product team in terms of privacy?

- **Product/Service Owner**
- Project/team leader
- Technical manager / architect
- Functionally responsible / service designer

Additional representatives if necessary
Legal clarifications

Privacy-by-design as part of the product development should be a part of an "agile journey", but unfortunately it is often not default as of today!

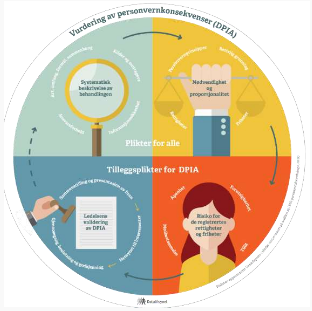
How to implement privacy-by design in a product

- Identify a first draft of the purposes early
    - Refine the purposes gradually according to the product's roadmap
- Focus on compliance with privacy principles as an inherent part of the Product Development
- For each purpose when ready: Identify measures for each principle as part of the team's specification process - assess risk when relevant
- The measures should be elaborated at an appropriate level as part of the product’s epics and user stories

Data Privacy and Product Development Process

Analysis of needs – Business case › During product development › In front of deployment of new release

- Privacy assessments as an inherent part of agile product development
  - Initial assessments early
  - Then gradual elaborate according to the product's roadmap
  - Relevant technical measures are gradually identified, implemented and documented
- Only updating formal DPIA for releases that introduce new processing of personal data or new measures
  - Continuously update the privacy documentation as part of the product documentation
  - In the case of frequent releases, most of the releases will not require updating of the privacy documentation


Vurdering av personvernkonsekvenser (DPIA)
Art, omfang, formål, sammenheng
Kilder og mottagere
Systematisk beskrivelse av behandlingen
Ansvarsforhold
Informasjonssikkerhet
Personvernprinsipper
Rettslig grunnlag
Nødvendighet og proporsjonalitet
Rettigheter
Friheter
Plikter for alle
Tilleggsplikter for DPIA
Sammenstilling og presentasjon av funn
Ledelsens validering av DPIA
Hensyner til interessenter
Gjennomgang, beslutning og godkjenning
Åpenhet
Forutsigbarhet
Risiko for de registrertes rettigheter og friheter
Medbestemmelse
Tillit
Datatilsynet

Questions?

Thank you for inviting me!

Knut Soelberg
Aboveit
email: Knut.Soelberg@aboveit.no
Phone: +47 915 833 84