ComplyCloud

GDPR in software development

www.complycloud.com

Jakob Krabbe Sørensen

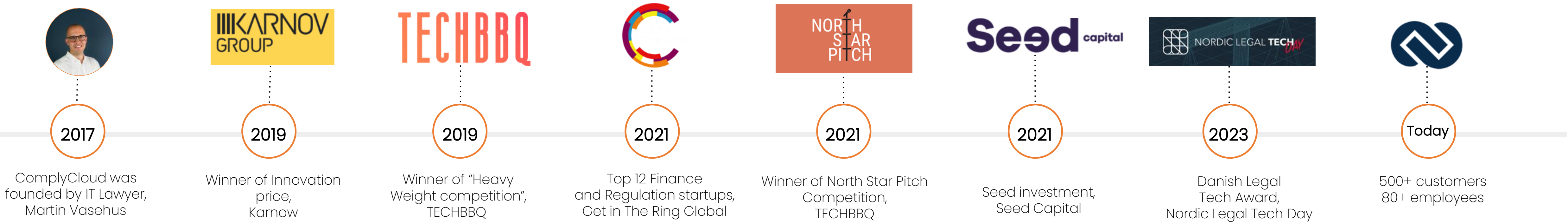
- Attorney
- Head of Legal Product at ComplyCloud
- Seven years of experience with cyber security, AI regulation and GDPR

ComplyCloud

www.complycloud.com

Who we are

We're a bunch of passionate compliance specialists, tech professionals and lawyers making it easy and accessible for any organisation to achieve and maintain data protection and IT security compliance.



2017
ComplyCloud was founded by IT Lawyer, Martin Vasehus

2019
Winner of Innovation price, Karnow

2019
Winner of "Heavy Weight competition", TECHBBQ

2021
Top 12 Finance and Regulation startups, Get in The Ring Global

2021
Winner of North Star Pitch Competition, TECHBBQ

2021
Seed investment, Seed Capital

2023
Danish Legal Tech Award, Nordic Legal Tech Day

Today
500+ customers
80+ employees

Compliance challenges that we solve

It’s complex to get the full picture

and to understand the compliance journey

It’s hard to comply with the requirements

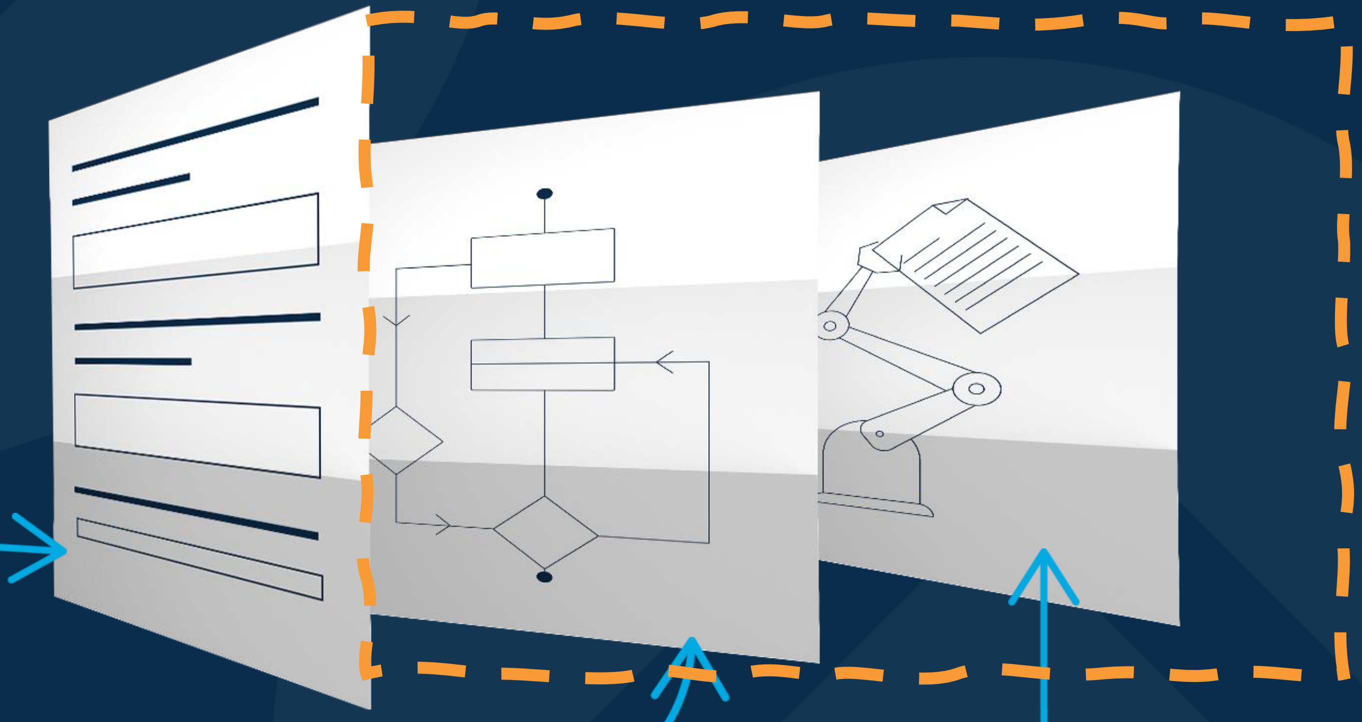
as they are difficult to understand and hard to document

It's a never-ending story

to follow legal development and maintain documentation and compliance tasks

☒ Lack of expertise and time

Compliance automation through software



1. Facts

The user provides the relevant facts needed.

2. Legal analytics

The software analyzes the facts' interplay with the rules.

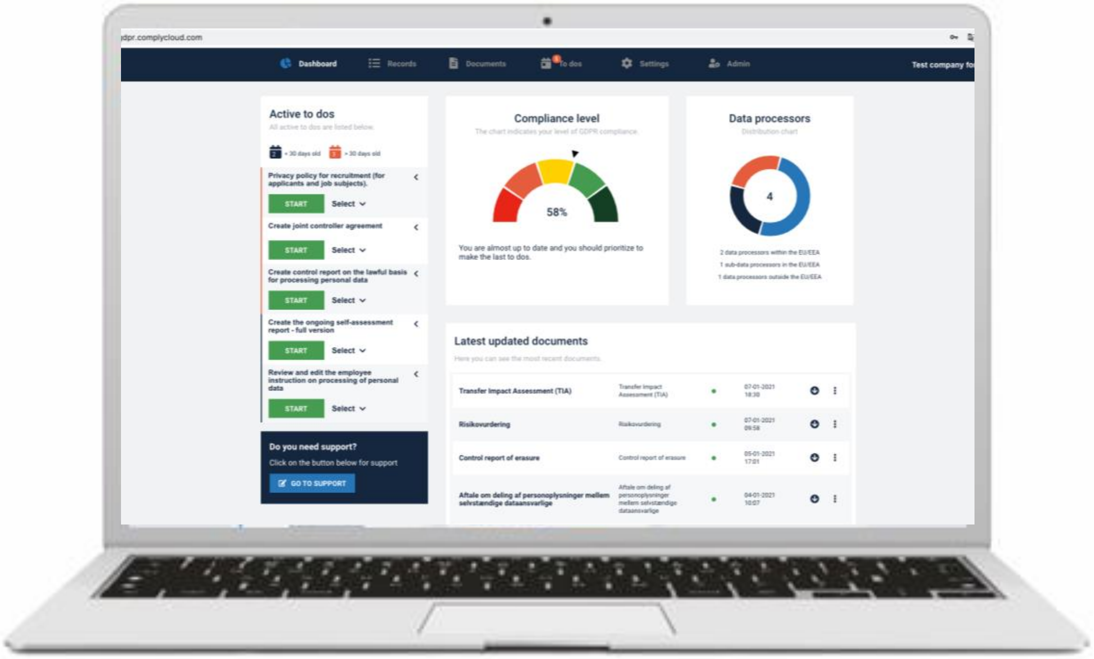
3. Algorithmic output

The software produces and provides all mandatory documentation and advises based on our deep business logic.

ComplyCloud

Agenda

1. When must you think GDPR?
2. Minimization and lawfullness
3. Data security
4. Data transfers
5. Rights of the users
6. Privacy by default
7. AI Act



Active to dos

All active to dos are listed below

< 30 days old > 30 days old

Privacy policy for recruitment (for applicants and job subjects).

Create joint controller agreement

Create control report on the lawful basis for processing personal data

Create the ongoing self-assessment report - full version

Review and edit the employee instruction on processing of personal data

Do you need support?

Click on the button below for support

Compliance level

The chart indicates your level of GDPR compliance.

You are almost up to date and you should prioritize to make the last to dos.

Data processors

Distribution chart

2 data processors within the EU/EEA

1 sub-data processors in the EU/EEA

1 data processors outside the EU/EEA

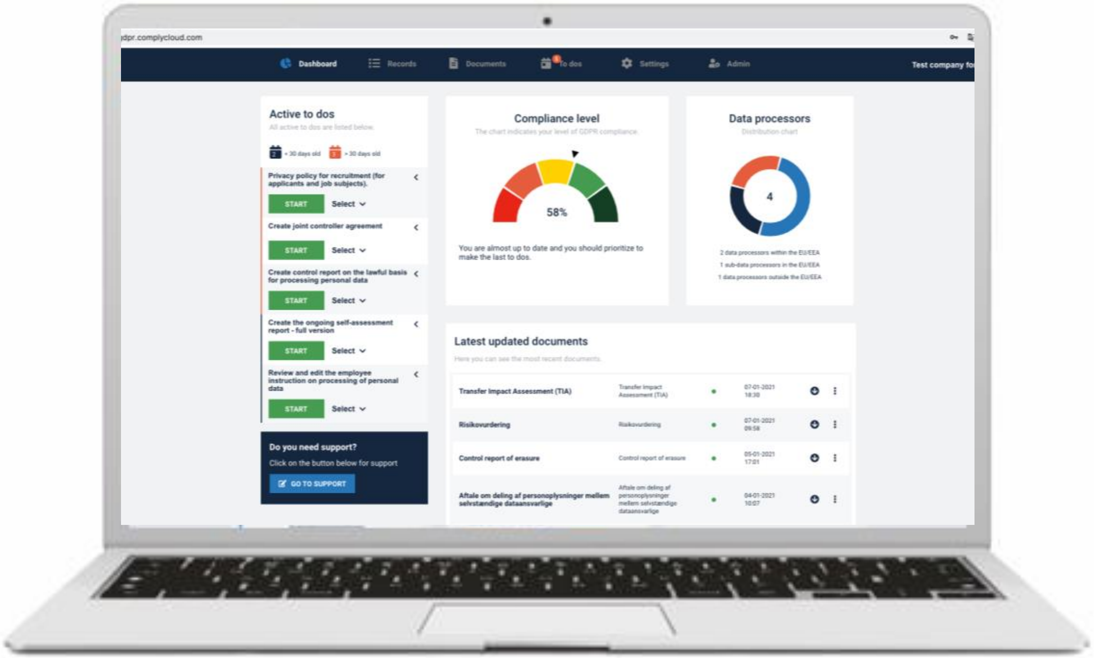
Latest updated documents

Here you can see the most recent documents.

Transfer Impact Assessment (TIA)	Transfer Impact Assessment (TIA)	●	07-01-2021 18:30
Risikovurdering	Risikovurdering	●	07-01-2021 09:58
Control report of erasure	Control report of erasure	●	05-01-2021 17:01
Aftale om deling af personoplysninger mellem selvstændige dataansvarlige	Aftale om deling af personoplysninger mellem selvstændige dataansvarlige	●	04-01-2021 10:07

Agenda

1. When must you think GDPR?
2. Minimization and lawfullness
3. Data security
4. Data transfers
5. Rights of the users
6. Privacy by default
7. AI Act



Active to dos

All active to dos are listed below.

- Privacy policy for recruitment (for applicants and job subjects).
- Create joint controller agreement
- Create control report on the lawful basis for processing personal data
- Create the ongoing self-assessment report - full version
- Review and edit the employee instruction on processing of personal data

Do you need support?

Click on the button below for support

Compliance level

The chart indicates your level of GDPR compliance.

You are almost up to date and you should prioritize to make the last to dos.

Data processors

Distribution chart

2 data processors within the EU/EEA

1 sub-data processors in the EU/EEA

1 data processors outside the EU/EEA

Latest updated documents

Here you can see the most recent documents.

Transfer Impact Assessment (TIA)	Transfer Impact Assessment (TIA)	●	07-01-2021 18:30
Risikovurdering	Risikovurdering	●	07-01-2021 09:58
Control report of erasure	Control report of erasure	●	05-01-2021 17:01
Aftale om deling af personoplysninger mellem selvstændige dataansvarlige	Aftale om deling af personoplysninger mellem selvstændige dataansvarlige	●	04-01-2021 10:07

When does GDPR apply?

The GDPR **applies to the processing of personal data** carried out by an organization in the EU/EEA or targeted at EU citizens.

Processing

- "Processing" in practice includes all forms of handling of personal data
- Examples of acts covered by "processing":

Registration

Editing

Emails

Analytics

Disclosure

Searching

Covered processing: All electronic processing + Non-electronic processing in registers

Personal data

- Personal data is defined as "Any information relating to an identified or identifiable natural person" (article 4(1))

because of GDPR i cant say name,
so gentleman with syphilis come in
ORTOPEDICKÁ AMBULANCIA
INTERNÁ A GERIATRICKÁ AMBULANCIA

Privacy by design

Article

25(1)

Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of users.

Lærerstandens
Brandforsikring

"The Danish Data Protection Agency established that – in addition to the use of all the recognized test forms – already from the development of the system's business processes and design, it is the responsibility of the data controller to ensure an effective implementation of the data protection principles by building this into the system, so that it provides the necessary guarantees in the processing of personal data and meets the requirements of the General Data Protection Regulation (GDPR)."

(my translation)

Privacy by design

Article

25(1)

Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, **implement appropriate technical and organisational measures**, such as pseudonymisation, which are designed to implement **data protection principles**, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing **in order to meet the requirements of this Regulation** and protect the rights of users.

An IT-system must support any requirement in GDPR already from the development phase

So what does this mean for your project?

- Personal data is everywhere, also in your system.
- In certain cases, data can be anonymized so that it's not considered personal data.
- The principle of privacy by design means that your system must be built to comply with the rules.

Agenda

1 When must you think GDPR?

2 Minimization and lawfullness

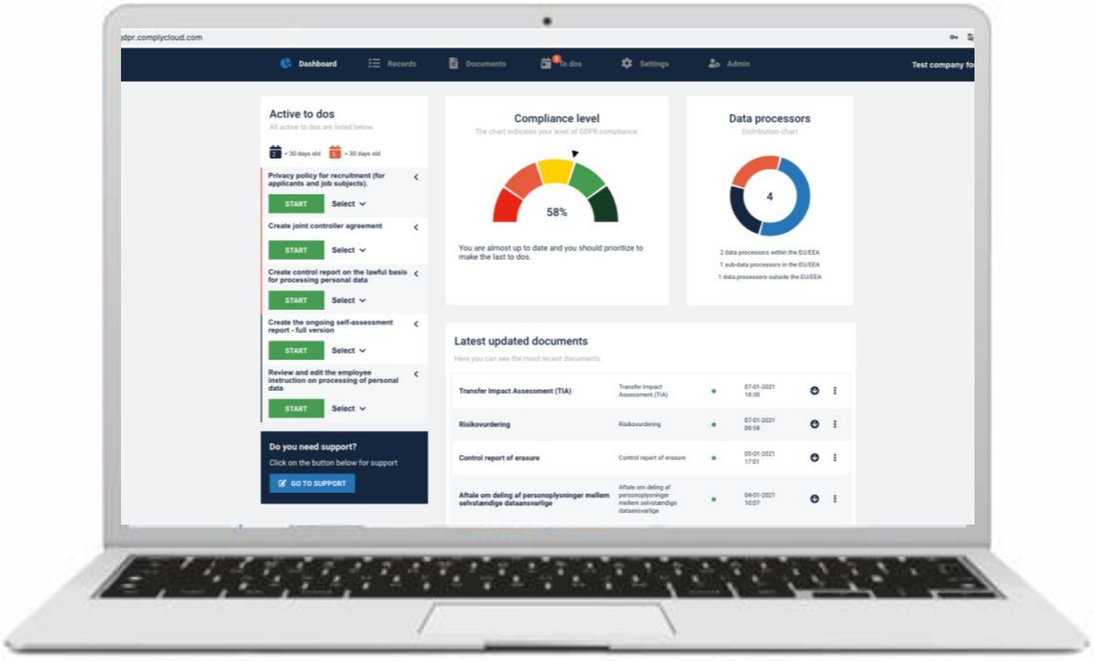
3 Data security

4 Data transfers

5 Rights of the users

6 Privacy by default

7 AI Act



Active to dos

All active to dos are listed below.

Privacy policy for recruitment (for applicants and job subjects).

Create joint controller agreement

Create control report on the lawful basis for processing personal data

Create the ongoing self-assessment report - full version

Review and edit the employee instruction on processing of personal data

Do you need support?

Click on the button below for support

Compliance level

The chart indicates your level of GDPR compliance.

You are almost up to date and you should prioritize to make the last to dos.

Data processors

Distribution chart

2 data processors within the EU/EEA

1 sub-data processors in the EU/EEA

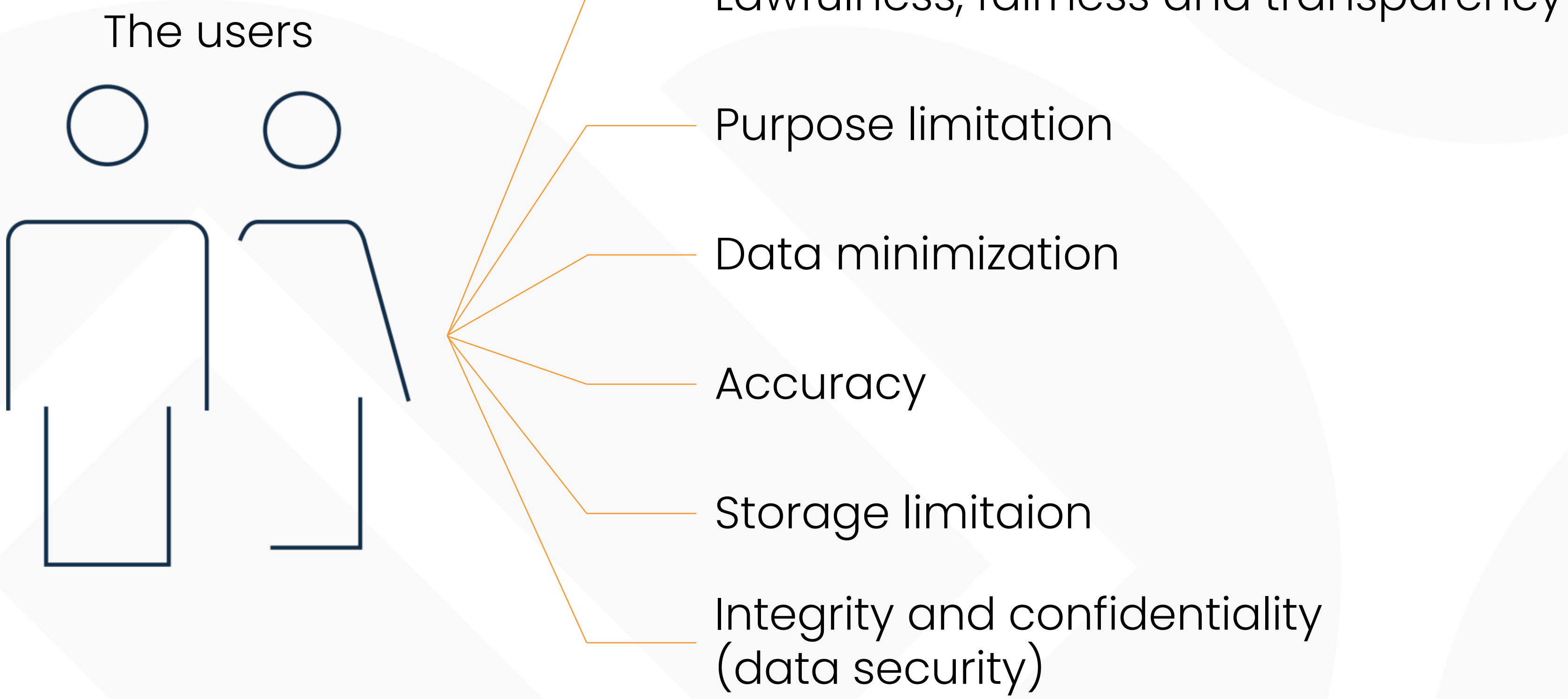
1 data processors outside the EU/EEA

Latest updated documents

Here you can see the most recent documents.

Transfer Impact Assessment (TIA)	Transfer Impact Assessment (TIA)	●	07-01-2021 18:30
Risikovurdering	Risikovurdering	●	07-01-2021 09:58
Control report of erasure	Control report of erasure	●	05-01-2021 17:01
Aftale om deling af personoplysninger mellem selvstændige dataansvarlige	Aftale om deling af personoplysninger mellem selvstændige dataansvarlige	●	04-01-2021 10:07

The basic principles of GDPR



The users

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitaion
- Integrity and confidentiality (data security)

Purpose Limitation

Purpose = Your good reason for processing personal data

To define the purpose:

- For each processing activity, ask: **Why** are we doing this?
- The purpose of the processing shall be **specific, explicit** and **legitimate.**

Data minimization

Personal information collected must be adequate, relevant and **limited to what is necessary** to the purposes for which they are processed.

Lawfullness

Any processing activity must have a **legal basis**.

Legal basis for processing personal data

Article
6(1)

Lawful processing can generally take place on the following basis (GDPR, Article 6(1)):

a. Consent of the user

b. Necessary for the performance of a contract to which the user is a party

c. Necessary to comply with a legal obligation

d. Necessary to protect vital interests of a natural person

e. Necessary to perform a service in the public interest

f. Necessary to pursue other legitimate interests, unless fundamental rights or freedoms prevail

Legal basis for processing personal data

Article
6(1)

Lawful processing can generally take place on the following basis (GDPR, Article 6(1)):

a. Consent of the user

b. Necessary for the performance of a contract to which the user is a party

c. Necessary to comply with a legal obligation

d. Necessary to protect vital interests of a natural person

e. Necessary to perform a service in the public interest

f. Necessary to pursue other legitimate interests, unless the data subject's interests prevail

Legal basis for processing personal data

Article
6(1)

Lawful processing can generally take place on the following basis (GDPR, Article 6(1)):

a. Consent of the user

b. Necessary for the performance of a contract to which the user is a party

c. Necessary to comply with a legal obligation

d. Necessary to protect vital interests of a natural person

e. Necessary to perform a service in the public interest

f. Necessary to pursue other legitimate interests, unless fundamental rights or freedoms prevail

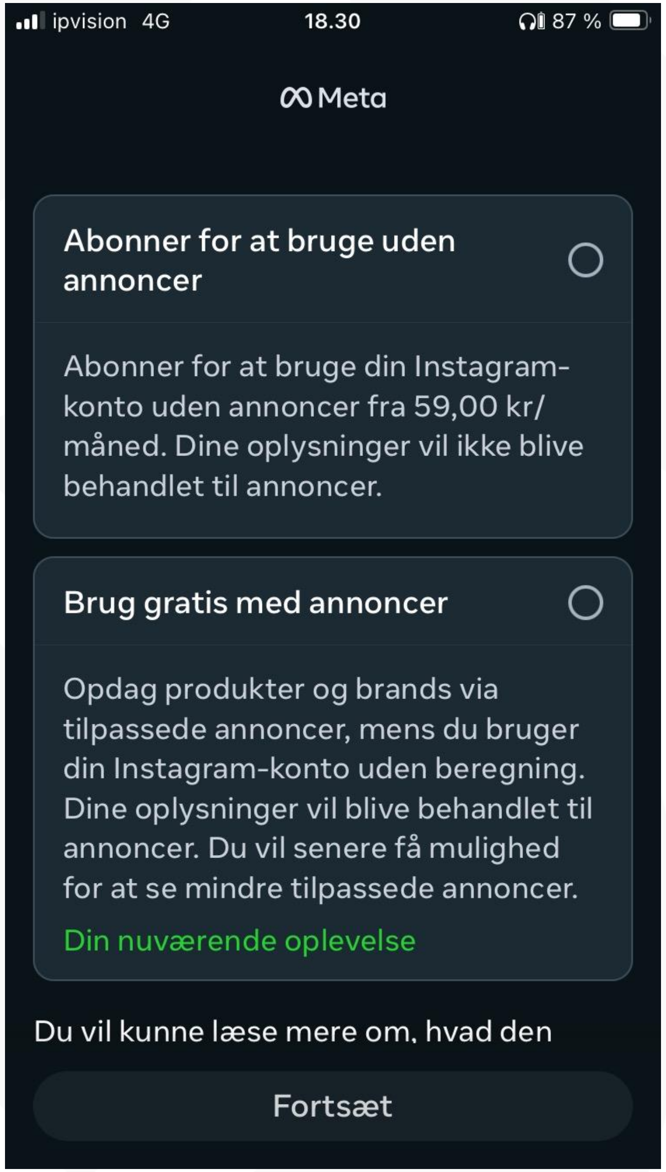
In addition, national law may create other legal basis, e.g. section 12 of the Danish Data Protection Act on employment conditions.

Avoid consent if possible by paying attention to the alternatives

- If you have to process in order to enter into or comply with a contract with the user.
- If you are required to do so by law.
- If necessary to pursue a legitimate interest, and there is no particular reason to believe that the user should want to avoid processing.

A case example: The public race

How are you going to make money on this?



Abonner for at bruge uden annoncer ○

Abonner for at bruge din Instagram-konto uden annoncer fra 59,00 kr/måned. Dine oplysninger vil ikke blive behandlet til annoncer.

Brug gratis med annoncer ○

Opdag produkter og brands via tilpassede annoncer, mens du bruger din Instagram-konto uden beregning. Dine oplysninger vil blive behandlet til annoncer. Du vil senere få mulighed for at se mindre tilpassede annoncer.

Din nuværende oplevelse

Du vil kunne læse mere om, hvad den

Fortsæt

So what does this mean for your project?

- Don’t use real personal data as test data. Use fake data or anonymized data.
- Always consider if consent is actually necessary.

Agenda

1 When must you think GDPR?

2 Minimization and lawfullness

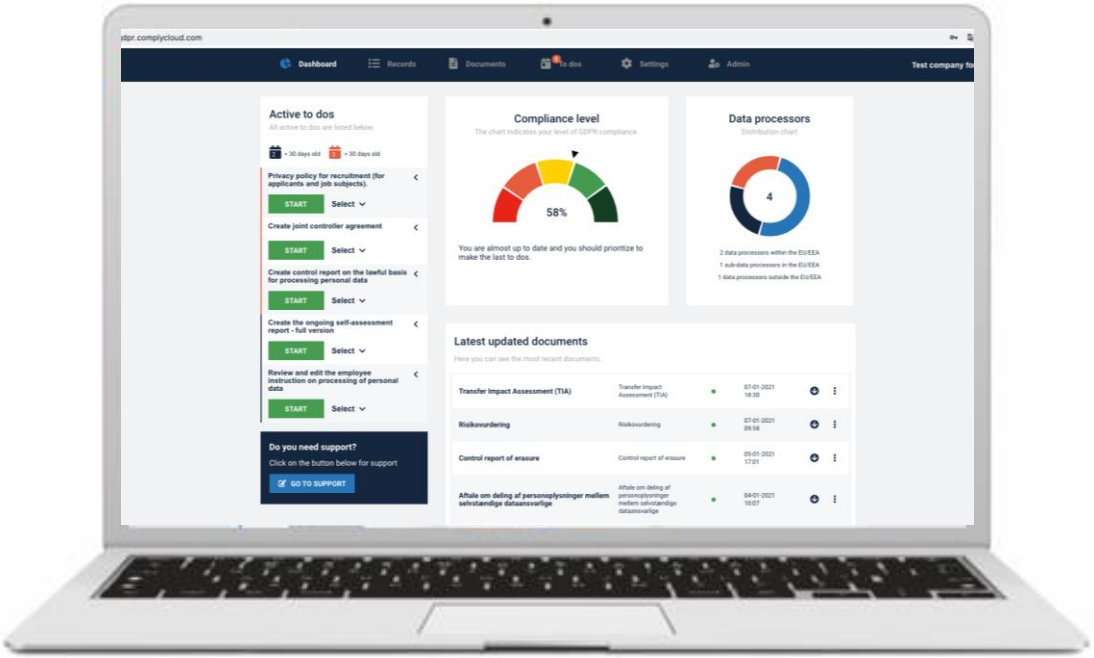
3 Data security

4 Data transfers

5 Rights of the users

6 Privacy by default

7 AI Act



Active to dos

All active to dos are listed below

< 30 days old · > 30 days old

Privacy policy for recruitment (for applicants and job subjects).

Create joint controller agreement

Create control report on the lawful basis for processing personal data

Create the ongoing self-assessment report - full version

Review and edit the employee instruction on processing of personal data

Do you need support?

Click on the button below for support

Compliance level

The chart indicates your level of GDPR compliance

You are almost up to date and you should prioritize to make the last to dos.

Data processors

Distribution chart

2 data processors within the EU/EEA

1 sub-data processors in the EU/EEA

1 data processors outside the EU/EEA

Latest updated documents

Here you can see the most recent documents.

Transfer Impact Assessment (TIA)	Transfer Impact Assessment (TIA)	●	07-01-2021 18:30
Risikovurdering	Risikovurdering	●	07-01-2021 09:58
Control report of erasure	Control report of erasure	●	05-01-2021 17:01
Aftale om deling af personoplysninger mellem selvstændige dataansvarlige	Aftale om deling af personoplysninger mellem selvstændige dataansvarlige	●	04-01-2021 10:07

Data security

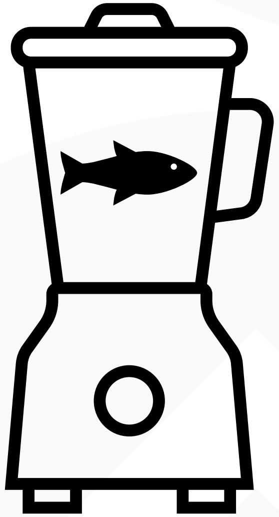
If you process personal data, you must ensure an **protect it** by implementing **security meassures** proportionally to the risks which mitigates the various **threats** that could undermine the users privacy.

Data security

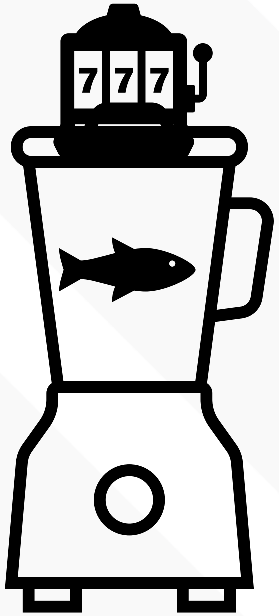
If you process personal data, you must ensure an protect it by implementing security meassures **proportionally to the risks** which mitigates the various threats that could undermine the users privacy.

Risk = Likelihood x Consequence

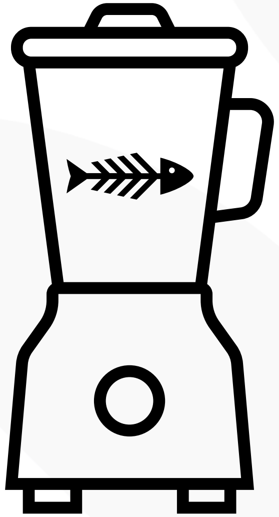
Threat under consideration



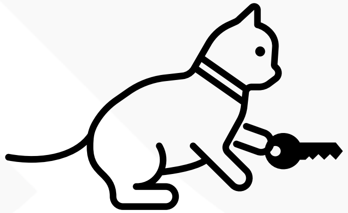
Likelihood that it becomes a reality



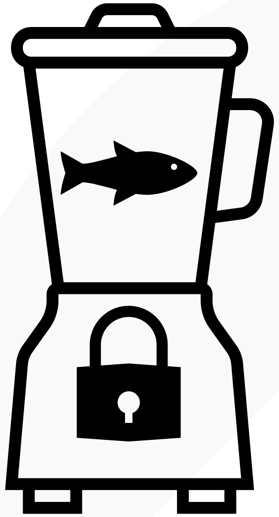
Consequences for the users



The risidual risk which must be acceptable

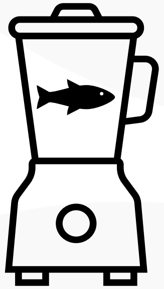


The level of security that is appropriate



Threats

- **Human error** cannot be avoided. No matter how good we are at creating the framework for the correct processing of information, mistakes can always happen.
- **Cyberattacks** are becoming more and more frequent, malevolent actors can try infiltrate your systems or sabotage them in other ways.
- **Phishing attacks** will try to manipulate the organization's employees into giving malevolent actors access to information, for example, by sending emails from fake addresses.
- **Irresponsible employees** may break laws and internal policies to pursue their own goals.
- **Technical errors** in our IT systems can never be ruled out. Neither hardware nor software is ever infallible.
- **"Acts of God"** - As ordinary mortals, there will always be events beyond our control. Fires and extreme weather are rarely attributable to a human actor.



What does the threats threaten?

- The objectives of data security

- **Confidentiality**

  - Is it a problem for the user if unauthorized persons can see the personal data?

- **Availability**

  - Is it a problem for the user if the personal data disappears?

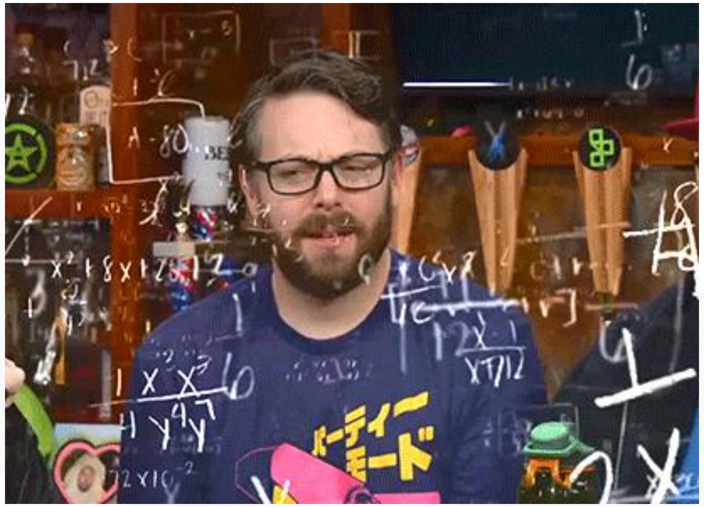
- **Integrity**

  - Is it a problem for the user if the personal data is not correct or up to date?

Security meassures = Technical, Organizational and Physical measures to safeguard the personal data against unintended processing

- **Technical security measures** will typically concern how your organization's computers, **software**, and networks are **configured**.
- **Organizational security measures** will typically concern your internal **"governance" in the organization**.
- **Physical security measures** will typically be about how your **organization's physical premises and archives are designed**.

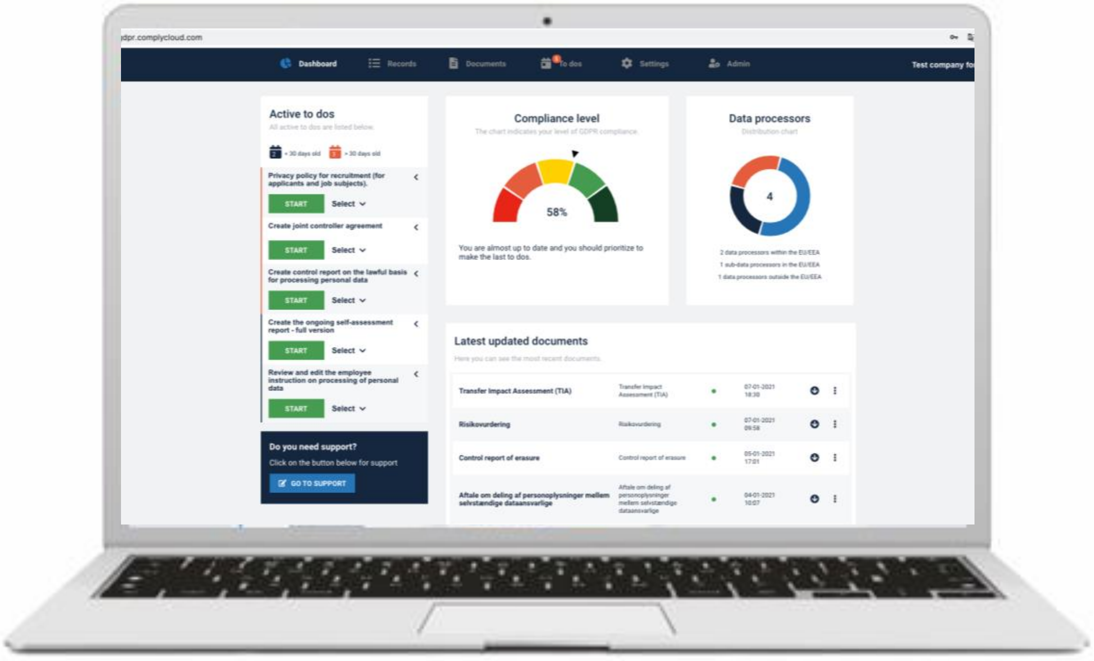
So what does this mean for your project?



- Consider the risks stemming from processing personal data in your system.
- Protect it proportionately to the identified risks.
- Is it your responsibility if people publish high risk information about themselves through your system?

Agenda

1. When must you think GDPR?
2. Minimization and lawfullness
3. Data security
4. **Data transfers**
5. Rights of the users
6. Privacy by default
7. AI Act



Active to dos

All active to dos are listed below.

• 30 days old • 30 days old

Privacy policy for recruitment (for applicants and job subjects).

Create joint controller agreement

Create control report on the lawful basis for processing personal data

Create the ongoing self-assessment report - full version

Review and edit the employee instruction on processing of personal data

Do you need support?

Click on the button below for support

Compliance level

The chart indicates your level of GDPR compliance.

You are almost up to date and you should prioritize to make the last to dos.

Data processors

Distribution chart

2 data processors within the EU/EEA

1 sub-data processors in the EU/EEA

1 data processors outside the EU/EEA

Latest updated documents

Here you can see the most recent documents.

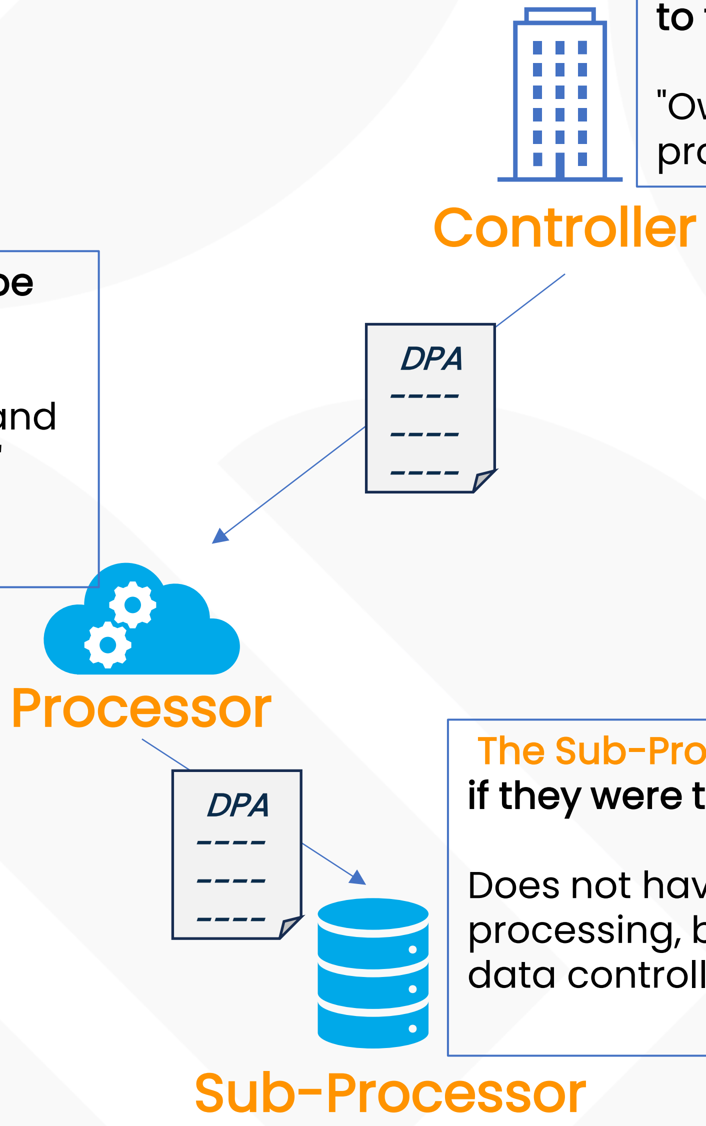
Transfer Impact Assessment (TIA)	Transfer Impact Assessment (TIA)	●	07-01-2021 18:30
Risikovurdering	Risikovurdering	●	07-01-2021 09:58
Control report of erasure	Control report of erasure	●	05-01-2021 17:01
Aftale om deling af personoplysninger mellem selvstændige dataansvarlige	Aftale om deling af personoplysninger mellem selvstændige dataansvarlige	●	04-01-2021 10:07

New IT system or hosting supplier = new transfer

- When you use an IT system or hosting provider, it will mean transfer of personal data, unless
  - You host all personal data on your own servers
  - (Use of the IT system does not involve the processing of personal data)
- In those cases, there will be a number of things you need to consider:
  - Data processing agreement
  - Third countries (data outside of EU)

The controller determines what happens to the information.

"Owns“ the purpose and legal basis for processing.



The processor is told what is to be done by the controller.

Does not have its own purpose and basis for processing, but “´lends" them from the controllers.

The Sub-Processor relates to 1st degree processors as if they were the controller.

Does not have its own purpose and basis for processing, but "borrows" the basis from the original data controller.

So what does this mean for your project?

- Probably nothing.
- But in theory, you should have a data processing agreement with for example your hosting supplier.

ComplyCloud

Agenda

1 When must you think GDPR?

2 Minimization and lawfullness

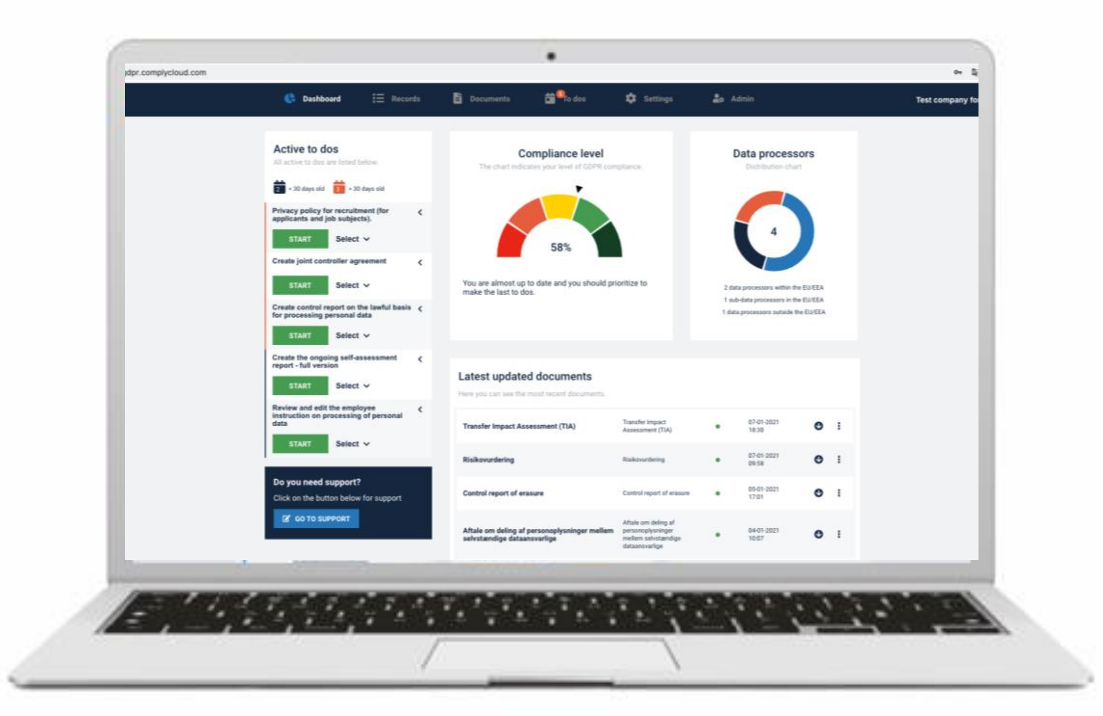
3 Data security

4 Data transfers

5 **Rights of the users**

6 Privacy by default

7 AI Act



Active to dos

All active to dos are listed below.

< 30 days old · > 30 days old

- Privacy policy for recruitment (for applicants and job subjects).
- Create joint controller agreement
- Create control report on the lawful basis for processing personal data
- Create the ongoing self-assessment report - full version
- Review and edit the employee instruction on processing of personal data

Compliance level

The chart indicates your level of GDPR compliance.

You are almost up to date and you should prioritize to make the last to dos.

Data processors

Distribution chart

2 data processors within the EU/EEA
1 sub-data processors in the EU/EEA
1 data processors outside the EU/EEA

Latest updated documents

Here you can see the most recent documents.

Transfer Impact Assessment (TIA)	Transfer Impact Assessment (TIA)	●	07-01-2021 18:30
Risikovurdering	Risikovurdering	●	07-01-2021 09:58
Control report of erasure	Control report of erasure	●	05-01-2021 17:01
Aftale om deling af personoplysninger mellem selvstændige dataansvarlige	Aftale om deling af personoplysninger mellem selvstændige dataansvarlige	●	04-01-2021 10:07

Do you need support?

Click on the button below for support

The users' rights

- The user has a number of rights, which vice versa are your obligations.
- The most relevant are probably the right to information, the right to erasure and the right to access.

Right to erasure

- The user has the right to get personal data erased if:

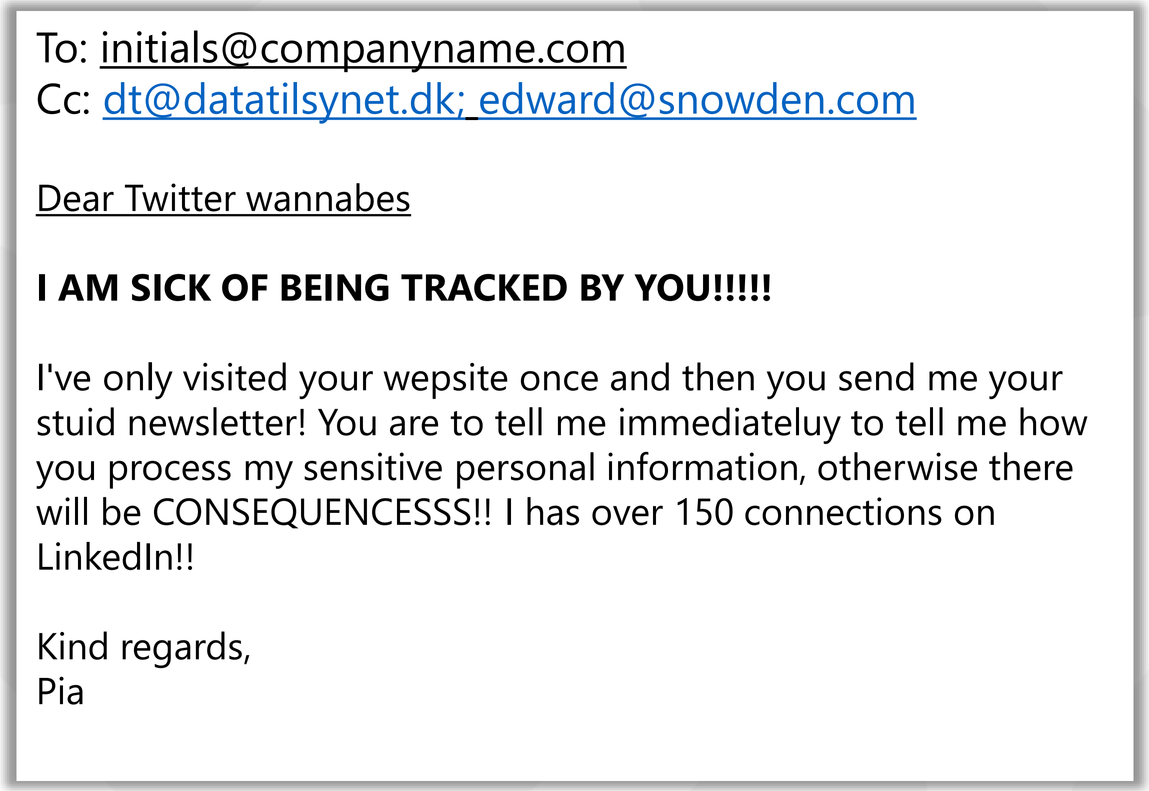
    a. It’s no longer necessary for you to keep it.
    b. The user asks for it under certain conditions.

Right to access

- The user has the right to request access from you.

- This means that you need to
  1. let them know if you are processing personal data about them;
  2. provide the user with a range of information, including, inter alia:
     a. what categories of personal data you process about them;
     b. for what purposes you process the personal data;
     c. to whom you disclosed it and where you obtained it from (if applicable); and

  3. provide a copy of the personal data



To: initials@companyname.com
Cc: dt@datatilsynet.dk; edward@snowden.com

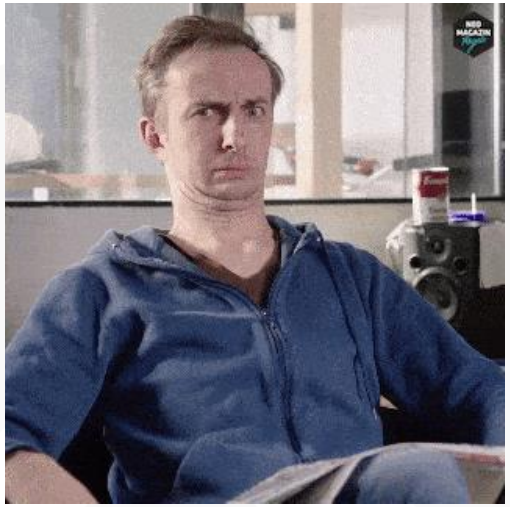
Dear Twitter wannabes

I AM SICK OF BEING TRACKED BY YOU!!!!!

I've only visited your wepsite once and then you send me your stuid newsletter! You are to tell me immediateluy to tell me how you process my sensitive personal information, otherwise there will be CONSEQUENCESSS!! I has over 150 connections on LinkedIn!!

Kind regards,
Pia

So what does this mean for your project?



- It must be possible to erase data and to easy to extract personal data to provide copies to the data subject.

Agenda

1 When must you think GDPR?

2 Minimization and lawfullness

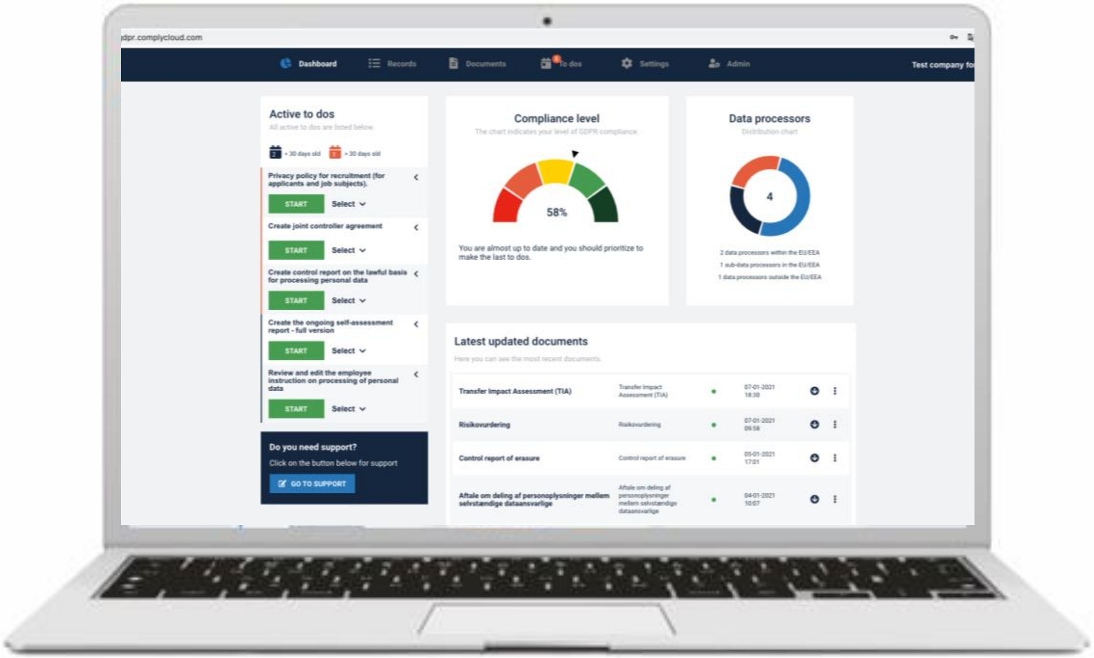
3 Data security

4 Data transfers

5 Rights of the users

6 Privacy by default

7 AI Act



Active to dos

All active to dos are listed below.

< 30 days old · > 30 days old

Privacy policy for recruitment (for applicants and job subjects).

Create joint controller agreement

Create control report on the lawful basis for processing personal data

Create the ongoing self-assessment report - full version

Review and edit the employee instruction on processing of personal data

Do you need support?

Click on the button below for support

Compliance level

The chart indicates your level of GDPR compliance.

You are almost up to date and you should prioritize to make the last to dos.

Data processors

Distribution chart

2 data processors within the EU/EEA

1 sub-data processors in the EU/EEA

1 data processors outside the EU/EEA

Latest updated documents

Here you can see the most recent documents.

Transfer Impact Assessment (TIA)	Transfer Impact Assessment (TIA)	●	07-01-2021 18:30
Risikovurdering	Risikovurdering	●	07-01-2021 09:58
Control report of erasure	Control report of erasure	●	05-01-2021 17:01
Aftale om deling af personoplysninger mellem selvstændige dataansvarlige	Aftale om deling af personoplysninger mellem selvstændige dataansvarlige	●	04-01-2021 10:07

Privacy by default

- **Standard settings** must be the option that entails the **most privacy**.

So what does this mean for your project?

- The standard setting for a profile on a social media must be that a **profile is private**.

Agenda

1 When must you think GDPR?

2 Minimization and lawfullness

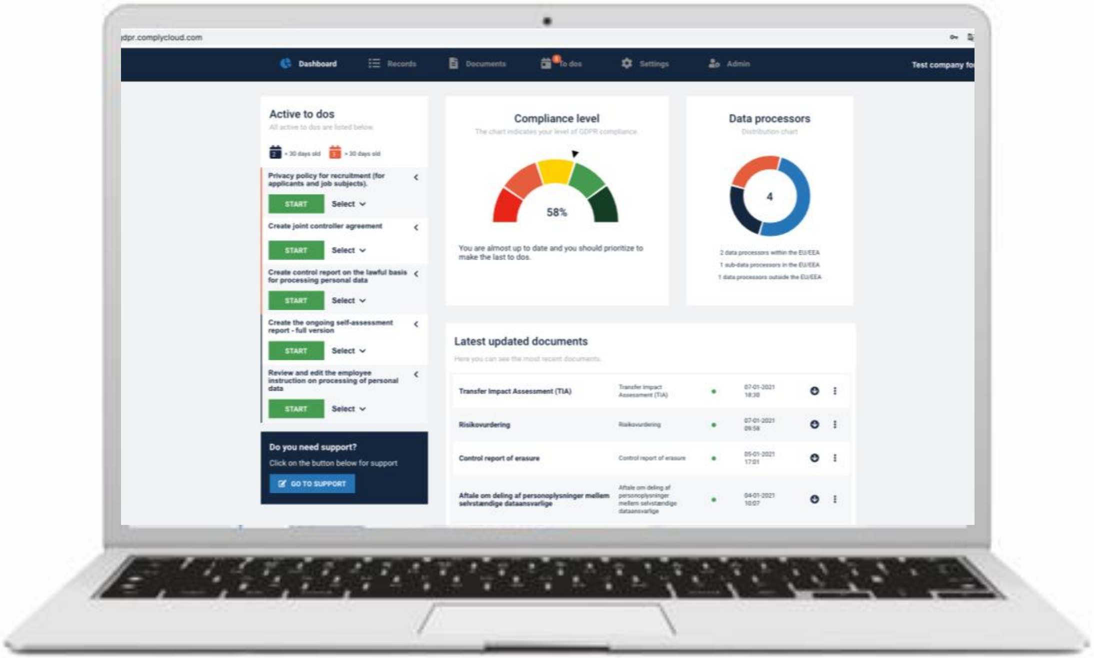
3 Data security

4 Data transfers

5 Rights of the users

6 Privacy by default

7 AI Act



Active to dos

All active to dos are listed below.

Privacy policy for recruitment (for applicants and job subjects).

Create joint controller agreement

Create control report on the lawful basis for processing personal data

Create the ongoing self-assessment report - full version

Review and edit the employee instruction on processing of personal data

Do you need support?

Click on the button below for support

Compliance level

The chart indicates your level of GDPR compliance.

You are almost up to date and you should prioritize to make the last to dos.

Data processors

Distribution chart

2 data processors within the EU/EEA

1 sub-data processors in the EU/EEA

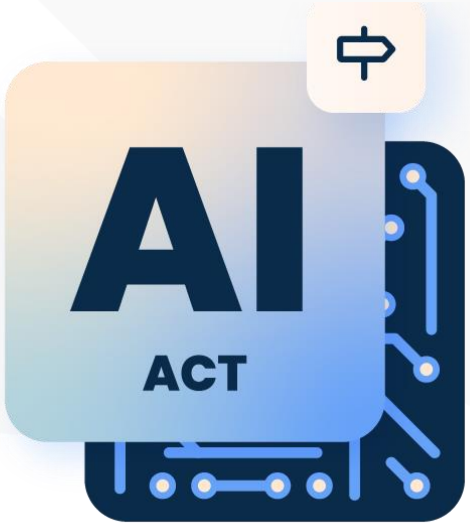
1 data processors outside the EU/EEA

Latest updated documents

Here you can see the most recent documents.

Transfer Impact Assessment (TIA)	Transfer Impact Assessment (TIA)	●	07-01-2021 18:30	
Risikovurdering	Risikovurdering	●	07-01-2021 09:58	
Control report of erasure	Control report of erasure	●	05-01-2021 17:01	
Aftale om deling af personoplysninger mellem selvstændige dataansvarlige	Aftale om deling af personoplysninger mellem selvstændige dataansvarlige	●	04-01-2021 10:07	

What if there’s AI in your IT-system?



Roles within the AI Act

	What they do	Typical examples
Provider	Developing, producing or marketing AI systems under its own name	Tech companies, software developers
Deployer	Using or using an AI system in practice	Companies, public authorities
Importer	Bringing AI systems from third countries into the EU	EU-based distributors
Distributor	Offering or selling AI systems without modifying them	Resellers, Cloud Platforms

Roles within the AI Act

Roll	What they do	Typical examples
Provider	Developing, producing or marketing AI systems under its own name	Tech companies, software developers
Deployer	Using or using an AI system in practice	Companies, public authorities
Importer	Bringing AI systems from third countries into the EU	EU-based distributors
Distributor	Offering or selling AI systems without modifying them	Resellers, Cloud Platforms

Roles within the AI Act

- **Provider**

Definition (Art. 3(3)):
*'provider' means a natural or legal person, public authority, agency or other body that **develops an AI system or a general-purpose AI model** or that **has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark**, whether for payment or free of charge;*

Core responsibilities:

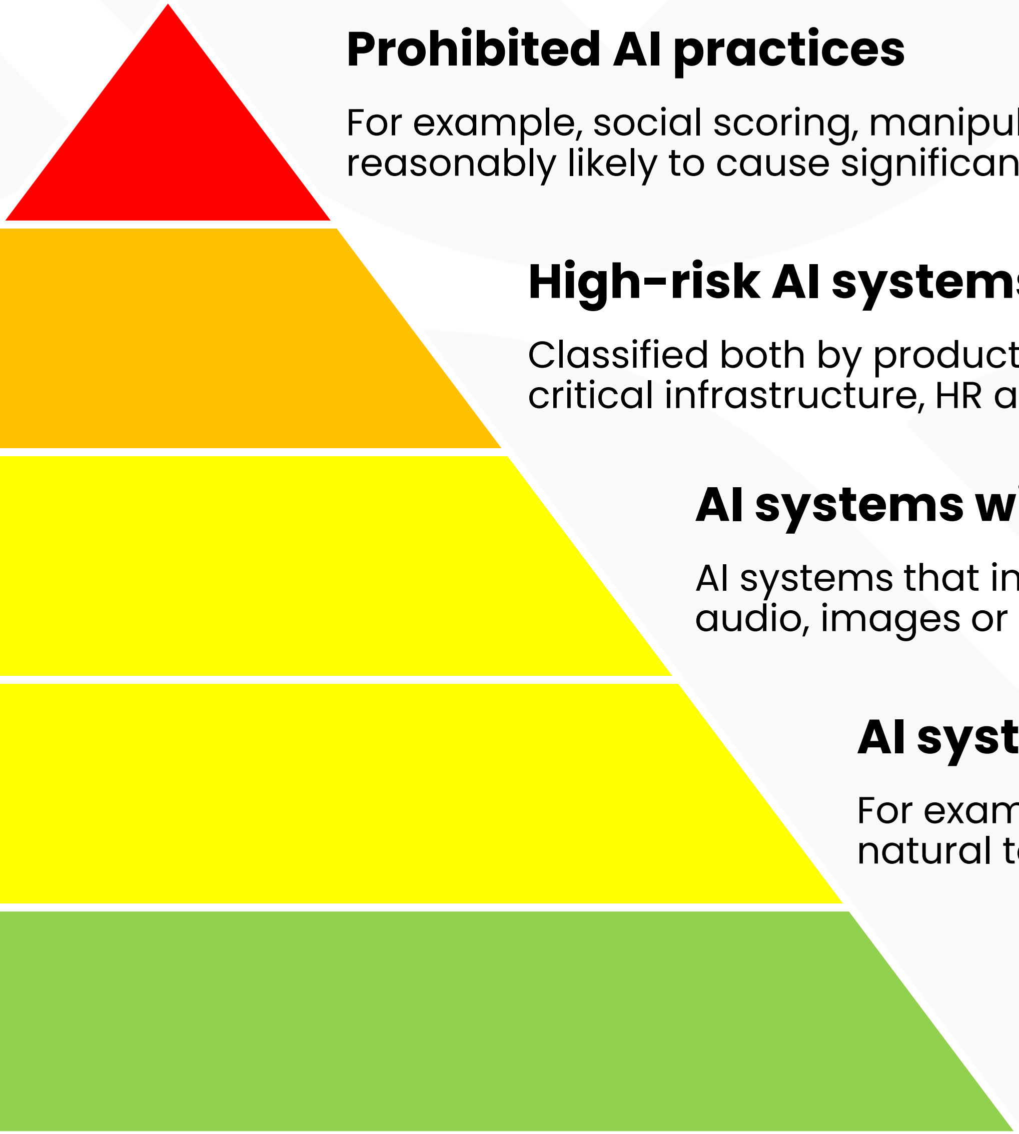
- Development, design and compliance.
- Ensure that the system meets all requirements before it is placed on the market.
- Maintain technical documentation.

The provider

- A provider is the actor who **develops, trains, designs, or commercialize** an AI system under its own name.

- The provider **is the "source" of the system** – the one who puts it into circulation on the market or provides it to other users.

- Providers can be anything from **large tech companies to smaller software developers or startups**.



Prohibited AI practices

For example, social scoring, manipulation, exploitation of vulnerabilities, etc. Note requirements that "cause or are reasonably likely to cause significant harm to that person, another person, or group of persons."

High-risk AI systems

Classified both by product range and specific use of AI. This applies in particular to the use of AI in critical infrastructure, HR and recruitment, as well as access to public and private services.

AI systems with transparency obligations

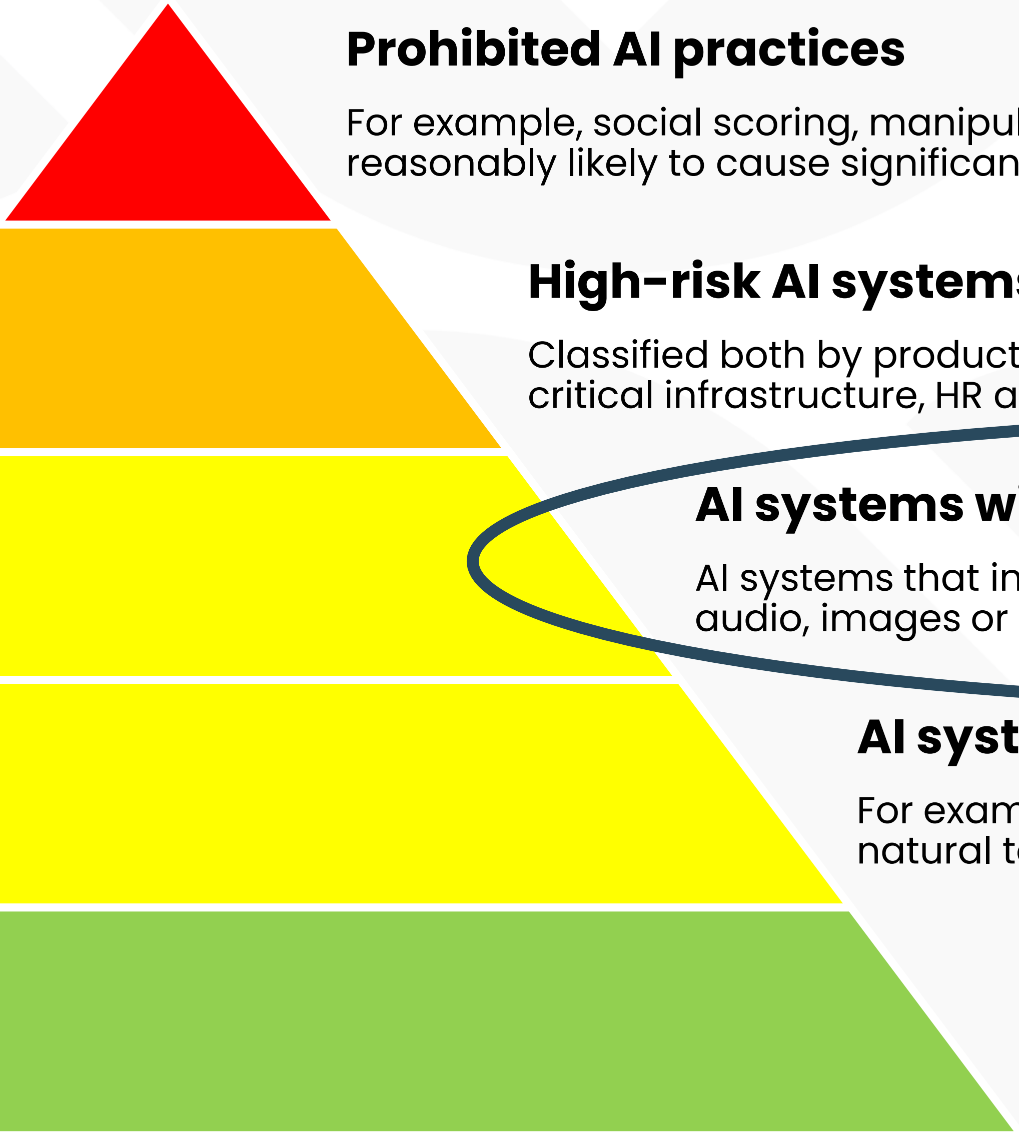
AI systems that interact directly with end-users. These include AI chatbots, AI for generating audio, images or video, and deepfake material.

AI systems and models for general use

For example, ChatGPT, Bard, NVIDIA and Copilot during 'normal use', where it will be natural to have internal procedures that match the risks that GenAI can bring.

AI systems with minimal risk

The residual group, which is not directly regulated by the AI Act, but rather by GDPR and ISMS obligations, among other things.



Prohibited AI practices

For example, social scoring, manipulation, exploitation of vulnerabilities, etc. Note requirements that "cause or are reasonably likely to cause significant harm to that person, another person, or group of persons."

High-risk AI systems

Classified both by product range and specific use of AI. This applies in particular to the use of AI in critical infrastructure, HR and recruitment, as well as access to public and private services.

AI systems with transparency obligations

AI systems that interact directly with end-users. These include AI chatbots, AI for generating audio, images or video, and deepfake material.

AI systems and models for general use

For example, ChatGPT, Bard, NVIDIA and Copilot during 'normal use', where it will be natural to have internal procedures that match the risks that GenAI can bring.

AI systems with minimal risk

The residual group, which is not directly regulated by the AI Act, but rather by GDPR and ISMS obligations, among other things.

Obligations for providers of non-high-risk AI systems

1. Transparency and support for deployers
2. Information and guidance for users
3. Complaint and improvement mechanisms
4. Voluntary standards and best practices (recommended)

1. Transparency and support for deployers

What do you need to ensure?

- The system must have features that allow providers to inform users that they are interacting with AI.
- You must provide clear instructions on how to enable and communicate such transparency features.

2. Information and guidance for users

What do you need to ensure?

- Describe the purpose, features, and any limitations to the user.
- Indicate how results should be interpreted and used responsibly.
- Make it easy to understand when the system uses automated decision logic.

Thank you

ComplyCloud