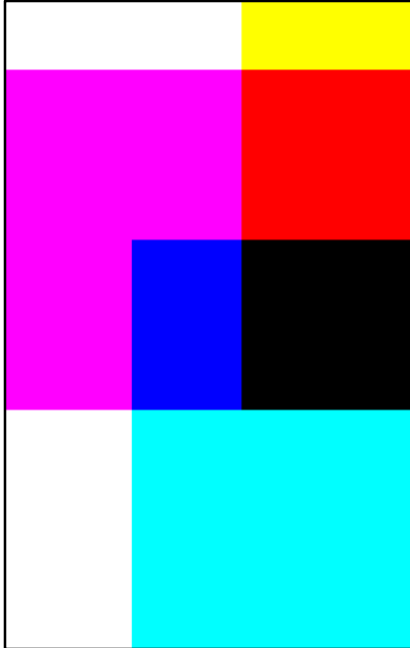




SKW
Schwarz

IT Law & Ethics

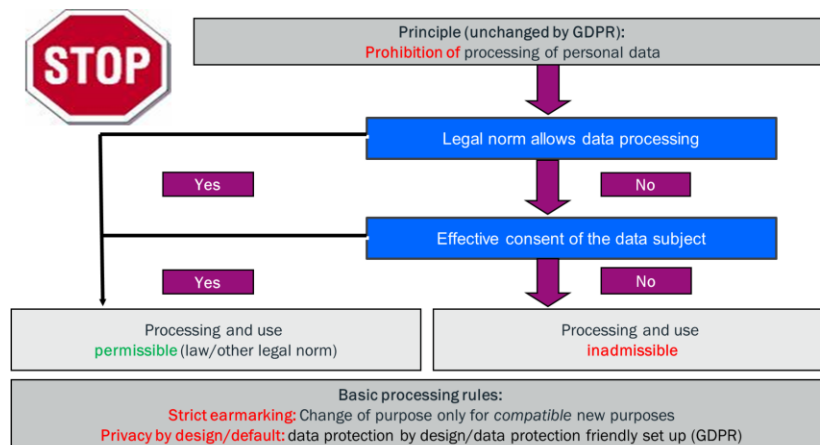
Rosenheim Technical University of Applied Sciences -
SoSe 2023 - 2/3
Dr. Matthias Orthwein, LL.M. (Boston)



GDPR - The principles of processing

Data protection and data security

Data protection principle - What is allowed?



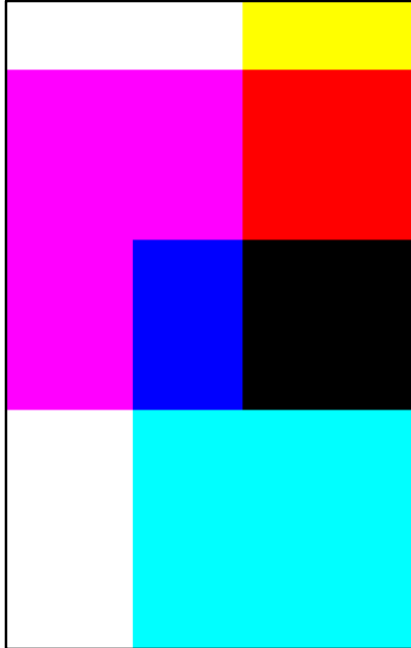
SKW Schwarz

IT Law & Ethics - SoSe 2023

3

Change of purpose is regulated in Art. 6 (4) GDPR

Responsible party must decide between consent and legal basis: If consent ceases to exist or is ineffective, no legal basis can save him "in the alternative"



GDPR - Permitted data processing

Data protection and data security

Prohibition with reservation of permission

Overview: Legal bases of data processing

→ Any data processing is prohibited unless the law allows it.

→ Legal bases of data processing relevant to practice

- Data processing for the **performance of a contract** to which the data subject is a party or for the implementation of pre-contractual measures, Art. 6 (1) lit. b GDPR
Example: Any information for billing
- Data processing is necessary for compliance with a **legal obligation** to which the controller is subject, Art. 6 (1) lit. c GDPR
Example: Storage of data to fulfill obligations under tax law
- Data processing is necessary for the **protection of the legitimate interests of the controller** or a third party, Art. 6 (1) lit. f GDPR
Note: Weighing of interests must be **documented**
- Data processing based on **consent** of the data subject, Art. 6 (1) lit. a GDPR

Legitimate interest may also be direct marketing by the responsible party for itself or third parties

But: with marketing, the advertising law (UWG) must always be observed, which, for example, only allows email advertising without consent to a very limited extent.

Data protection - Consent (1)

Effectiveness requirements for consent

→ **Recognizability**

→ **Reference** to the purpose, nature and scope of any data processing

→ **Voluntary:**

- problematic for employees
- No coupling of contract and consent to data processing that is not necessary for the contract

→ For **sensitive data** (e.g., health data), specifically list the types of data

→ Previous reference to the right of the user to **revoke** consent at any time with effect for the future

→ Separation of consent to **newsletter order/advertising**

→ Regular use of consent

SKW Schwarz

IT Law & Ethics - SoSe 2023

6

Consent is regulated in Article 7 of the GDPR, in addition to other areas of special legislation.

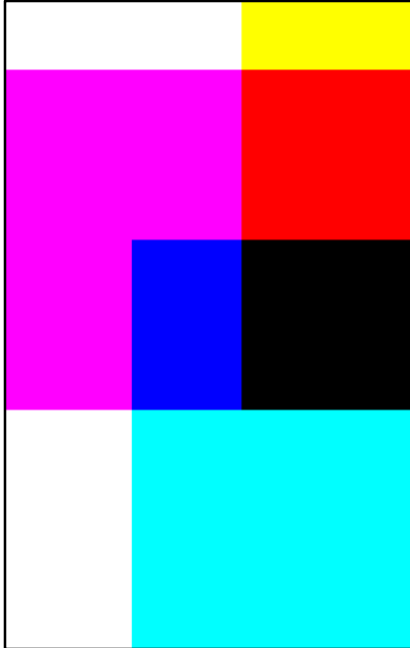
For detailed explanations, see Working Paper 259 of the Art. 29 Group (http://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51030).

Consent retains its validity over several years only if it is also used regularly (AG Hamburg Urt. v. 24.8.2016 - 9C 106/16). At least once in 1.5 years and BGH, 1.2.2018 - III ZR 196/17: permitted two years

Data protection - Consent (2)

Form of consent

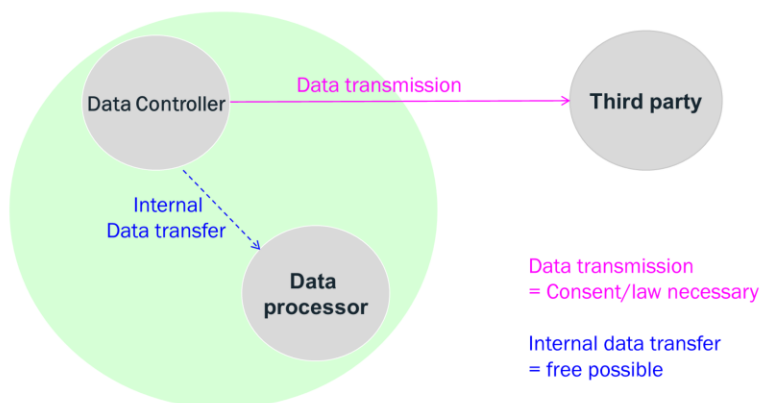
- Consent does **not** have to be in **writing**
- Can also be unambiguous gesture or given verbally
- *But:* only as active **opt-in**, no pre-ticked boxes.
- **Explicit consent** (e.g., written) required for:
 - Processing of sensitive data (e.g. health data)
 - Transfer outside the EU (without other coverage)
 - Automated individual case decisions (profiling)
- Consent of **children** (Germany: under 16) to online services
 - Only with permission of the legal guardian
 - *Problem:* Age verification



GDPR - Data processing by third parties - commissioned data processing

Data protection and data security

data processor (1)



SKW Schwarz

Bechtle Upskilling Program: Cloud Workshop

Was called before DSGVO: Commissioned data processing and commissioned data processing agreement (ADV) (§ 11 BDSG old).

Today: Art. 28 GDPR; there is Brief Paper No. 13 on this from the Data Protection Conference

Liability of the processor:

Direct right of action of the person concerned, Art. 79 para. 2

Claim for compensation for material as well as immaterial damage, with joint and several liability, Art. 82 par. 1

The threat of a fine (Art. 83 Para. 4 (a)) in particular in the case of lack of documentation according to Art. 30 and 33

Defects in TOM according to Art. 32

Violation of formal documentation and contractual obligation Art. 2

Documentation obligation of the processor Art. 30, 32 and 33

Processing on behalf must be documented

Implementation of the TOM

Risk/protection needs analysis

Authorization concept

Implementation of the obligation to report data breaches

data processor (2)

Subject matter and roles of commissioned processing

| Delineation of roles: | | | | | |
|---|---|-------------|-----------|---|--|
| <p>In the case of commissioned processing, the data does not leave the area of responsibility of the responsible party.</p> <p>It therefore does not require the consent of the data subject.</p> <p>Nevertheless, processor has access to data and is therefore jointly responsible.</p> | <table> <tr> <th>Responsible</th><th>Processor</th></tr> <tr> <td> <p>is the one who decides on the purpose, means and type of data processing, even if he delegates the decision on the use of specific technical means and implementation of the TOMs to a service provider (=data processor).</p> </td><td> <p>The purpose of the processing must refer to the instruction of the client and has no processing purposes of its own</p> </td></tr> </table> | Responsible | Processor | <p>is the one who decides on the purpose, means and type of data processing, even if he delegates the decision on the use of specific technical means and implementation of the TOMs to a service provider (=data processor).</p> | <p>The purpose of the processing must refer to the instruction of the client and has no processing purposes of its own</p> |
| Responsible | Processor | | | | |
| <p>is the one who decides on the purpose, means and type of data processing, even if he delegates the decision on the use of specific technical means and implementation of the TOMs to a service provider (=data processor).</p> | <p>The purpose of the processing must refer to the instruction of the client and has no processing purposes of its own</p> | | | | |

SKW Schwarz

Berchle Upskilling Program: Cloud Workshop

Order data processing:

- Service provider must always proceed in accordance with the instructions and under the material responsibility of the client
- Client prescribes the technical and organizational measures for data security, decides on data handling and assesses the organizational measures for data security

Examples of Processors:

- DP-technical work for payroll or financial accounting by computer centers,
- Outsourcing of personal data processing in the context of cloud computing, without the need for content-related data access by the cloud operator,
- Advertising address processing in a letter-shop,
- Processing of customer data by a call center without any significant decision-making scope of its own there,
- Outsourcing of e-mail management or other data services to websites (e.g. support of contact forms or user requests),
- Data capture, data conversion or document scanning,
- Outsourcing of backup security storage and other archiving,
- Data media disposal by service providers,

- Testing or maintenance (e.g. remote maintenance, external support) of automated processes or data processing systems, if access to personal data cannot be ruled out during these activities.
- Centralization of certain "shared services" within a group, such as business trip planning or travel expense reports (in any case, unless a case of joint responsibility under Art. 26 GDPR)

data processor (3)

The data processing contract

→ data processing must be contractually agreed

- can also be in electronic form
- EU standard contractual clauses also possible

→ Minimum content of the contract:

- Binding of the processor to instructions
- Confidentiality obligation for involved employees
- Use of subcontractors
- Ensuring IT security by the processor
- Representation of the TOMs
- Processor's duty to notify in the event of data leakage
- Obligation to delete data after the end of the contract
- Audit right for customer

SKW Schwarz

Bechtle Upskilling Program: Cloud Workshop

Sample AVV: https://www.lida.bayern.de/media/muster_adv.pdf

data processor (4)

Audit obligations in the data processing relationship



1. object

Compliance with technical and organizational measures

2. time

before transferring data and then regularly

3. proof

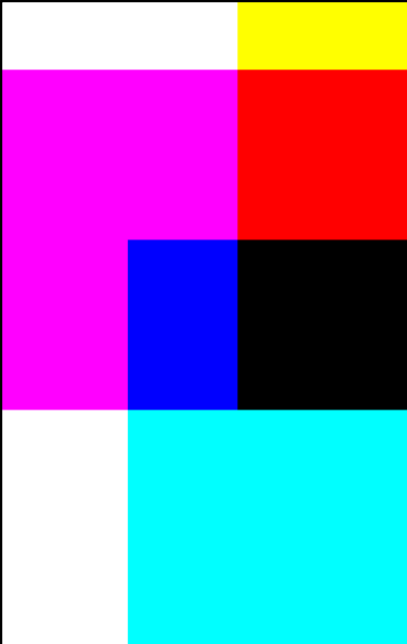
- but: only if they are up-to-date and related to data protection
- ISO 27001/ISO 9001?: because organization certificates questionable
- ISO 27018: Specifically for data protection in the cloud; formulated from a provider perspective
- EU data protection authorities (Art. 29 group): Client must always also check the test reports of the certifications

SKW Schwarz

Bechtle Upskilling Program: Cloud Workshop

Problem:

Supervisory authorities (e.g. BaFin for the banking sector) sometimes do not recognize the outsourcing of auditing responsibilities through certifications, but expect that the responsible body must always convince itself of the permissibility under data protection law; certificates can then only be an aid

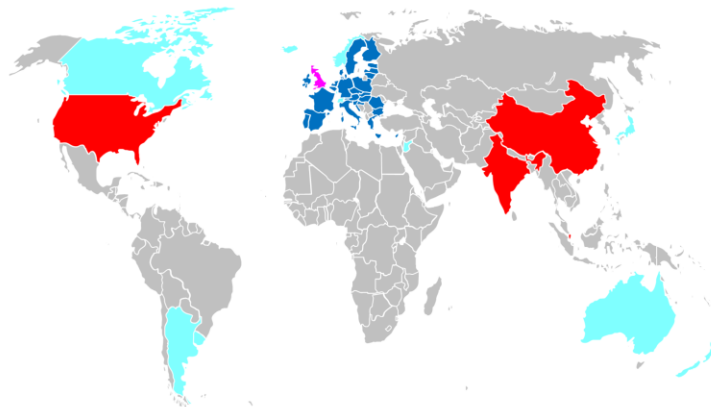


GDPR - International Data Transfer

Data protection and data security

International data transfer

The GDPR's view of the world



Data transfer within the **EU**:

- Is regulated and permissible according to DSGVO

Outside the EU only if the recipient entity's level of data protection is adequate = equivalent to that in the EU:

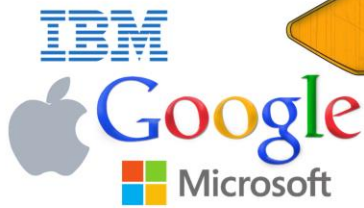
- Iceland, Norway, Liechtenstein (equivalent based on EEA treaties)
= **safe third countries**
- Andorra, Argentina, Australia, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Canada, New Zealand, Switzerland, South Korea, Uruguay, Japan (recognized as equivalent by decision of the EU Commission).
= **safe third countries**

All other countries (esp. USA, India, China, Singapore) = **unsafe third countries**

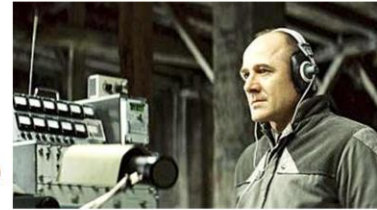
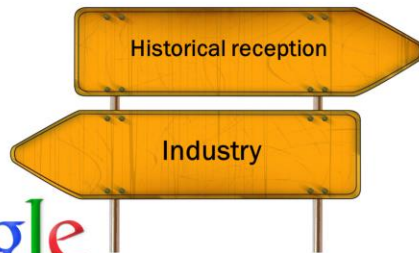
- **Only with adequate safeguards**, e.g. EU standard contractual clauses, binding corporate policies (only for group companies) or **explicit consent**
- **Special case UK** (adequacy decision has been made, but durable?)

Clash of privacy cultures

Why is privacy so different in the EU and in the US?



SKW Schwarz



BASF
We create chemistry

DAIMLER



BOSCH
Invented for life

15

Compliance in international data transfer

The problem

- GDPR requires safeguards for the protection of personal data when transferred from the EU or accessed from outside the EU, which US law does not provide, especially to non-US citizens
- US cloud or AI providers also cannot establish these guarantees through contractual promises alone, because US law is mandatory and not avoidable
- In response to complaints by Max Schrems, the ECJ has already twice declared attempts by the EU and the U.S. to regulate the situation through state agreements to be insufficient
- Technically, it cannot be ruled out in the cloud, even with a "Europe" server location ("tenant location"), that support must access from the USA or that information about current security threats is exchanged globally across all tenants. Also AI analysis is mostly done on US servers
- Additional risk: telemetry and training data used by providers for their own purposes



Compliance in international data transfer

The requirements

- Whoever is responsible for the collection and use of data must account for how, for what purposes, where and on what legal basis they process data (**accountability**, Art. 5 GDPR)
- When data leaves the EU or is accessed from outside the EU, the controller must assess the associated risks (**Transfer Impact Assessment**, TIA)
- Service providers may only be used if their level of data protection has been checked and an data processing agreement has been concluded (DPA)
- If the EU Model Data Transfer Contract (SCC) is not sufficient on its own to protect data, e.g., because of mandatory laws, additional security guarantees must be created:
contractual, technical and organizational

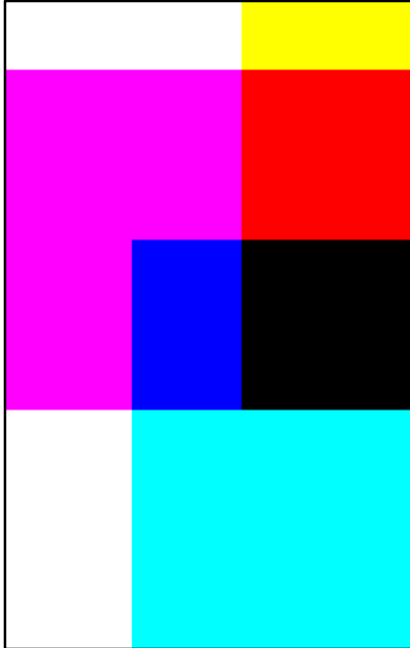


Compliance in international data transfer

The (legal) state of affairs

- Since the end of 2022, the EU model clauses (SCC) may only be used in the version of June 2021: update if necessary.
- As soon as the EU Commission recognizes President Biden's Executive Order of 7.10.2022 as equivalent data protection, DPA without SCC will suffice
- Microsoft's data protection addendum to the license agreement (MS-DPA) is not sufficient on its own, according to German data protection authorities (25.11.2022)
- Microsoft has published new version of MS-DPA on all forms of licenses effective Jan. 1, 2023: explicitly states support for customer accountability, must be agreed separately for legacy licenses
- Additional technical guarantees: EU only hosting, Hold your own key encryption, Disabling telemetry functions, spare data from algorithm training activities.
- Additional organizational guarantees: strictly narrowing of data access
- Customer must document with TIA that data flows are clearly identifiable and adequately secured





The rights of data subjects

Data protection and data security

Information requirements

Information according to Art. 13 and 14 GDPR (1)

In the entrepreneurial sphere, a basic distinction must be made between three areas:

Customers and suppliers

- Concerns the actual core business
- Main purpose of data processing is the execution of contractual relationships
- The most relevant legal basis is Art. 6 (1) lit. b GDPR: execution of contracts

Website

- Visiting a website constitutes an independent user relationship between the operator of the website and the user
- The most relevant legal basis is Art. 6 (1) lit. f GDPR: prevailing interest of the website provider

Employee context

- Concerns exclusively data processing of employee data for the enforcement and fulfillment of mutual rights and obligations
- The relevant legal basis is Art. 6 (1) lit. b GDPR together with § 26 (1) BDSG: execution of employment contracts

Information requirements

Information according to Art. 13 and 14 GDPR (2)



No legislative requirements
regarding the **form**



In principle also possible verbally,
however due to **accountability**
according to Art. 5 GDPR **text form**
recommended



Provision is owed;
Data subject **does not have to**
consent! (Information \neq Consent)



Translation into the **respective**
national language required for
international activities

Overview: Further data subject rights

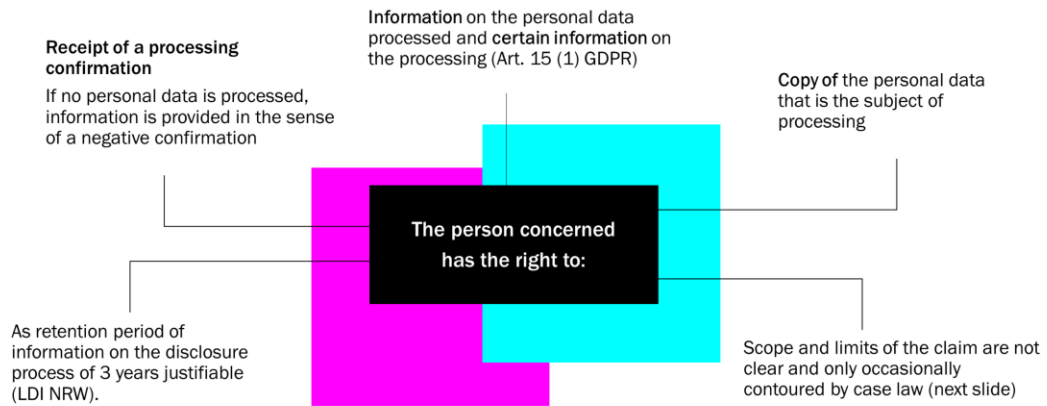
Data protection law understands "rights of the data subject" to mean the rights of each individual against data controllers.

- Information Art. 15 GDPR (very comprehensive obligation to provide information, right to receive a copy of the data)
- Correction Art. 16 GDPR
- Deletion Art. 17 GDPR ("right to be forgotten")
- Restriction of processing Art. 18 GDPR
- Right to data portability Art. 20 GDPR
- Right of objection Art. 21 GDPR
- Right not to be subject to exclusively automated processing, including profiling, Art. 22 GDPR

Recommendations for action:

- Development of a complaint management process
- Preparation of sample letters to the data subjects for the fulfillment of individual claims

Data subject rights - Right of information



Data subject rights - Right of deletion

The data subject has a
"right of deletion".

(Art. 17 GDPR)

Right of data deletion,
in particular after

- omission of the legal basis,
- revocation of consent or
- in the event of unlawful processing

In the case of **publication** by the person responsible, he or she must also inform third parties who have taken over data about requests for deletion

Exceptions to the obligation to delete, in particular under aspects of **freedom of expression / freedom of information** and the **exercise / defense of legal claims**

Attention:

Irrespective of any exercise of this right by the data subject, the controller must regularly delete in a data protection compliant manner

Data subject rights - Right of deletion

Obligation to delete/block (1)

- The controller must also ensure itself that it only processes personal data to the extent, as is permissible under data protection law (principle of storage limitation according to Art. 5 (1) e) GDPR)
- Usually, this obligation is fulfilled by a deletion and blocking concept
- If personal data is retained solely for the purpose of fulfilling retention obligations, the processing is to be restricted (common term "blocking")
 - Blocking means that there is no productive use and only a small group of people have access to the data
 - Blocking periods can be partially extendable; frequent procedure from practice (with some residual risk): Blocks one to three years after the primary legal basis has ceased to exist (such as complete contract fulfillment), depending on the frequency of incidents (such as disputes with customers).

Data subject rights - Right of deletion

Obligation to delete/block (2)

- Deletion periods result from retention obligations and other retention interests
- Most important deadlines from tax and commercial law:
Accounting-related documents usually 10 years, commercial letters usually 6 years.
- Common mistake:
Retention requirements refer to records, not the data they contain
 - Invoice must be kept for 10 years
 - Name and address (included in the invoice) but may not be stored separately for 10 years
- Other information is often kept for 3 years due to the general statute of limitations (residual risk, since no real retention obligation)

Data subject rights

Overview of other data subject rights

Art. 16 GDPR

Right to rectify
inaccurate data

Art. 18 GDPR

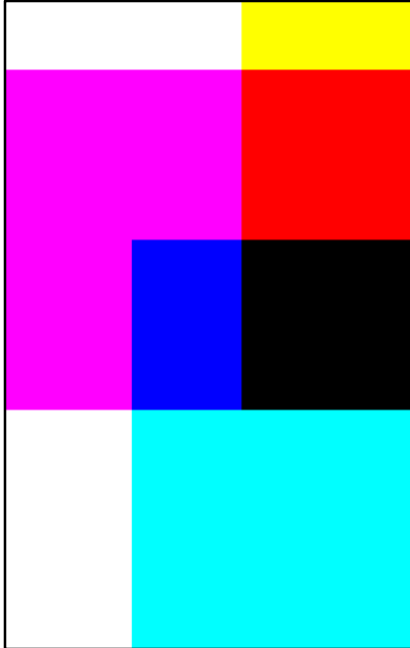
Right to restriction
of processing
Parallel to the
blocking obligation
already discussed,
but of little
practical relevance
as an active right

Art. 20 GDPR

Right to data
portability for
transferred data

Art. 21 GDPR

General right to
object to data
processing and
profiling



Liability and sanctions

Data protection and data security

Fine framework

| Art. 83 (5) | Art. 83 (5) | Art. 83 (6) | Art. 82 (1) |
|--|---|---|--|
| up to EUR 10 million or up to 2% of the global sales of the previous year | up to EUR 20 million or up to 4% of worldwide sales in the previous year | up to EUR 10 million or up to 2% of the global sales of the previous year | Liability and right to compensation |
| whichever is higher (!) | | | |
| Violations of regulations concerning e.g. <ul style="list-style-type: none"> Protective measures (TOM) Order processing (also against processors) | Violations of regulations concerning e.g. <ul style="list-style-type: none"> Principles (Art. 5) Legality | Violations of orders of the supervisory authority | In principle, any violations of the regulation Compensation of any material and immaterial damage |
| According to Recital 148 of the GDPR, infringements should in principle also be punished by fines, unless this would represent a particular hardship for the data controller. The amount of the fine depends on the individual case and takes into account a variety of indicators such as the degree of fault, assistance in clarifying the facts or economic performance. Alternatively, other measures pursuant to Art. 58 GDPR may be considered, such as administrative orders . | | | |

Compensation for GDPR violation

Intangible damages - compensation for pain and suffering

Art. 82 GDPR

gives the person concerned the right to

- Compensation for material damage to property and
- Compensation for immaterial damage (= compensation for pain and suffering), which has arisen as a result of a breach of the GDPR.



Targets both the controller and the processor



Both can exempt themselves by proving that they are not at fault

Data protection law

Who is liable then now?

Any person who, in the performance of the duties for the controller or processor, commits infringements him- or herself
(German transposition law:
Up to EUR 300,000)

Controller
(i.e. the company)

Processor
(i.e. the company)

Management
(within the scope of general
compliance liability)

Data Protection Officer
(is co-responsible for
monitoring data protection
according to GDPR)



AI and data protection

What data does the chatbot access?

- Public sources vs. own data and systems
- Earmarking principle
- Principle of data accuracy

Who is responsible under data protection law?

Own responsibility of the operator vs. commissioned processing?

Privacy

How can I protect myself in the best possible way?

Data minimization and transparency

Conclusion:

Will the GDPR stop Artificial Intelligence?

AI and data protection

Authorities take action (status april/may 2023)

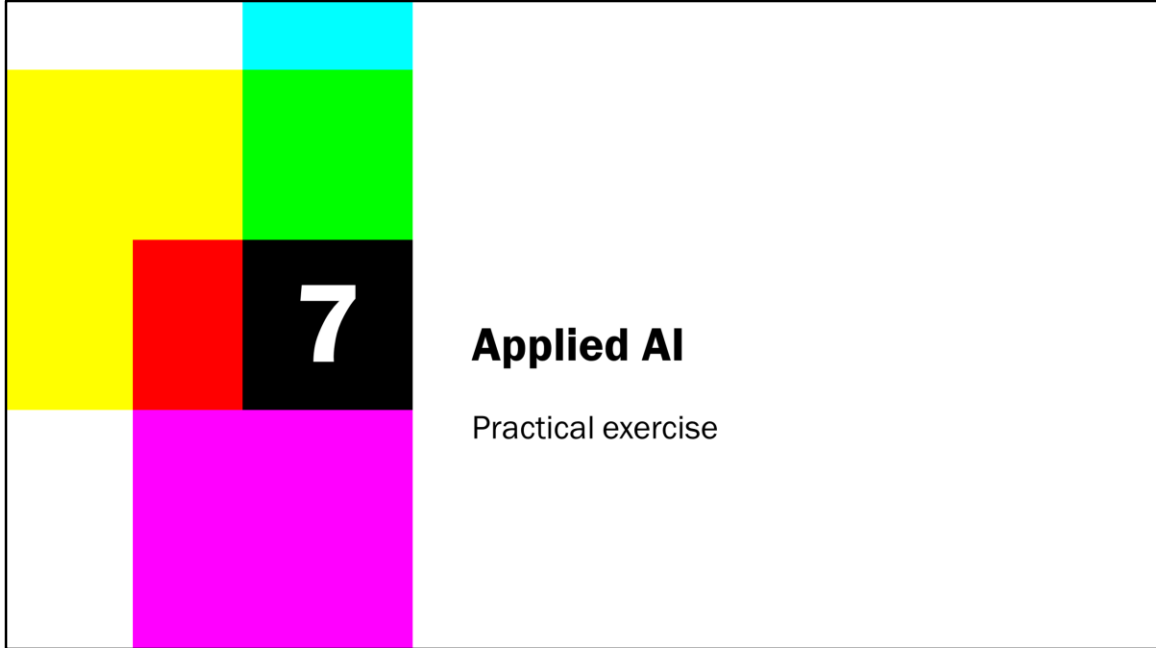
→ Action by **Italian data protection authority** (march/april 2023): blocked access to ChatGPT for Italian users due to privacy concerns:

- **Lack of transparency** with regard to scope and purposes of processing the prompted data
- No legal basis for the use of prompted data for OpenAI's **training of algorithm** purposes
- Consent as legal basis would be available but needs to respect **protection of minors** (<13 years of age)
- OpenAI has not seat or subsidiary in Europe, thus any authority is eligible to take actions

→ **OpenAI reacts:**

- Users may **opt-out** of their prompted data being used for training purposes (including data history)
- OpenAI added **more information**
- Respective consent restriction on minors and **age verification** introduced
- "ChatGPT Business": will include general opt out of training and may **run on premise**

→ **Germany:** task force of authorities has been implemented



Applied AI – practical exercise

Rosenheim AI, Inc.: services for logistics

- Rosenheim AI, Inc. has developed a data model that allows to analyse a number of live data from intra-campus vehicles of large industry sites and to predict needs for maintenance as well as common traffic routes
- Analyses:
 - Vehicle data: movement, hours of operation, GPS data, vibration, sounds, LIDAR data
 - Predicts: need for maintenance, risk of traffic congestion, time of travel for individual routes
- Services:
 - Predictive maintenance
 - Improvement of efficient routing
 - Improvement of use of vehicles and human operators

Applied AI – practical exercise

Rosenheim AI, Inc.: services for logistics

→ Questions:

1. What assets or means do we need to offer our services?
2. Who can provide the assets and means?
3. What contracts do we need and with whom?
4. What do we offer? What contracts do we need and with whom?
5. Is there a privacy issue to address?

Remember:

Only things and rights can be subject of contracts

