



**Invoice Number**

2563

Amount due

\$440

Payment method

Bank Transfer

Date

20-01-2023

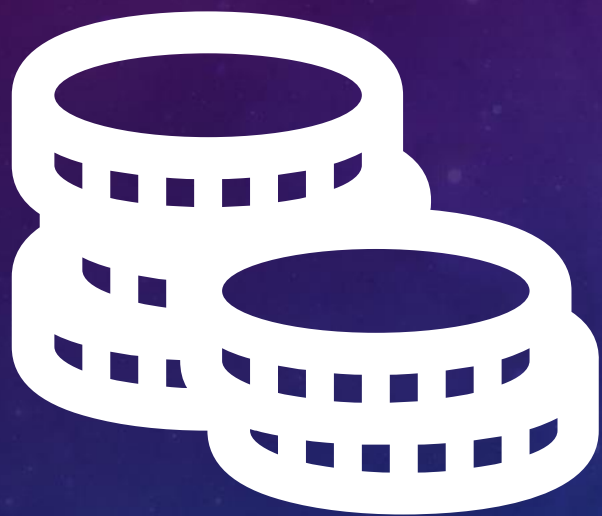
Billed to

Luca Di Lorenzo
Vansk Avenue 8
00000 City
CRN: 123 456 789A

Billed from

Lucy Myers
Round Square 52
00000 City
CRN: 000 562 114B

Description	Unit cost	Quantity	Total
Service 1	\$70	1	70
Service 2	\$10	5	50
Service 3	\$20	2	40
Service 4	\$20	2	40



+ 21 %



CLEAN DRIVING RECORD
NO CAR ACCIDENT
NO FINE



300 pages report:
Every single trip you took over 6 months
Hard breaking, high speeds, rapid acceleration





CAR COMPANY

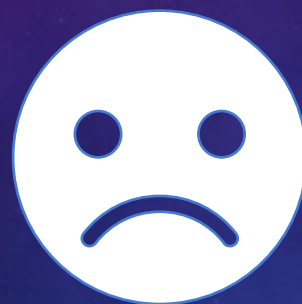


INSURANCE COMPANY



INSURANCE COMPANY







**Czech
AI Factory**

HOW AI MET THE GDPR

RESPONSIBLE AND TRUSTWORTHY AI

LETNÍ ŠKOLA CZECH AI FACTORY

PETRA PETREK LAŠOVÁ



WHAT IS GDPR?

EU regulation, effective since 2018.

WHAT DOES GDPR HAVE TO DO WITH AI?

NOTHING 😊

...AI is not mentioned in its text

But wait...REALLY?!

WHAT DOES GDPR HAVE TO DO WITH AI?

Magic word:

DATA

GDPR IS...

...technologically NEUTRAL.

...does NOT care which tech you use.

...only cares about DATA.

...not all the DATA.

...PERSONAL DATA.

GDPR IN ONE SENTENCE

GDPR...

...sets rules on HOW to PROCESS personal data.



Mark all options with Personal Data

① The Slido app must be installed on every computer you're presenting from

slido

WHAT IS PERSONAL DATA?

- Name?
- Surname?
- Address?
- Device IDs?
- E-mail address?
- Static IP address?
- Dynamic IP address?
- Logs?
- Prompts?
- Chat histories?
- Profiles?
- Scores?
- Predicted behavior?
- Inferred data?

PERSONAL DATA - GDPR DEFINITION

any information relating to an **identified (1)** or **identifiable (2)** natural person

IDENTIFIED NATURAL PERSON

Name: Richard

Surname: Hruška

Born: 29/2/1986

- Easy one: We can immediately identify the person
- Typical personal data (name, pictures, contact info)

IDENTIFIABLE NATURAL PERSON

Less typical personal data:

Information that can be linked to an identifiable individual considering all the means reasonable likely to be used.

I ASK: How much resources do I need to identify the persons? Time? Money? Is it reasonably likely that I will use that time and money for identification?

AI AND GDPR - SUMMARY

- AI is data hungry
- AI needs data
- GDPR applies to any processing of personal data, including AI systems
- When AI uses personal data = Application of GDPR

REAL CASES

CASE NO. 1: CLEARVIEW AI



CLEARVIEW AI

- WEB SCRAPPING: scrapping photos from social networks, news sites, multiple online sources
- FACIAL RECOGNITION DATABASE: building a massive searchable facial recognition search engine
- BIOMETRIC DATA: biometric identification

CLEARVIEW AI

“We will only use it for law enforcement.”

Reality check: biometric database sold to Walmart, Bank of America, United Arab Emirates...etc....

WHAT WAS THE MAIN PROBLEM?

- A) Web scrapping without rules and limitations
- B) Building a HUGE dabatase of facial recognition and selling it to anyone who paid

CLEARVIEW AI: FINES

The Netherlands: **35,5** mil. eur plus ban

France: **20** mil. eur plus ban

UK: **7,55** mil. eur plus ban

Italy: **20** mil. eur plus ban

Greece: **20** mil. eur plus ban

Canada: Clearview lost lawsuit, service banned

USA (Illinois): service banned

Australia: service banned

CLEARVIEW AI LECTURE: WHAT CAN WE LEARN?

CLEARVIEW AI WORKING METHOD:

We can freely use everything (personal data) what is accessible online.



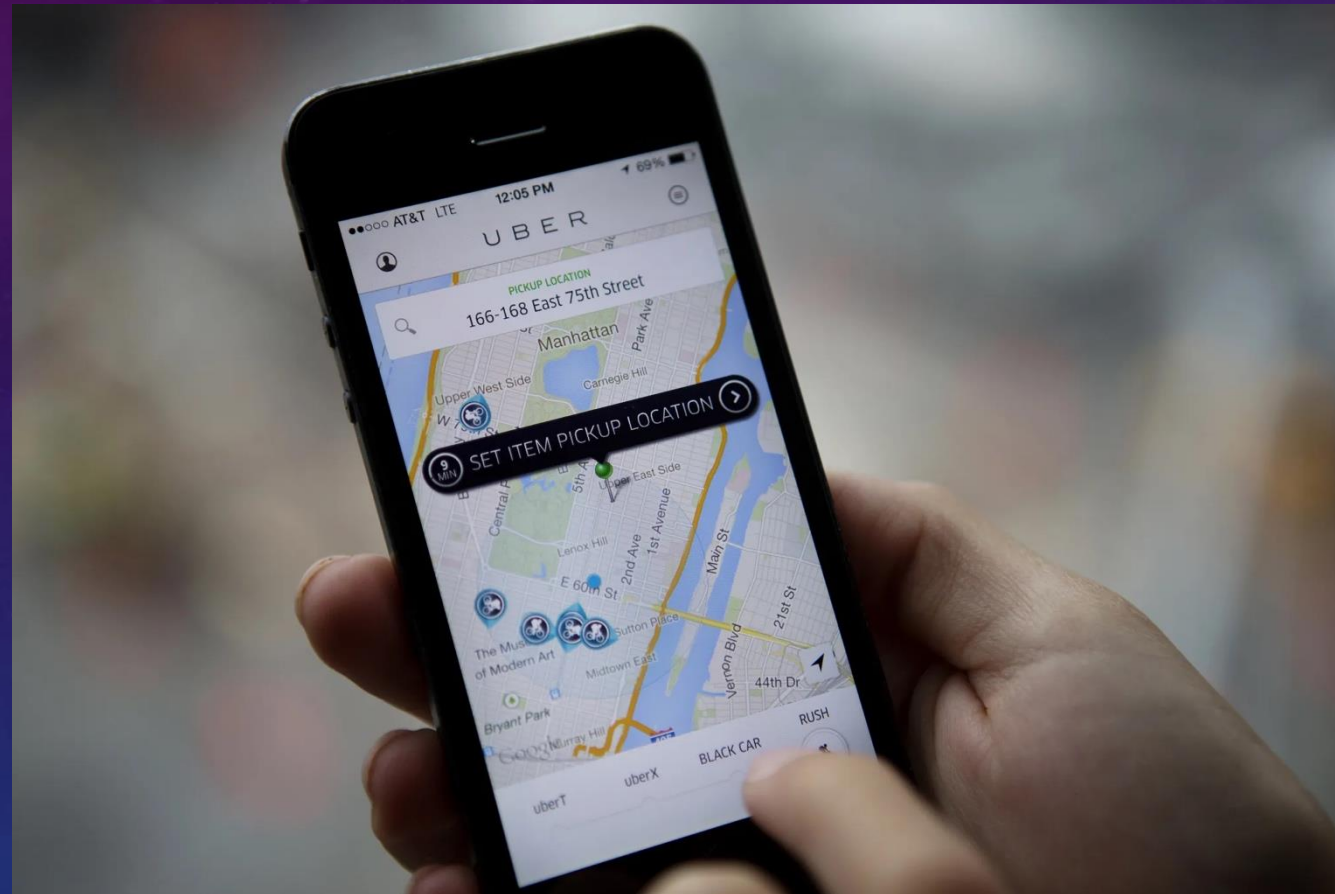
CLEARVIEW AI LECTURE: WHAT CAN WE LEARN?

If something (personal data) is online, it does not mean I can use it however I want.

CLEARVIEW AI: RULES INFRINGEMENTS

- NO valid legal basis (consent, contract, legitimate interest...)
- NO data minimisation
- NO transparency (individual, web page)
- NO access request answer

CASE NO. 2: UBER



UBER

- Software: tracking drivers and passenger ratings.
- Result = algorithmic decisions (e.g. low ratings) = account deactivation (sometimes permanently).
- Decision taken by AI.
- UBER drivers did not know about it.

UBER CASE CONSEQUENCE: JOB LOSS

“From one moment to the next they (UBER drivers) no longer had any income ... a computer should not make decisions on its own that have (such) major consequences.”

Monique Verdier, Dutch Data Protection Authority

UBER FINE (AUGUST 2026)

The Netherlands: €825 million eur

UBER LECTURE: WHAT ARE THE ISSUES?

Can I use AI driven automated decision making?

Well, under certain circumstances, you can, BUT...

HUMAN IN THE LOOP PRINCIPLE

If you comply with Art. 22 GDPR and decide to use (AI driven) automated decision making:

“Human in the loop principle”

Human who **can have an actual influence over** the process (not just signing of the paper)

to avoid biased or discriminatory results.

HUMAN IN THE LOOP PRINCIPLE = THREE R 😊

- 1) R: Right to: obtain human in the loop intervention + meaningful explanation of the logic involved
- 2) R: Right to: Express point of view
- 3) R: Right to: Contest the decision

CASE NO. 3: SAMSUNG



SAMSUNG

- Employees of SAMSUNG were using ChatGPT
- Data Leak (input stage): confidential company documents (trade secret) and source code uploaded to ChatGPT
- Data uploaded to servers beyond company's control

SAMSUNG

No fine, but the company has lost trade secret and valuable documents, source codes...

= financial damage

SAMSUNG LECUTRE: SECURITY OF PROCESSING

- Protect the data you dispose with
- Prevent data leaks (information, education, technical and operational measures)
- Tailor the measures to your needs

SAMSUNG LECUTRE: TRANSFERS OF PERSONAL DATA

- Within EU – free movement of data
- Other countries – special GDPR rules that need to be followed (depends on concrete country)
- Difference if I send the data to Sweden, USA, Japan or China

SAMSUNG CASE SUMMARY

- Be careful about your data flow (map it)
- Keep in mind the security of processing
- Follow the rules on data transfers

SUMMARY

GDPR RULES - IMPORTANT NOTE:

GDPR does NOT say: DO NOT process personal data

GDPR says: process personal data IF you follow the rules

GDPR also says: if you process personal data and do not follow the rules, you might face huge fines and a possible ban

3 IMPORTANT LECTURES FROM TODAY

- (1) **CLARVIEW LECTURE:** If something (personal data) is online, it does not mean I can use it however I want.
- (2) **UBER LECTURE:** Algorithmic decision making ALWAYS needs “Human in the Loop.”
- (3) **SAMSUNG LECTURE:** Do not feed generative AI tools with personal data, confidential company data.

Respecting privacy is not optional; it's a legal and ethical baseline.

USEFUL SOURCES

GDPR text: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679>

Guidelines, Opinions, Statements: European Data Protection Board (EDPB):
https://www.edpb.europa.eu/documents_en

EDPB Guidelines on Web Scrapping: https://www.edpb.europa.eu/public-consultations/guidelines-032026-on-web-scraping-in-the-context-of-generative-ai_en#no-back

EDPB Opinion on Personal Data in the context of AI models: https://www.edpb.europa.eu/documents/opinion-of-the-board-art-64/opinion-282024-on-certain-data-protection-aspects-related-to_en

Thank you 😊

JUDr. Petra Petrek Lašová, LL.M., CIPP/E
petra.petrek@indrc.cz

BONUS SLIDES

PSEUDONYMISED VS ANONYMISED DATA

- Pseudonymised data: re-identification is still possible using separate additional information = still personal data, GDPR regime applies
- Anonymised data: re-identification is not possible anymore – GDPR does not apply

GOOD TO KNOW

- Special category of personal data
- stricter rules of processing
- E.g.: political opinions, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation...

WHO IS RESPONSIBLE – WHO SHOULD CARE?

- Easy answer: everybody should care about personal data 😊
- Complex answer: Responsibility depends on one's decisive powers. Responsible is the one who decides why and how the personal data is processed (his name is „Controller“).
- Controller is the one who determines purposes and means of personal data processing

WHO IS RESPONSIBLE?

- Josef is an AI developer
- Startup idea – AI system to detect fraudulent behaviour or content
- Needs data to train his AI model
- Josef wants to process data - personal data as well
- Great that he knows – oh, there is something like GDPR!
- What should Josef do?

JOSEF'S QUESTION FOR DATA PRIVACY LAWYER

- Well, we have internet 😊, everything is online anyway.
 - Josef thinks: I will just collect the data from internet without need to follow legislation.
 - Can I do it?
-
- Data Privacy Lawyer's answer: no. Well, you can do it, but you have to follow the rules.
 - Explanation: even if data is available online, it does not mean I can use it how I want.
 - Josef should look at it as a completely new starting point – new task with data – new rules

JOSEF'S TASKS

- Define purpose, means of processing
- Legal basis
- Principles
- Data Mapping, ROPA
- DPIA
- Human in the loop principle
- Security measures
- Data subjects rights
- Data transfers rules

EXAMPLES ON THE FOLLOWING SLIDES

JOSEF'S PURPOSE

- = reason
- WHY do I do it?
- Why do I need to collect/use personal data?
- Josef's answer: Startup idea – AI system to detect fraudulent behaviour or content – I need personal data to train my AI model
- Keep in mind: purpose limitation – what does Josef plan to do next? Josef cannot just collect the data for one purpose and then use it for a purpose NOT compatible with the original purpose

JOSEF'S LEGAL BASIS

6 possibilities (Consent, Contract, Legal obligation, Vital interest, Public interest, Legitimate interest)

- In this type of processing (the most usually): **legitimate interest**

JOSEF'S PRINCIPLES - DATA MINIMISATION

- Collecting data **NECESSARY** for the purpose **ONLY**.
- **POSSIBLE TO** collect large volume of data, if it is **NECESSARY** for the purpose

JOSEF'S PRINCIPLES – DATA MINIMISATION

- Josef should answer to these questions: Could I use synthetic data instead of personal data? How do I define precise data collection? Do I have filters at place which exclude the collection of certain categories of data (e.g.bank transaction data, location data)? Can I exclude certain categories of websites?

JOSEF'S PRINCIPLES – DATA MINIMISATION

- Josef shall also consider:
- Where feasible, anonymisation or pseudonymisation of personal data.
- Applying syntax-based filtering mechanisms to filter out personal data identifiable by their format (e.g. social security number, telephone number)
- If possible, replacing some real data with synthetic data in order to reduce exposure to personal data.

JOSEF'S PRINCIPLES - ACCURACY

- Data must be accurate and updated
- Josef shall consider:
- Using data from reliable sources (e.g. official webpage)
- Timestamping of the data
- Validating the data before AI training: correction of formats (e-mail, phone numbers...), spot-check random samples for accuracy

JOSEF'S PRINCIPLES - TRANSPARENCY

- People must be informed about personal data processing
- Privacy notice – what personal data do you process, purpose, legal basis, for how long
- But first, you must know what you process 😊

JOSEF'S ACCESS REQUEST COMPLIANCE

- People have the right to access their data
- When access request comes, you have to respond and provide information

„Do you process my data?“

„Yes, we do. We process your data: name, surname....“