Human-centred data ethics in practice

Kristofers Kalniņš-Liberis, Data Protection Officer, Debate mentor

kristoferskl@gmail.com; www.linkedin.com/in/kk-l

DO IMPACT, Social Entrepreneurship Association of Latvia (7/11/2025)

Privacy risks *you may haven't thought of (luckily)* **& solutions** *you might need*

Kristofers Kalniņš-Liberis, Data Protection Officer, Debate mentor

kristoferskl@gmail.com; www.linkedin.com/in/kk-l

DO IMPACT, Social Entrepreneurship Association of Latvia
(7/11/2025)

Can a shadow be personal data?

Can a shadow be per data?

Data protection by design and by default

WAY OF THINKING & WORKING

EASIER TO IMPLEMENT AT START THAN TO DEAL WITH CONSEQUENCES

MINIMISING RISKS TO PEOPLE AND ORGANISATIONS

SECURITY (TECHNICAL & ORGANIZATIONAL) MEASURES

DOCUMENTING YOUR INTENTIONS, ASSESSING BEST MODE OF ACTION, HAVING EVIDENCE

EMPLOYEE AWARENESS-RAISING

Legal basis: consent vs agreement: which is better?

Consent if data processing of more casual nature

Agreement if withdrawal of consent can create negative impact or processing more complex and needs more informing

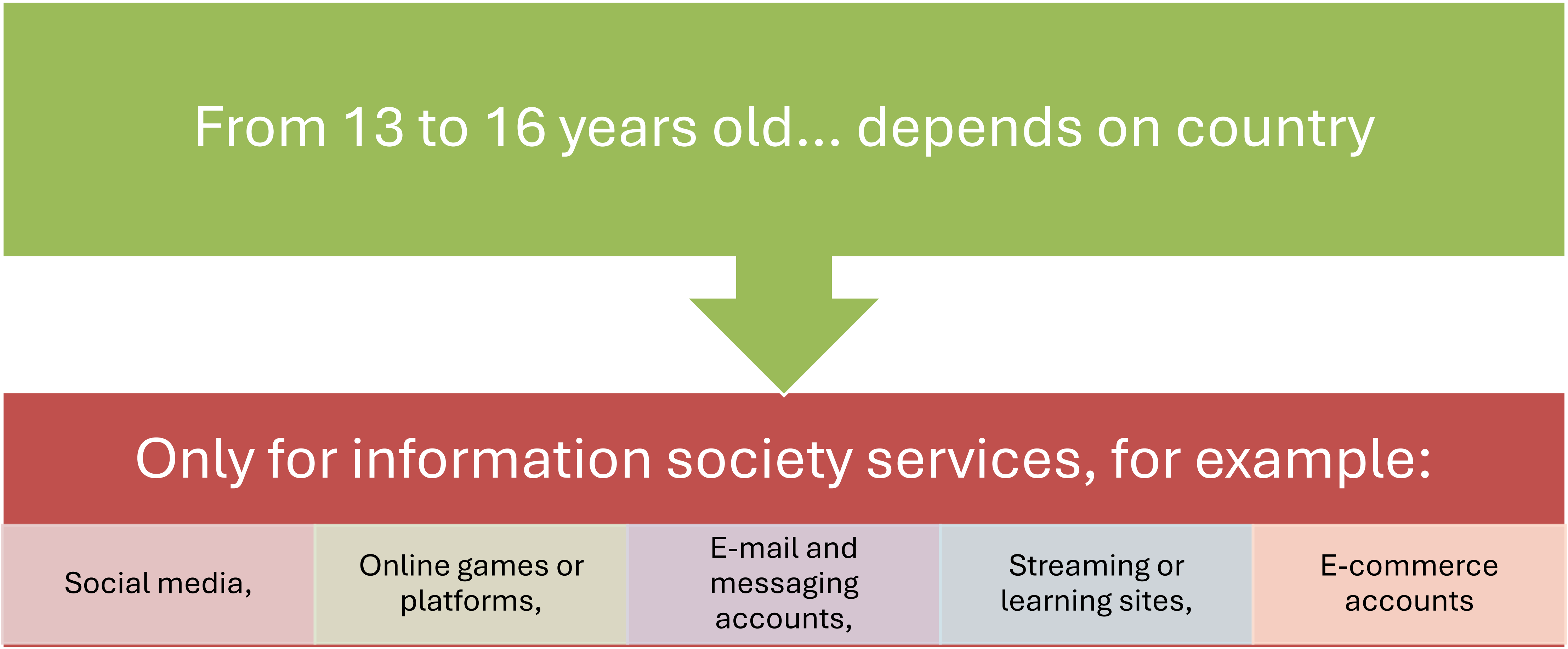
Multiple legal basis for processing activity

General rule: 1 activity = 1 purpose = 1 legal basis

In reality: legal obligation to process but Company has freedom to chose HOW to process

Example: AML obligation to Know Your Client (KYC) – obligation to know but documentation and tools are for you to choose

ePrivacy: age of consent for data processing



From 13 to 16 years old… depends on country

Only for information society services, for example:

- Social media,
- Online games or platforms,
- E-mail and messaging accounts,
- Streaming or learning sites,
- E-commerce accounts

Documents moving outside Controller’s place

Risk of intentional un unintentional loss and theft

(Better to delete internally than to lose outside)

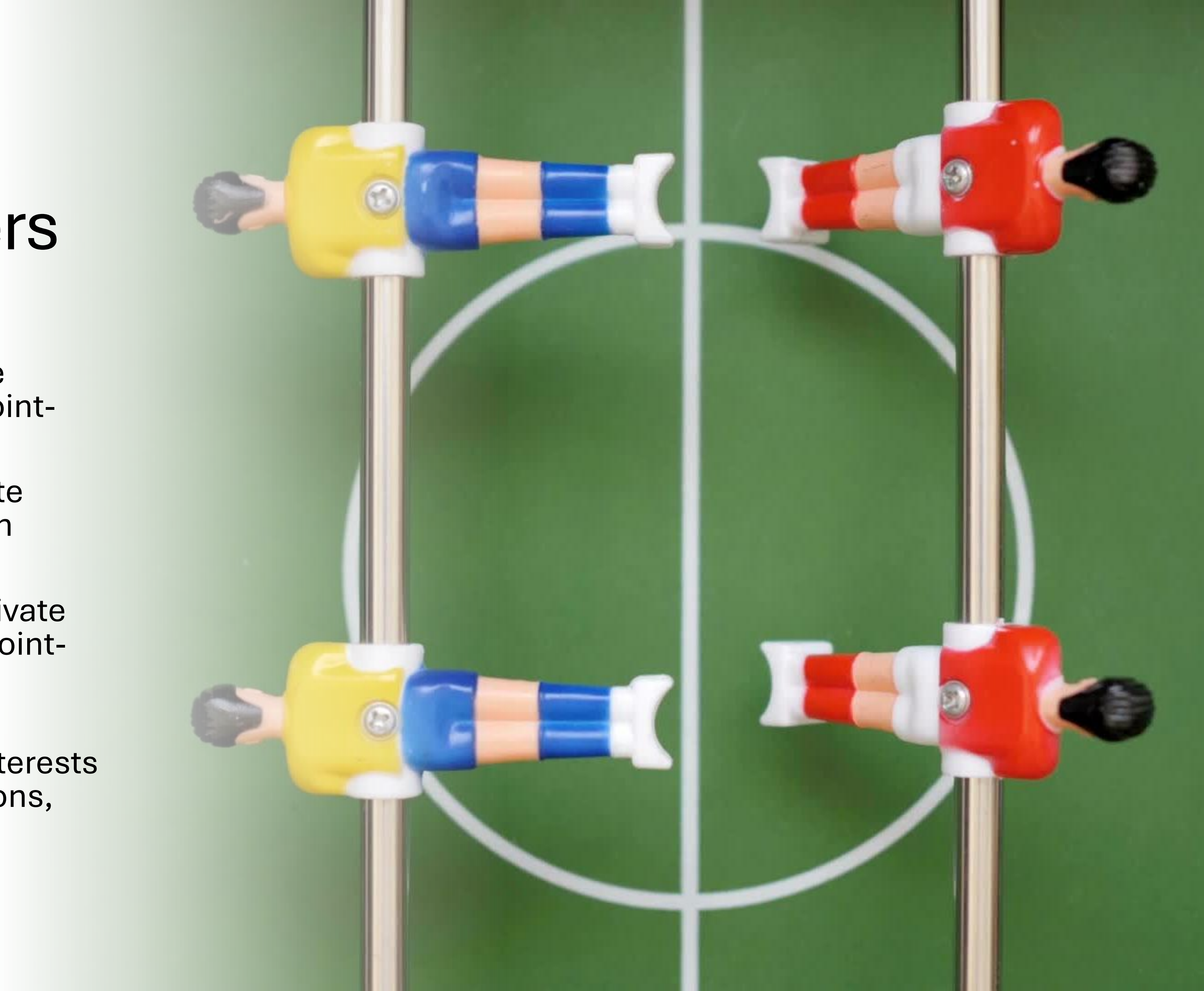
Suggestion: personal data documents are kept within premises

Less is more: data minimisation brings results

- Especially visible in cases of prediction/profiling
- Input – output: real behavior more important than labels

Separate vs Joint Controllers

- If purposes and procedure determined jointly: then Joint-Controllers
- If Controllers have separate purposes or interests: then separate Controllers
- In the context of Public-Private Partnerships: most likely Joint-Contoller
- Note: Processors may be Controllers in their own interests (e.g. legal claims, obligations, specific internal security measures)

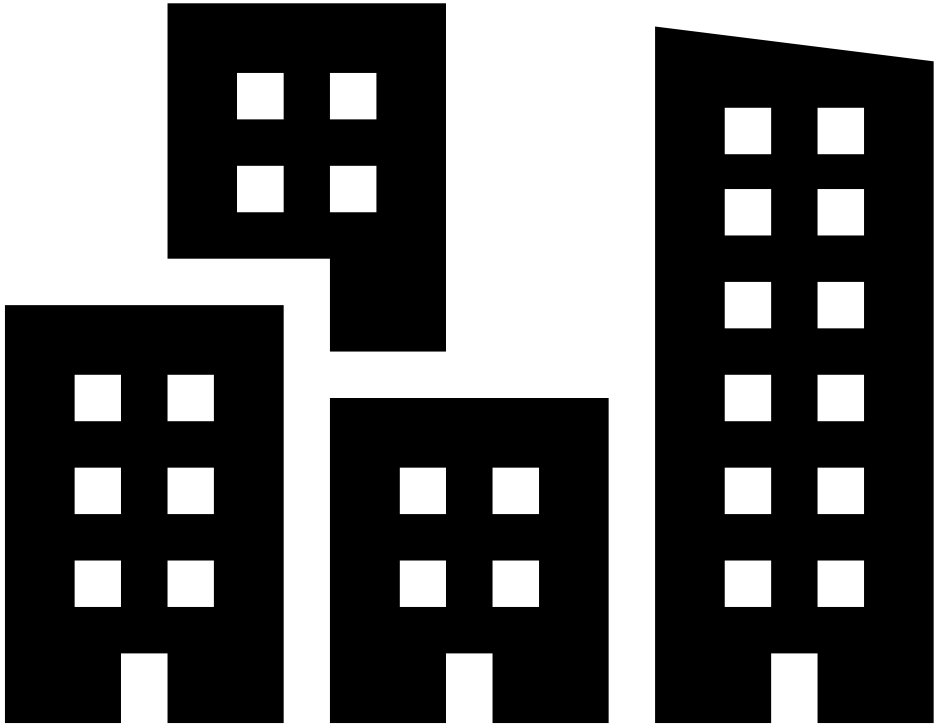


Name.Surname@company.eu: personal data?

- Personal data in any case
- Less protection if information made public or of a public person

Info/Office@company.eu: personal data?

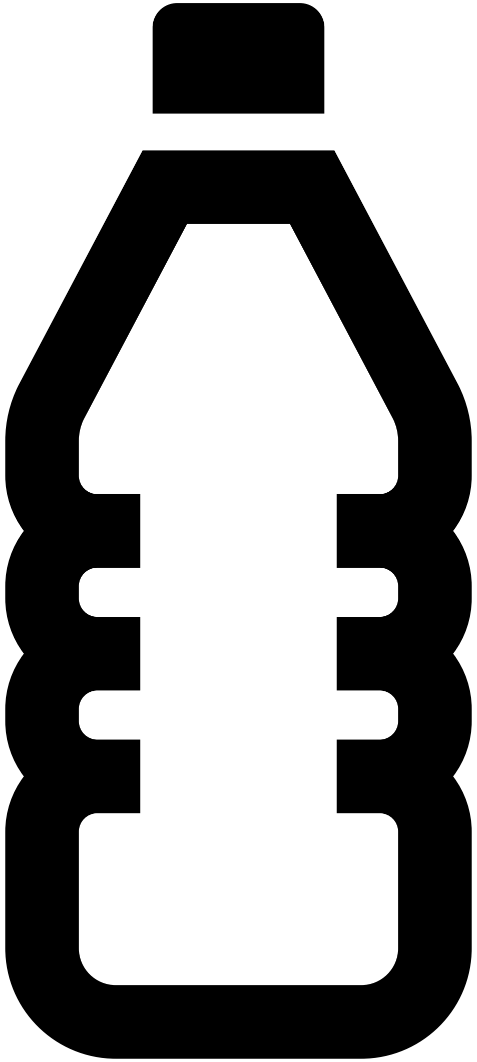
- Not personal data
- Except if recipient of e-mail known



Company transfers pseudonymized data to other company? Is it personal data?

Depends if recipient can identify person

Example: bottle-deposit system providers & retail stores



Data transfer to third countries: inevitable. Focus on information!

Example: large service providers, social media

Using Company data as evidence by a private employee in personal court – curiosity & emotions

Controller's purpose vs private interest

Personal data breach

Both private employee & company held liable

A judge cannot 'unsee' evidence, even if obtained illegally. Judge can only add less value to the evidence.

Apotheca Estonia: 3,5 million EUR fine

INSUFFICIENT SECURITY (TECHNICAL & ORGANIZATIONAL) MEASURES – LINK ENGINEERING

THIRD PERSON ACCESSED 750’000 APOTHECA CLIENT BACKUP DATA (INCL. PURCHASE HISTORY)

CAN BE USED FOR BLACKMAILING OR FRAUD

True cost of Artificial intelligence

Data scraping personal data breaches & copyright infringement

Commercial & confidential information sharing

Errors (halucinations) – small and large

Loss of skills & creativity

AI slop – loss of authenticity and quality

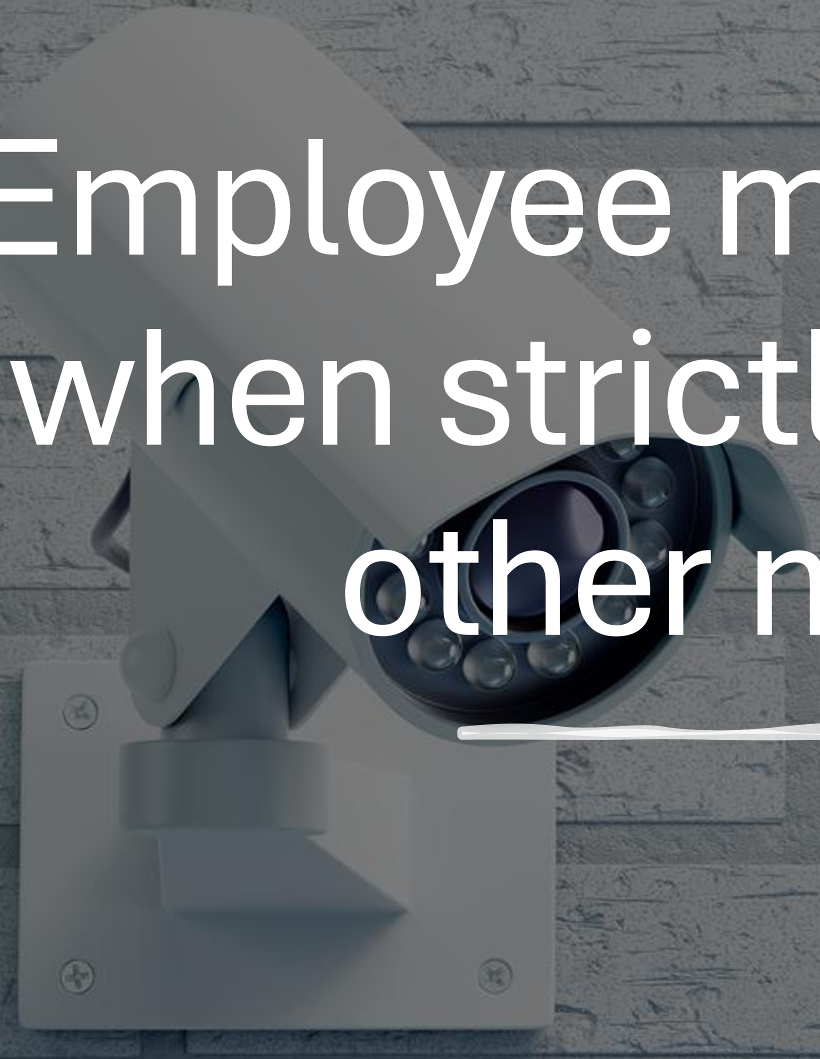
Informing recipients about use of AI

Right not be subject to automated processing. Have human oversight!

AI Chatbot Companions: loneliness, echo chamber psychosis & depression

Recruitment AI: trash in; trash out

Employee monitoring: only when strictly necessary if other means fail



Access rights & data retention: not that hard

PERSON WHO PROCESSES DATA SHOULD HAVE ACCESS ONLY TO WHAT IS NECESSARY – NO SHARED ACCOUNTS OR GENERAL ACCESS

PROCESSING DONE ONLY WHEN NECESSARY FOR THE PURPOSE

DATA DELETION GOES TOGETHER WITH DATA MINIMIZATION – IF NOT NECESSARY FOR A PURPOSE THEN PROCESSING SHOULD BE LIMITED (I.E. LIMITING ACCESS E.G. ARCHIVAL, HISTORICAL PURPOSE)

Cookie policy vs Privacy policy?

- Cookie policy is for website tracking mechanisms (strictly necessary; marketing; analytical etc.) – explaining how and why
- Privacy policy is about all processing acitivites that relate to person

One Privacy policy
vs
many Privacy policies

- Think about what should be publicly available and internal (e.g. Consumers, Visitors & Business partners vs Employees)
- Dividing information between different types of interaction with Controller

Providing information (privacy policies & notices):

legalese & technical terms

vs

simple language

What privacy and data protection is about?

- Respecting peoples' interests and preferences
- Informing people in a transparent manner
- Documenting your processes and evidence
- Having control of procedures and security
- Knowing what you do and why
- Giving people rights to know, to influence, and to withdraw
- You can both be a Controller and a Data subject

Practical session of yesterday

Kristofers answers

Scenario 1: Member Data Management

Your organisation collects personal details from members, including contact info, skills, service info, and participation history. A new staff member suggests creating a shared Excel file to easily track members and share it with volunteers or other stakeholders outside of the organisation.

Security & Privacy:

- Is it safe to store and share member data this way? Why or why not?
- What measures would you put in place to protect privacy?

Policies & Guidelines:

- What internal rules or policies should guide access to this data?
- Who should be allowed to see or edit it?

Ethical Considerations:

- Are there ethical concerns about sharing member data with volunteers or external stakeholders?

Relevance to Your Organisation:

- Could a similar situation happen at your organisation?
- How would you currently handle it? Would your approach change after this discussion?

Scenario 2: Digital Tools for Impact Tracking

You start using a mobile app to track beneficiaries' progress in a social programme. The app requires collecting sensitive health or financial data. Some participants are uncomfortable sharing this digitally.

Consent & Privacy:

- How would you ensure participants give informed consent to share their data?
- How do you respect participants' comfort levels with digital data collection?

Data Security:

- What measures can you put in place to protect sensitive information collected by the app?

Ethical Considerations:

- What ethical concerns arise when using digital tools to collect personal or sensitive data?

Relevance to Your Organisation:

- Could a similar situation happen in your organisation?
- How do you currently handle digital data collection, and would you change anything after this discussion?

Scenario 3: Beneficiary Information Sharing

Your organisation partners with other NGOs. A partner asks for detailed beneficiary data to coordinate services. You're unsure which information can be shared.

Data Sharing:

- What information can you ethically and legally share with partners?
- What guidelines or rules should determine what is shared?

Privacy vs. Collaboration:

- How do you balance the benefits of collaboration with the need to protect beneficiaries' privacy?

Policies & Procedures:

- Would your organisation need policies or agreements for data sharing? What might they include?

Relevance to Your Organisation:

- Could a similar situation happen in your organisation?
- How would you currently handle it, and would you change anything after this discussion?

Scenario 4: Using Photos for Promotion

You want to showcase your programmes on social media. Volunteers suggest posting photos of beneficiaries participating in workshops. Some beneficiaries might not want their images online.

Consent:

- How would you obtain informed consent from beneficiaries before using their photos?
- What information should you provide to ensure consent is truly informed?

Privacy & Alternatives:

- What alternatives exist to using identifiable images (e.g., illustrations, silhouettes, group photos without faces)?

Ethical Considerations:

- What ethical concerns arise when posting photos of beneficiaries online?

Relevance to Your Organisation:

- Could a similar situation happen in your organisation?
- How do you currently handle photos for promotion, and would you change anything after this discussion?

Scenario 5: Data Retention and Deletion

Your organisation has collected data from participants over the past 10 years. Some files are outdated, but staff are unsure whether to delete them or keep them “just in case.”

Data Retention:

- How long should different types of data be stored?
- What criteria would you use to decide whether to keep, delete, or anonymize data?

Privacy & Security:

- What risks exist if old or outdated data is kept unnecessarily?
- How can you mitigate these risks?

Policies & Procedures:

- Should your organisation have formal rules for data retention and deletion? What might they include?

Relevance to Your Organisation:

- Could a similar situation happen in your organisation?
- How would you handle it currently, and would you change anything after this discussion?

Stay safe and ethical!
Time for questions.

Kristofers Kalniņš-Liberis, Data Protection Officer

kristoferskl@gmail.com; www.linkedin.com/in/kk-l. Feel free to reach out.