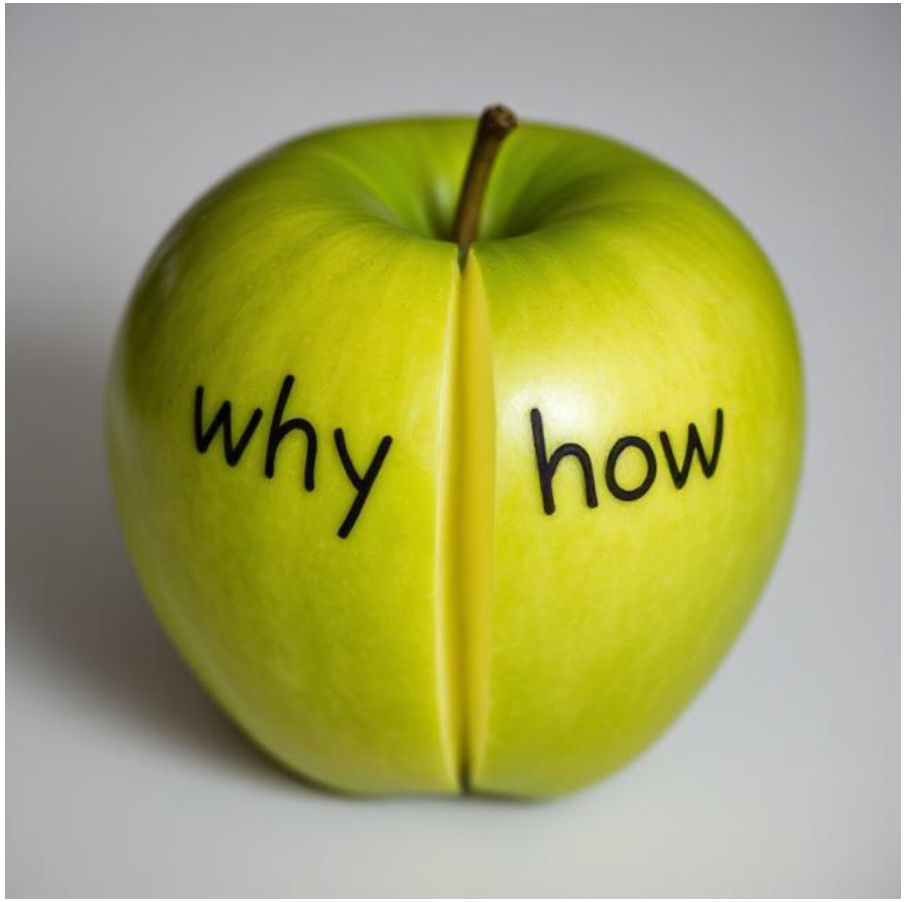
Data ethics in perspective

Dr. Aleksandrs Potaičuks

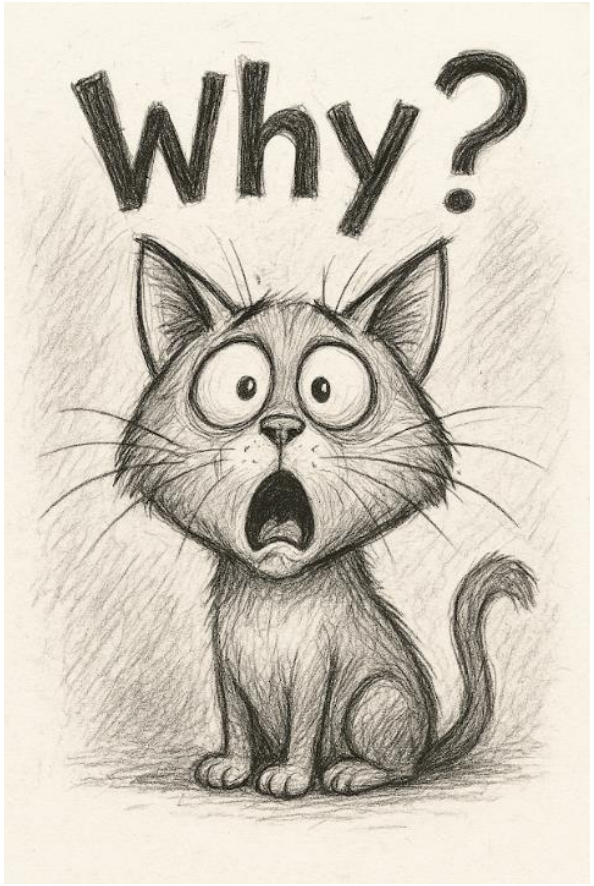
07/11/2025

Introduction: method & scope

Why does data protection matter?



How can you ensure that you are acting ethically with data?



Why does data protection matter?

Physical, material or non-material damage

→ What negative consequences could there be if we breach someone's data protection rights (the GDPR)?

- Go to slido.com and:
  - enter the code: #6012247
  - or scan the QR code

Physical, material or non-material damage

Disclosure of sensitive health personal data to the employer: Radu v. Moldova

- Ms Radu underwent artificial insemination. Due to complications and a high risk of miscarriage, she was hospitalised. She submitted a standard sick note citing pregnancy-related complications. However, her employer (Police academy) requested more detailed medical information from her healthcare provider.

- Extremely sensitive personal data was subsequently disclosed, including not only her hospitalisation date and miscarriage risk, but also details about her artificial insemination, twin pregnancy, hepatitis B, blood type, obstetric complications and treatment (the medical file was included in full). Ms. Radu soon suffered a miscarriage, which she attributed to the stress caused by the breach of confidentiality. Rumours circulated at her workplace, and even her husband resigned under similar pressure (*Radu v. Moldova*).

- Violation of Article 8 as disclosure was not "in accordance with the law“: domestic law did not provide adequate precision and safeguards (discretion conferred on the public authority) (*Radu v. Moldova, §§ 31*)

Physical, material or non-material damage

Use of your image by a public authority for a good purpose: PTAC saga

- PTAC organised an awareness campaign about the risks involved in buying a second-hand vehicle. Within this campaign, the PTAC created and shared a video online. Notably, the PTAC used the image and voice of a well-known Latvian journalist - an expert in the automotive sector - without his knowledge and consent. The PTAC rejected the journalist's objection to the online dissemination of the video and his request for compensation, as it considered raising awareness to be part of its public function.

- Supreme Court: the good intentions of public authorities cannot override the fundamental principles of data protection.

- Data processing that goes against a person's will, such as publishing their personal data in an unacceptable manner or context, primarily affects their private autonomy to object against the use of their persona (public image). This, in turn, affects their integrity and dignity.

Physical, material or non-material damage

Use of your image by a public authority for a good purpose: PTAC saga II

- ‘Reputation, honour and dignity’: the social disadvantage, worries, humiliation and anxieties suffered by the data subject; and the long-term and future consequences for the data subject’s reputation.

- Supreme Court: the applicant is a public figure who has cultivated his respectful public image over a long period (nearly 30 years). Therefore, in this case, the impact on the applicant’s image - and, accordingly, on his honour and dignity - may be more significant than in a case involving a person who is not publicly known.

- Supreme Court: the video was distributed by other websites, causing the applicant to suffer as a result of clickbait culture - a practice where sensational or misleading headlines are used to attract views. The video was widely distributed over an extended period in a digital environment, reaching a broad audience and negatively affecting his reputation.

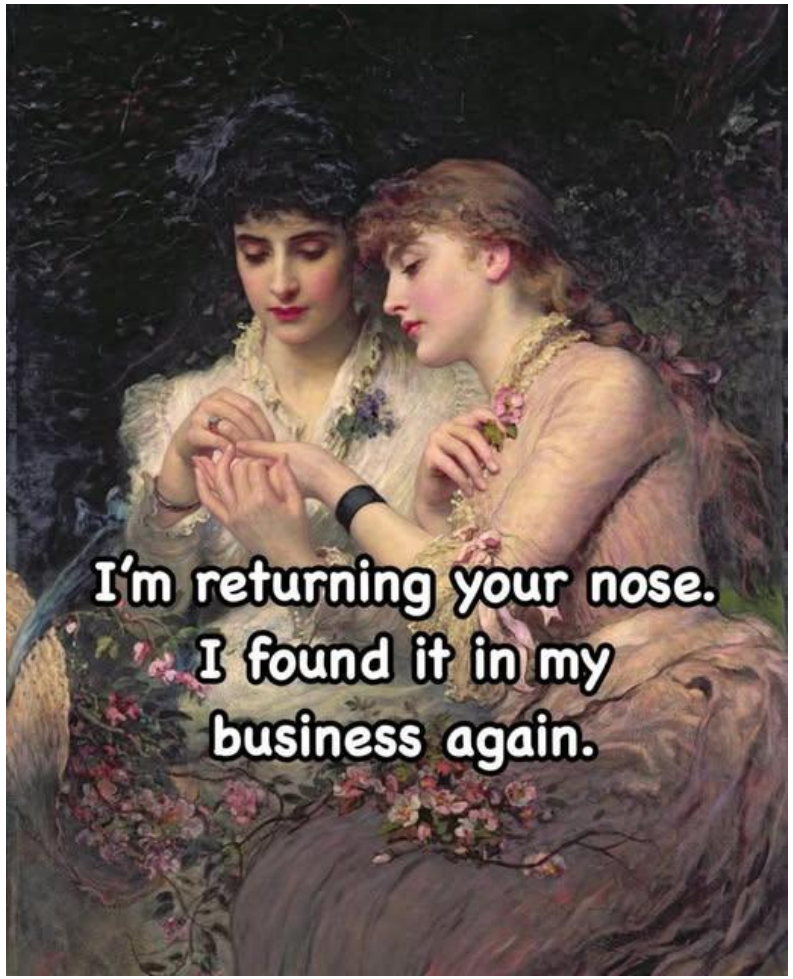
Physical, material or non-material damage

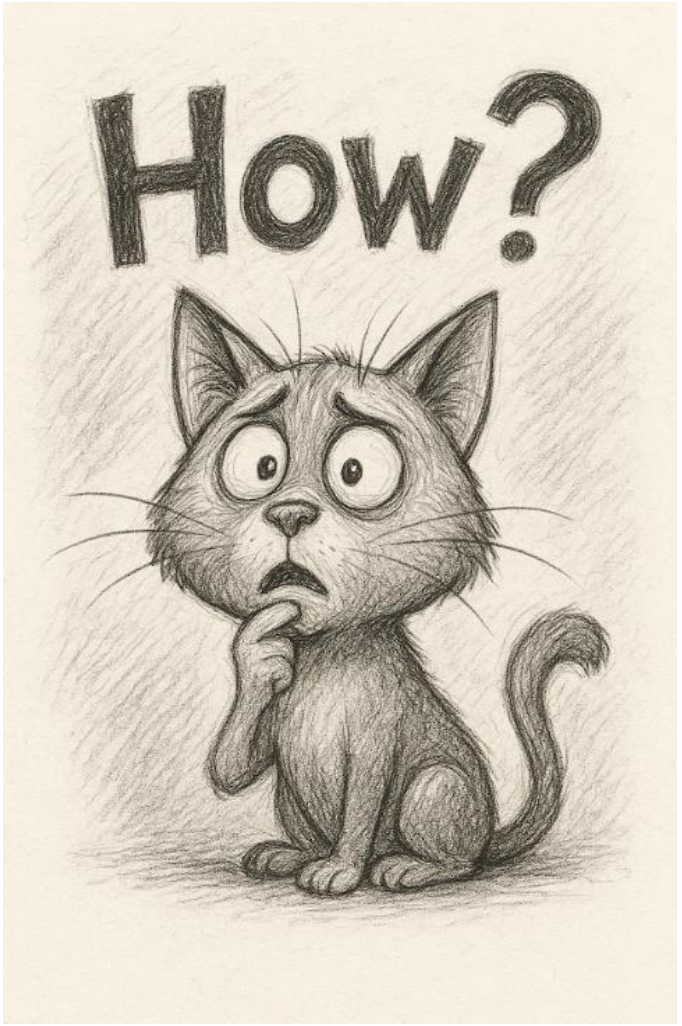
- GDPR: may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality, other significant economic or social disadvantage. Revealing racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life.

- GDPR: where personal aspects are evaluated, in particular analysing or predicting aspects (AI) concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, in order to create or use personal profiles

- The most common non-material damages: unwelcome public exposure, worries, anxiety and the discrimination that comes from it; loss of feeling of security (home address); leaving wrong impression in society (publishing picture where it is not appropriate); treating a person as just a piece of data (reducing someone's identity, individuality, and personal value); and limiting a person's ability to grow and develop their personality etc.

Physical, material or non-material damage





How should we treat personal data?

Steps to take to comply

→ How should we treat personal data? What action should be taken?

- Go to slido.com and:
  - enter the code: #3878 947
  - or scan the QR code

How: extra short ABC

Key requirements for social enterprises:

1. Lawfully collect and process personal data – with consent or another legal basis.
2. Be transparent – explain what data is collected and why (privacy notice).
3. Ensure data security – protect personal data from breaches.
4. Allow rights of data subjects – access, correction, deletion, restriction of processing, and data portability.
5. Report breaches – notify authorities and affected individuals if a breach occurs.

Personal data: beneficiaries or service users; donors and supporters; volunteers and staff; partners or funders etc.

When we can process? A: 6

Consent: of the individual to the processing of their personal data.

Legitimate interest: of the organisation or the third parties engaged.

Contractual necessity: processing is needed in order to enter into or perform a contract.

Legal obligation: for which the organisation is obliged to process personal data for.

Vital interest: of individuals, where processing is necessary to protect their lives.

Public interest: specific to organisations exercising official authority or carrying out tasks in the public interest.

How to process? (Key processing principles: A: 5)

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

1. The lawfulness, fairness and transparency

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')

- Have a valid legal basis (previous slides)
- Must inform the data subject concerned and must be able demonstrating compliance
- Not mislead or exploit individuals, ethical manner (fair)
- Be open and clear about how the data is used; transparency with rules, safeguards and rights regarding the processing (privacy policy, but not only!)

- Example of a breach: An enterprise provides vocational training to unemployed youth. They collect personal information such as names, contact details, and education history. Later, without telling participants, the enterprise sells the email list to a marketing company that sends unrelated advertisements
- An enterprise organises a camp for children living with HIV. Personal data collected: names, health status, pictures. Later, they publish photos of the children publicly without consent.

2. Purpose limitation

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; [..] ('purpose limitation');

- The purpose of processing data must be defined before processing is started
- The processing of personal data for undefined and/or unlimited purposes is thus unlawful.
- There can be no further processing of data in a way that is incompatible with the original purpose
- Every new purpose for processing data which is not compatible with the original one must have its own particular legal basis and cannot rely on the fact that the data were initially acquired or processed for another legitimate purpose

- Example of a breach: An enterprise runs a community food program for low-income families. They collect participants' data: names, addresses, phone numbers, and dietary preferences. Later, they start using the addresses and phone numbers to promote unrelated paid cooking classes without asking participants for consent.

3. The data minimisation principle

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')

- Data must be limited to what is necessary (to fulfil a legitimate purpose)
- Only collect the minimum personal data required for your activities
- Does not request excessive data (like home address or social media profiles, unrelated personal preferences)

- Example of a breach: An enterprise organises a summer camp for children from disadvantaged backgrounds. When parents register their children, the enterprise collects: child's name ✓ Child's age ✓ Parent's phone number ✓ Parent's nationality ☒ Parent's marital status ☒

4. The data accuracy principle

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')

- Data must be reviewed and updated regularly and kept up to date to secure accuracy.
- Collect data carefully – use validation tools or double-entry checks.
- Provide update mechanisms – online forms or contact points to correct data. For example, dedicated email address (e.g. privacy@yourenterprise.org) to request corrections

- Example of a breach: A participant updates their phone number or home address, but the enterprise fails to update the database. As a result, the participant does not receive important program updates or interview invitations or information is received by unrelated person
- A social enterprise creates an online community platform to connect young entrepreneurs. Users' private messages and profiles are indexed by search engines because of poor privacy settings.

5. The storage limitation principle

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; [..] ('storage limitation')

- Time limits should be established by the controller for erasure or for a periodic review (GDPR recital 39) - document how long each data category is kept and the legal or operational reason.
- Should delete or anonymize it when the data is no longer necessary
- Justify exceptions: if you retain data for historical, statistical, or public-interest archiving, ensure safeguards (encryption, limited access) are in place.
- Inform individuals (in your privacy notice) how long their data will be retained and why.

- Example of a breach: An enterprise providing digital skills training to disadvantaged groups collects personal data about: participants (names, contact details, age, background); assessment results; attendance records; feedback forms. The enterprise keeps personal data indefinitely, even for participants who completed training five years ago. No data retention policy is in place, and the files remain fully identifiable — including names, phone numbers, and addresses (It increases risk of unauthorised access, loss, or misuse).

6. The accountability principle

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

- The controller shall be responsible for, and be able to demonstrate compliance with all the principles mentioned before.
- Double-check recipients; use encrypted email for sensitive info; Role-based permissions - staff access only what they need
- Provide regular data protection and security training
- Organisational & technical measures: what can leaders do, and what can machines ensure

- Example of a breach: An enterprise runs a community support and job-matching platform connecting unemployed people with local employers and mentors. They store all data in a cloud database. To make reporting easier, an employee exports the entire database to a spreadsheet and uploads it to a computer disk, which is accessible to people beyond the individuals concerned. Moreover, that system is accessible to external partners, who should not see personal data.

How to process? (Key processing principles: A: 5)

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

Thank you for your attention!