PERSONA impact assessment training (I): basic concepts of I AM PERSONA (the benchmark)

Dariusz KLOZA, Nikolaos IOANNIDIS, Alessandra CALVI, J. Peter BURGESS, Simone CASIRAGHI

Vrije Universiteit Brussel (VUB)
Research Group on Law, Science, Technology & Society (LSTS)
Brussels Laboratory for Data Protection & Privacy Impact Assessments (d.pia.lab)

18 May 2020
online
All about us

- **the Research Group on Law, Science, Technology & Society (LSTS) at the Vrije Universiteit Brussel (VUB), created in 2003**
- works predominantly in English
- ca. 60 full-time researchers
- 5 spin-off’s:
  - Brussels Privacy Hub
  - Privacy Salon
  - Brussels Laboratory for Data Protection & Privacy Impact Assessments (d.pia.lab) (2015)
  - Cyber and Data Security Lab (CDSL)
  - Health and Ageing Law Lab (HALL)
- ERC: COHUBICOL (Counting as a Human Being in the Era of Computational Law)
- policy briefs of **d.pia.lab**
  - 1st (framework) published in May 2017 [EN] [FR] [PT]
  - 2nd (method) published in November 2019 [EN] [FR] [DE] [PT]
  - 3rd (model/template) expected in June 2020 [EN]
<table>
<thead>
<tr>
<th>scheme</th>
<th>H2020</th>
</tr>
</thead>
<tbody>
<tr>
<td>call</td>
<td>H2020-SEC-2016-2017-2</td>
</tr>
<tr>
<td>topic</td>
<td>SEC-18-BES-2017</td>
</tr>
<tr>
<td></td>
<td>Acceptance of no gate crossing point solutions</td>
</tr>
<tr>
<td>duration</td>
<td>01/09/2018 – 28/02/2021</td>
</tr>
<tr>
<td>cost</td>
<td>EUR 2,984,700.-</td>
</tr>
<tr>
<td>aim</td>
<td>developing an impact assessment method tailored to no-gate crossing point solutions</td>
</tr>
</tbody>
</table>
Purpose

- PERSONA end-users are to carry out test studies type C... (T4.4)
- ... and to report therefrom in deliverables D4.3, D4.4 and D4.5 (August 2020)
- the purpose of all the test studies is to check if the I AM PERSONA method (in progress) works
- as a prerequisite, the purpose of this training is to familiarize the PERSONA end-users with the concept of impact assessment
4 on-line sessions @ 2 hours each

- sessions are devoted to each main element of the **architecture** of impact assessment

- **1**st session (18 May 2020): introduction & basic concepts of impact assessment (**benchmark**)
- **2**nd session (20 May 2020): **framework** & **method** for impact assessment
- **3**rd session (25 May 2020): **method** for impact assessment (specific aspects)
- **4**th session (27 May 2020): practical exercise
Agenda 1st session

1. human rights (law)
2. privacy (law)
3. personal data protection (law)
4. border management law
5. ethics
6. societal acceptance

Q&A
Human rights (law)
Human rights

- rights that *every person* has;
- by virtue of merely *existing*; and
- that aim to secure for such a person certain benefits or freedoms that are of *fundamental importance* to any human being (Arosemena 2017)
Human rights

- civil & political rights
  - right to life
  - prohibition of torture*
  - prohibition of slavery & forced labour
  - liberty and security
  - fair trial (due process)
  - privacy (and data protection)
  - freedom of thought, conscience and religion
  - freedom of expression
  - freedom of assembly and association
  - freedom of religion
  - prohibition of discrimination
  - ...

- social rights
  - right to education
  - right to work
  - access to health services
  - ...

- collective rights*
  - development
  - peace
  - environment
  - ...

*Note: Some rights may vary depending on the international agreements and context.
Characteristics

- multiple dimension: law, morality, politics, ...
- justification:
  - ’highest moral precepts and political ideals’ (Moyn 2010)
  - human rights ‘provide benefits that are attractive from any cultural standpoint’ (Arosemena 2017)
- higher (supreme?) legal norms, i.e. other legal norms must conform therewith
- individual rights, against the state (normally)
- positive (‘to do’) vs. negative (‘to refrain’) rights
- majority non-absolute rights, i.e. can be legally interfered with
- multi-layered protection system: global, regional & national
## Protection mechanisms

### United Nations
- Universal Declaration of Human Rights (1948)
- International Covenants (1966)
- Human Rights Council (Geneva, Switzerland)

### European Union
- Charter of Fundamental Rights of the EU (2000/2009)
- Court of Justice of the European Union (Luxembourg)

### Organization of American States
- Inter-American Commission on Human Rights (San Jose, Costa Rica)
- Inter-American Court of Human Rights (San Jose, Costa Rica)

### Council of Europe
- European Convention on Human Rights (1950)
- European Court of Human Rights (Strasbourg, France)
- nb. individual application

### African Union
- African Court on Human and Peoples' Rights (Arusha, Tanzania)

### National
- Bill of rights
  - Constitution (2006) (Serbia)
- National courts
ARTICLE 8

Right to respect for private and family life

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Article 52

Scope of guaranteed rights

1. Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

2. Rights recognised by this Charter which are based on the Community Treaties or the Treaty on European Union shall be exercised under the conditions and within the limits defined by those Treaties.

3. In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection.
Privacy (law)
Why privacy?

http://hasbrouck.org/articles/PNR.html
Dimensions of privacy

- personal zone: solitude
- intimate zone: intimacy
- semi-private zone: secrecy
- public zone: inconspicuousness

Access:
- bodily privacy
- spatial privacy
- communicational privacy
- proprietary privacy

Informational privacy:
- intellectual privacy
- decisional privacy
- associational privacy
- behavioral privacy
Legal protection of privacy as a human right

ARTICLE 8

Right to respect for private and family life
1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Article 7

Respect for private and family life
Everyone has the right to respect for his or her private and family life, home and communications.

Article 8

Protection of personal data
1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.
Privacy in courts of law

- European Court of Human Rights (Strasbourg)
  - Ivashchenko v. Russia (61064/10) (2018)
  - ‘...customs rules on inspecting goods and other regulations had not provided any legal basis for copying electronic data in a laptop. There had been no requirement to assess whether the measure was proportionate and it had been carried out without there being a reasonable suspicion of an offence.’ (press release)

- Court of Justice of the European Union (Luxembourg)
  - the draft EU-Canada PNR agreement ‘could not be concluded in its current form, since it was adopted on the wrong legal basis and several of its provisions were incompatible with fundamental rights’ (Kuner 2018)
  - ‘... the interferences in question are justified by the pursuit of an objective of general interest to ensure public security’ (press release)
  - ‘As regards the necessity of those interferences ... several provisions of the agreement are not limited to what is strictly necessary and do not lay down clear and precise rules’ (press release)
Personal data protection (law)
Preliminary observations

**Data** is a plural of datum, which is originally a Latin noun meaning “something given.”
- Today, data is used in English both as a plural noun meaning “facts or pieces of information” and as a singular mass noun meaning “information”.
- For the purposes of data protection law, ‘data’ is considered a noun in singular.

**GDPR** is a pivotal legislative piece in regulating personal data protection law, but:
- [Law Enforcement Directive 2016/680](#) criminal offences or the execution of criminal penalties
- [Regulation 2018/1725](#) by European Union institutions, bodies, offices and agencies
- [Convention 108 and Protocols](#) (Council of Europe, 55 States Parties in the Convention)
- Sector-specific framework (e.g. Consumer Rights, eCommerce, Unfair Terms)
Serbia & Israel

Serbia

• Within the framework of the Council of Europe, Serbia is party of
  • the European Convention on Human Rights
  • the Convention 108.

• Law on Protection of Personal Data 87/2018
  • Extraterritorial application
  • Data subjects’ rights

Israel

• Council of Europe
  • Observer to the Parliamentary Assembly

• Privacy Protection Act, 5741-1981 (PPA)
  • Chapter B on data protection

• Data Security Law 5777-2017
• Biometric Database Law 5770-2009
Difference between a Regulation, a Directive and Guidelines

EU Regulation:
• Directly applicable and enforceable
• National legislation that defines the competent national authorities, inspection and sanctions on the subject matter.

EU Directive:
• Sets certain aims, requirements and concrete results that must be achieved in every Member State
• National authorities must create or adapt their legislation

Guidelines and best practices:
Article 29 Data Protection Working Party (WP29)
European Data Protection Board (EDPB)
Guidelines of national supervisory authorities (DPAs)
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>DPA</td>
<td>an independent regulatory authority chartered to enforce privacy or data</td>
</tr>
<tr>
<td></td>
<td>protection laws and regulations</td>
</tr>
<tr>
<td>Data processor</td>
<td>organization/individual that processes data on behalf of the data controller</td>
</tr>
<tr>
<td>Data controller</td>
<td>organization/individual with the authority to decide how and why personal</td>
</tr>
<tr>
<td></td>
<td>data about data subjects is to be processed ('means and purposes')</td>
</tr>
<tr>
<td>Data subject</td>
<td>an individual about whom information is being processed</td>
</tr>
</tbody>
</table>
What is “personal data”?

“any information relating to an identified or identifiable natural person”
Any information collected or meant to be collected
- Broad concept of personal data
- Nature / Content / Format

Relationship by content or by purpose or by result

Identified: Direct - person defined by name or characteristics.
Identifiable: Indirect – “by means reasonably like to be used... to identify the natural person”

Existing human being (applicable to a natural person, in principle not to a legal person)
- No post-mortem protection of personal data (Recital 27)
Household exception (Article 2.c + Recital 18)

- a purely personal or household activity
- with no connection to a professional or commercial activity

Examples:
- Correspondence and the holding of addresses on a home PC
- Records relating to family members’ health checks, school reports
- Social networking and online activity undertaken within the context of such activities

Guidelines on video surveillance
The user of video surveillance at home needs to assess:
- Any personal relationship with the data subject
- Whether the scale or frequency of the surveillance suggests some kind of professional activity
- Adverse impact on the data subjects
“any operation performed upon personal data”
GDPR Principles in Processing of Personal Data

Lawfulness, Fairness, Transparency → Purpose limitation

Data minimization, Proportionality → Accuracy

Storage limitation → Confidentiality

Integrity → Accountability
GDPR Principles in Processing of Personal Data

• Accountability / Risk-based approach (Article 5.2)
  • Risk and balance of the organization’s rights to process data against an individual’s right to privacy
  • Prioritize risks, determine and allocate budgets

• Data Protection by design
  • Organisations should build data protection into their products throughout their lifecycles
  • Appropriate technical and organizational measures integrated into the system (e.g. Data minimisation and pseudonymisation)

• Data Protection by default
  • Requires to ensure that one only processes the data that is necessary to achieve a specific purpose
  • Limited accessibility to personal data.
  • Need to specify this data before the processing starts and appropriately inform individuals
  • It does not require to adopt a ‘default to off’ solution
### Controller or Processor

<table>
<thead>
<tr>
<th>Controller</th>
<th>Processor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Human being / legal entity, processing personal data alone or jointly with others</td>
<td>Human being / legal entity, processing personal data on behalf of the controller</td>
</tr>
<tr>
<td>A controller is the one who <strong>determines the purposes and means of processing</strong></td>
<td>On a basis of a <strong>contract</strong></td>
</tr>
<tr>
<td>Has wider legal <strong>obligations</strong>: he shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with GDPR.</td>
<td>Has also accountability obligations</td>
</tr>
</tbody>
</table>
Data Protection Officers (DPOs)

- Not entirely new concept – introduced by the Data Protection Directive 95/46/EC
- GDPR: Data Protection Officer (DPO) a corporate role tasked with facilitating compliance
- Designation of DPO (Art. 37) - Position of DPO (Art. 38) - Tasks of DPO (Art. 39)

- [...] a data protection officer in any case where:
  - the processing is carried out by a public authority or body [...].
  - the core activities [...] processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
  - the core activities [...] processing on a large scale of special categories of data [...]

<table>
<thead>
<tr>
<th>Data Protection Authorities (DPAs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Independent status of the DPAs</td>
</tr>
<tr>
<td>General conditions for the members of the supervisory authority</td>
</tr>
<tr>
<td>Rules on the establishment of the supervisory authority</td>
</tr>
<tr>
<td>Competence, tasks and powers of a DPA</td>
</tr>
<tr>
<td>Activity reports</td>
</tr>
<tr>
<td>Cooperation between DPAs</td>
</tr>
<tr>
<td>European Data Protection Board</td>
</tr>
<tr>
<td>Right to lodge a complaint with a supervisory authority</td>
</tr>
<tr>
<td>Right to an effective judicial remedy against a supervisory authority</td>
</tr>
<tr>
<td>Right to an effective judicial remedy against a controller or processor</td>
</tr>
<tr>
<td>Representation of data subjects</td>
</tr>
<tr>
<td>Suspension of proceedings</td>
</tr>
<tr>
<td>Right to compensation and liability</td>
</tr>
<tr>
<td>General conditions for imposing administrative fines</td>
</tr>
<tr>
<td>Penalties</td>
</tr>
</tbody>
</table>
Data Protection Authorities (DPAs) - Tasks

**In relation to the GDPR**
- monitor and enforce the application of the GDPR
- promote the awareness of controllers and processors of their obligations under the GDPR
- conduct investigations on the application of the GDPR

**In relation to the data subjects**
- provide information concerning the exercise of their rights under the GDPR
- handle complaints

**In relation to controllers and processors**
- encourage the drawing up of codes of conduct
- approve binding corporate rules
- establish and maintain a list in relation to the requirement for data protection impact assessment
<table>
<thead>
<tr>
<th>Data Protection Authorities (DPAs) - Powers</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Investigative powers</strong></td>
</tr>
<tr>
<td>• carry out investigations and review certifications</td>
</tr>
<tr>
<td>• obtain access to any premises of the controller and the processor, including to any data processing equipment and means</td>
</tr>
<tr>
<td><strong>Corrective powers, including to issue substantial fines</strong></td>
</tr>
<tr>
<td>• issue warnings and reprimands for the controller</td>
</tr>
<tr>
<td>• order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation</td>
</tr>
<tr>
<td>• <strong>impose an administrative fine</strong></td>
</tr>
<tr>
<td><strong>Authorization and advisory powers</strong></td>
</tr>
<tr>
<td>• authorize model Clauses and binding corporate rules</td>
</tr>
</tbody>
</table>
Article 6 - Lawfulness of processing

Processing shall be lawful only if and to the extent that at least one of the following applies:

- Consent
- Legitimate interest
- Legal Bases (six grounds)
- Legal obligation
- Contractual necessity
- Protection of vital interests
Conditions for Consent

- Freely given
- Specific
- Informed
- Unambiguous
- Indication of wishes
- Easy withdrawal
Special Categories of data

Processing of personal data revealing

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data for the purpose of uniquely identifying a natural person
- data concerning health
- data concerning a natural person’s sex life
- sexual orientation

Explicit consent
Employmen t context
Vital interests
Not-for-profit purposes
Public available data
Public interest
Legal claims
Research and Statistics
Public health

Processing is prohibited unless
Data subject’s rights
Information to be provided prior to the processing (≈Privacy Policy)

• the identity [...] of the controller [...] 
• the contact details of the data protection officer 
• the purposes of the processing [...] the legal basis for the processing 
• the legitimate interest(s), [...] 
• the recipients [...] of the personal data, if any 
• [...] intends to transfer personal data to a third country 
• the period for which the personal data will be stored 
• the existence of the right to request [...] access to and rectification or erasure [...] or restriction of processing concerning the data subject or to object to processing [...] the right to data portability; 
• [...] the existence of the right to withdraw consent at any time 
• the right to lodge a complaint with a supervisory authority; 
• the existence of automated decision-making, including profiling and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
Example of prior information to data subjects

GOOGLE PRIVACY POLICY

When you use our services, you’re trusting us with your information. We understand this is a big responsibility and work hard to protect your information and put you in control.

This Privacy Policy is meant to help you understand what information we collect, why we collect it, and how you can update, manage, export, and delete your information.

Effective January 22, 2019  Archived versions  Download PDF
Right of access (Article 15)

Data subjects shall have access to:

• The source of the personal data.
• A copy of the personal data that is being processed in the same form in which the request was made.
• Confirmation of processing.
• Processing information: what / who / where / when / why
• Existence of automated decision-making
• Meaningful information about the logic involved
• Significance and envisioned consequences of the processing
Exercising the right of access against Facebook

Personal data requests

Download your info

To download a copy of your Facebook data:
1. Click « at the top right of any Facebook page.
2. Choose Account settings.
3. Click Download a copy of your Facebook data at the bottom of the page.

Most of your data is available to you when you log in to your Facebook account. For example, you can look at your Timeline to see posts you’ve shared and photos you’ve been tagged in, while Messages contains your chat history.

You can also go to your Activity Log to see a history of actions you have taken on Facebook. This includes posts you have liked or commented on, apps you have used, and anything you’ve searched for.

This doesn’t answer my question

Send
Exercising the right of access against Twitter

Where can I find my Twitter data?

If you are logged into Twitter on the web, you can also:

1. Click your profile icon in the top right navigation bar.
2. Select Settings and privacy from the drop-down menu.
3. From the menu on the left, click Your Twitter data.
4. Enter your password and click Confirm.

If you do not have a Twitter account, can also go to Twitter.com and click the Personalization link at the bottom of the page. From there you can access your Personalization and Data settings as well as your Twitter data.

On Twitter for Android or iPhone:

1. Go to your account settings.
2. Underneath your Personalization and data settings, you’ll see a link to Your Twitter data.
3. Tap the Your Twitter data link.
Schengen access rights

Schengen Information form (www.ip-rs.si) Request for Information on Data in the Schengen Information System in Slovenia


1. Information about me:
First name: ___________ Last name: ___________ Address (street, town, postal code): ___________ Date of birth: ___________
Place of birth: ___________ Nationality: ___________

Information: These data serve as identifiers to search the SIS database reliably for data relating to you, and to mail the information to you. Please make sure the spelling is correct and avoid mistakes. The data you give here are not going to be additionally stored in SIS. Only the fact that the SIS has been searched for your data is recorded in the system’s log files.

2. Further information relating to this request (please mark with a cross [x]):

Information: The following information is voluntary and helps to speed up the process.

[ ] I was refused a Slovene Visa, a residence permit or a permanent residence permit [ ] [ ] I was refused entry to Slovenia at the following border control station ___________ [ ] Other: ___________

Place and date: Signature:

APPEAL

The Slovenian body competent to rule on the appeal submitted by an individual whose request to review personal data pertaining to him/her has either been refused or unanswered, shall be the Information Commissioner, which shall also be competent to perform the supervision over implementation of the right to correct incorrect data or delete illegal personal data in Slovenia. Address: Information Commissioner, Zaloška 59, 1000 Ljubljana. Telephone: 01 230 97 30, fax: 01 230 97 78, e-mail: gp.ip@ip-rs.si, web page: http://www.ip-rs.si.
Right to Rectification (Article 16)

- Correction
  - Objectively incorrect
  - Subjectively correct
- Completion
- Close links to the accuracy principle of the GDPR (Article 5(1)(d))

Limitations

- Identification of the requester
- Protection of others’ rights and freedoms
- Purpose of the request
Data portability (Article 20)

Extension of access right:
✓ Structured, commonly used and machine-readable
✓ Interoperable
✓ Transfer to data subject, or another controller or a third party

Application: three cumulative conditions
✓ Personal data processed by automatic means based on consent or contact
✓ Personal data concerning and from the data subject
✓ Not adversely affecting the rights and freedom of the others
Right to erasure (‘right to be forgotten’) (Article 17)

Obligation to erase personal data without undue delay

(a) the personal data are no longer necessary [...] 
(b) the data subject withdraws consent [...] and where there is no other legal ground for the processing 
(c) the data subject objects [...] and there are no overriding legitimate grounds for the processing [...] 
(d) the personal data have been unlawfully processed 
(e) [...] erased for compliance with a legal obligation in Union or Member State law [...] 
(f) the personal data have been collected in relation to children

Google Spain case: Request to Google to delete outdated information regarding financial difficulties about the applicant from its search list results

- Google claimed it merely provides a hyperlink to the publisher’s web page
- While indexing content Google becomes a data controller to which responsibilities and obligations under EU law apply
- The right to have one’s personal data erased when the processing is outdated or no longer necessary also covers data controllers that replicate the information
Right to restriction of processing (Article 18)
- Accuracy
- Unlawfulness
- Not necessary
- Objection to processing
- Prior information before lifting the restriction

Right to object to processing (Article 21)
- Unless public/legitimate interests
- Unless research/statistical purposes
- Absolute right with regards to direct marketing
Automated individual decision-making, including profiling

Right not to be subject to a decision based:

- solely on automated processing, including profiling which produces legal effects concerning him or her or similarly significantly affects him or her

Exceptions:

- necessary for [...] a contract
- authorized by Union or Member State law to
- based on explicit consent

In case of the exceptions the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least:

- the right to obtain human intervention on the part of the controller,
- to express his or her point of view and
- to contest the decision
- (a right to explanation)
Definition Data minimisation - Article (5.1.c)

Data collected and processed should not be held or further used.

In the GDPR this is defined as data that is:

- **Adequate** – sufficient to properly fulfil your stated purpose
- **Relevant** – has a rational link to that purpose
- **Limited** – to what is necessary for the purposes for which they are processed.

Questions when collecting data:

- Does the individual know that I am collecting the data and why?
- How am I planning to use this data?
- Is there a way of achieving this purpose without having to collect the data?
- How long will I need the data for to achieve the purpose?
### What is “anonymous data”?### What is “pseudonymous data”?

<table>
<thead>
<tr>
<th>“any information not related to an identified or identifiable natural person”</th>
<th>“any information not fully anonymous”.</th>
</tr>
</thead>
<tbody>
<tr>
<td>“any information rendered unidentifiable”</td>
<td>“any process that detaches the aspects of the data attributed to a specific individual”</td>
</tr>
<tr>
<td>“any information not considered personal data under the GDPR”</td>
<td>“any security measure that makes the use of the data less risky”</td>
</tr>
<tr>
<td></td>
<td>“any information subject to data protection law”</td>
</tr>
</tbody>
</table>
The WP29 has identified the following 7 techniques that can be used to anonymize records of information:

- **Noise Addition**: The personal identifiers are expressed imprecisely (e., weight is expressed inaccurately +/- 10 lb).

- **Substitution/Permutation**: The personal identifiers are shuffled within a table or replaced with random values (e., a zip code of 80629 is replaced with “Magenta”).

- **Differential Privacy**: The personal identifiers of one data set are compared against an anonymized data set held by a third party with instructions of the noise function and acceptable amount of data leakage.

- **Aggregation/K-Anonymity**: The personal identifiers are generalized into a range or group (e., a salary of $42,000 is generalized to $35,000 - $45,000).
• **L-Diversity**: The personal identifiers are first generalized, then each attribute within an equivalence class is made to occur at least “l” times. (e., properties are assigned to personal identifiers, and each property is made to occur with a dataset, or partition, a minimum number of times).

• **Pseudonymization – Hash Functions**: The personal identifiers of any size are replaced with artificial codes of a fixed size (e., Paris is replaced with “01”, London is replaced with “02”, and Rome is replaced with “03”).

• **Pseudonymization – Tokenization**: The personal identifiers are replaced with a non-sensitive identifier that traces back to the original data, but are not mathematically derived from the original data (i.e., a credit card number is exchanged in a token vault with a randomly generated token “958392038”).
From personal to anonymous data

**Personally Identifiable Data**
Data that contains personal direct and indirect identifiers.

High Re-identification Risk

**Pseudonymous Data**
Data from which identifiers are replaced with artificial identifiers, or pseudonyms, that are held separately and subject to technical safeguards.

Remote Re-identification Risk

**De-Identified Data**
Data from which direct and indirect identifiers have been removed.

Residual Re-identification Risk

**Anonymous Data**
De-Identified Data where technical safeguards have been implemented such that data can never be re-identified.

Zero Re-identification Risk

Source: Bryan Cave (www.bclplaw.com)
Border management law
EU Border management law

Structure

- Overview EU framework and actors
- Relevance for IAM PERSONA and Test Studies type C
EU Border management law

Overview

- Primary Law: EU Treaties (TEU and TFEU)
- Secondary law
  - Rules on passports and ID
  - EU large-scale databases (interoperability)
  - Other systems exchanges of information (e.g. Prüm Treaty, PNR, API)
  - Border practices (e.g. SBC)
- Actors (e.g. national police, euLISA, Frontex)
EU Border management law

Principles

- Internal frontiers (AFSJ) vs External frontiers
- EU Citizens vs Non-EU Citizens
### Existing and planned EU large-scale IT systems

<table>
<thead>
<tr>
<th>IT system</th>
<th>Main purpose</th>
<th>Persons covered</th>
<th>Applicability</th>
<th>Biometric identifiers</th>
</tr>
</thead>
<tbody>
<tr>
<td>European Trantypography (Eurodac)</td>
<td>Determine the Member State responsible to examine an application for international protection. Assist with the control of irregular immigration and secondary movements.</td>
<td>Applicants and beneficiaries of international protection, migrants in an irregular situation</td>
<td>18 EUMS + SAC</td>
<td></td>
</tr>
<tr>
<td>Visa Information System (VIS)</td>
<td>Facilitate the exchange of data between Schengen Member States on visa applications.</td>
<td>Visa applicants and sponsors</td>
<td>24 EUMS (Ee, GR, HR, IE, UK) + SAC</td>
<td></td>
</tr>
<tr>
<td>Schengen Information System (SIS II) - police</td>
<td>Safeguard security in the EU and Schengen Member States</td>
<td>Missing or wanted persons</td>
<td>16 EUMS (not CY, IE) + SAC</td>
<td></td>
</tr>
<tr>
<td>Schengen Information System (SIS II) - borders</td>
<td>Enter and process alerts for the purpose of refusing entry into or stay in the Schengen Member States.</td>
<td>Migrants in an irregular situation</td>
<td>25 EUMS (not CY, IE, UK) + SAC</td>
<td></td>
</tr>
<tr>
<td>Schengen Information System (SIS II) - return</td>
<td>Enter and process alerts for third-country nationals subject to a return decision</td>
<td>Migrants in an irregular situation</td>
<td>25 EUMS (not CY, IE, UK) + SAC</td>
<td></td>
</tr>
<tr>
<td>Entry Exit System (EES)</td>
<td>Calculating and monitoring the duration of authorized stay of third-country nationals admitted and identify over-stayers</td>
<td>Travellers coming for a short-term stay</td>
<td>22 EUMS (not BG, CY, HR, ES, RO, UK) + SAC</td>
<td></td>
</tr>
<tr>
<td>European Border Information and Authorisation System (EBAAS)</td>
<td>Assess if a third-country national who does not need a visa poses a security, irregular migration or public health risk.</td>
<td>Visa free travellers</td>
<td>26 EUMS (not CY, DE) + SAC</td>
<td></td>
</tr>
<tr>
<td>European Criminal Records Information System for Third-Country Nationals (ECRIS-TCON)</td>
<td>Share information on previous convictions of third-country nationals.</td>
<td>Third-country nationals with a criminal record</td>
<td>27 EUMS (not DK)*</td>
<td></td>
</tr>
<tr>
<td>Intraoperability - Common Identity Repository</td>
<td>Establish a framework for interoperability between EES, VIS, ECRIS, EIS, EIS II and ECRIS-TCON</td>
<td>Third-country nationals covered by Eurodac, VIS, SIS II, EIS, EIS II, and ECRIS-TCON</td>
<td>28 EUMS + SAC</td>
<td></td>
</tr>
</tbody>
</table>

EU Border management law – Interoperability

Fields

- **borders and visa** (EES, VIS, ETIAS and SIS)
  
- **police and judicial cooperation, asylum and migration** (Eurodac, SIS and ECRIS-TCN)
EU Border management law – Interoperability

EU Border management law – Interoperability

Data protection challenges

- biometrics
- purpose limitation → function creep
- data minimization
- GDPR or LED?
- ...

VUB | LSTS | LAW, SCIENCE, TECHNOLOGY & SOCIETY RESEARCH GROUP
Fundamental rights challenges

- overlap law enforcement and border control
- fairness towards non-EU nationals
- ...

EU Border management law – Interoperability
New border practices

- third-country nationals subject to thorough checks against databases (EU, national, Interpol etc.)
- self-service systems for border checks, e-gates
- Automated border control systems designed in a way:
  - to be used by all persons (except children under 12)
  - that fully respects human dignity, in particular in cases involving vulnerable persons.
- ...
EU Border management law – Border Practices

New technical requirements

- Standards for biometrics (and error rates)
- Compatibility of National Interfaces and Central Systems
- Data security
- Data availability
- ...

[Logos and branding]
EU Border management law – Relevance for the IAM PERSONA

Legal requirements of no gate crossing solutions

- Respect of fundamental rights
- Compliance with data protection rules
- Compliance with technical and security provisions
- Compliance with border management practices
(5) Ethics
Overview

i. Basic concepts of ethics

ii. The PERSONA ethics base-line principles

iii. The PERSONA ethics requirements
i. Basic concepts of ethics

What is normative ethics?
What is applied ethics?
ii. The PERSONA base-line principles

Autonomy
Do no harm
Justice
Explicability
ii. The PERSONA base-line principles

- Autonomy
- Do no harm
- Justice
- Explicability
iii. The PERSONA ethics requirements

- Autonomy
  - Do no harm
- Justice
- Explicability

- Informed consent
- Respect of freedoms
- Identity
  - Dual use and misuse
  - Technical robustness and safety
  - Privacy and data protection
  - Equality
  - Accessibility
  - Accountability
  - Transparency
  - Legal due diligence
iii. The PERSONA ethics requirements

- Autonomy
- Do no harm
- Justice
- Explicability

- Informed consent
- Respect of freedoms
- Identity
- Dual use and misuse
- Technical robustness and safety
- Privacy and data protection
- Equality
- Accessibility
- Accountability
- Transparency
- Legal due diligence
iii. The PERSONA ethics requirements

- Autonomy
- Do no harm
- Justice
- Explicability

Informed consent
Respect of freedoms
Identity
Dual use and misuse
Technical robustness and safety
Privacy and data protection
Equality
Accessibility
Accountability
Transparency
Legal due diligence
iii. The PERSONA ethics requirements

**Autonomy**

**Do no harm**

**Justice**

**Explicability**

- Informed consent
- Respect of freedoms
- Identity
- Dual use and misuse
- Technical robustness and safety
- Privacy and data protection
- Equality
- Accessibility
- Accountability
- Transparency
- Legal due diligence
iii. The PERSONA ethics requirements

For further details:

D1.3 PERSONA benchmark for the assessment process:

Chap 5 Ethical requirements
Social acceptance
How to distinguish social acceptance from ethics?
Social acceptance & ethics

- subjective perceptions and emotional states
- shared human values and ethical principles of society

Bridging the Gap between Social Acceptance and Ethical Acceptability

Behnam Taebi²

Social acceptance refers to the fact that a new technology is accepted—or merely tolerated—by a community. Ethical acceptability refers to a reflection on a new technology that takes into account the moral issues that emerge from its introduction.
Social acceptance and ethical acceptability are complementary:

- **Social acceptance studies** do not capture all the morally relevant features of (emerging) technologies

- **Ethical analyses** do not include stakeholders’ opinions, lack empirical input
How is social acceptance (of technology) assessed?

• In the 1980s:
  • computers entered in people's homes and workplaces
  • “usability” and “utility” were the main features for assessing the user-friendly character of the novel devices

• Since the 1990s:
  • with the “technology acceptance research” social acceptance has become a separate and autonomous field for assessing the performance of emerging technologies referring to the psychological, social, cultural, ethical models behind the human-technology interaction
Technology acceptance model (TAM)

- TAM:
  - Different models
  - To predict information technology acceptance and usage on the job

- Unified theory of acceptance and use of technology (UTAUT):
  - Comprehensive framework
  - To predict behavioural intention for the adoption of technology

- PERSONA: UTAUT inspires part of the impact assessment method (to be discussed in session 3: public participation)
Why focusing on social acceptance in PERSONA?
SEC-18-BES-2017 - Acceptance of no gate crossing point solutions

For the traveller it would be ideal to cross borders without being slowed down. It is indeed likely that, in the next 10 years or so, technologies make it possible to implement "no gate crossing point solutions" that allow for seamless crossing of borders and security checks for the vast majority of travellers who meet the conditions of entry, and make sure that those who do not fulﬁl such conditions are refused entry.

There is a broad variety of technologies and systems including information systems and (networks of) sensors that will become available to support border checks based on risk-assessment methods. Some are to be deployed in the vicinity of border crossing points, others can be mobile and used to check travellers data along his/her journey.

However, in the intensive use of technologies that this will require bears the risk to invading people’s privacy, and the societal and political acceptance of technologies for “no gate solutions” is required prior to their implementation.

- Information systems that better manage personal information and support the automated checking and analysing of various entry and exit data, without increasing the risk of loss of privacy thanks to close cooperation with actions resulting from SEC-15-BES–2017: Risk-based screening at border crossing.
- Networks of sensors that better collect information needed for border checks, without increasing the risk of loss of privacy thanks to close cooperation with actions resulting from SEC-15-BES–2017.
- A method, and metrics, to assess acceptability by the society of the concept of border control processes based on "no gate crossing point solutions", and of the various technology components that may be required.
✓ Social acceptance is not just an obstacle to technological deployment!

✓ The question to ask is ALSO why a technology is not accepted, and not merely how to ensure it is accepted

✓ Social acceptance is necessary, but not sufficient when deciding on new technologies to deploy
  • E.g. Facial recognition technologies
How will you assess social acceptance? (to be continued...)

✓ Social acceptance can be assessed with an appropriate stakeholder participation phase (to be discussed in session 3: public participation)

✓ NB: These perceptions can vary greatly for different groups of people, e.g. technologies can facilitate border crossing for some people but not for others
To sum up: benchmark requirements

1) human rights
2) privacy (law)
3) personal data protection (law)
4) border management law
5) ethics
6) societal acceptance

These are the requirements against which you need to assess a given technology.

How to assess? Impact assessment method (Next session, May 20 2020)
Thank you!

dariusz.kloza@vub.be
simone.casiraghi@vub.be
alessandra.calvi@vub.be
nikolaos.ioannidis@vub.be
james.peter.burgess@vub.be

LSTS.research.vub.be
dpialab.org
@dpialab