PERSONA training on impact assessment

18 – 20 – 25 – 27 May 2020
13:30 – 15:30 (Brussels time)

29 May 2020

Table of Contents

1 Agenda

Note: Attendance mandatory for partners: MOPS-INP, SMOI and SPA.

Language of instruction: English.

Time	Description	Presenters
Session 1 18 May 2020 13:30-15:30	**Introduction** ▪ the objectives of the training session **Basic concepts of I AM PERSONA (the benchmark)** ▪ human rights ▪ privacy (law) ▪ personal data protection (law) ▪ border management law ▪ ethics ▪ societal acceptance Q&A	 DK DK DK NI AC PB SC
Session 2 20 May 2020 13:30-15:30	**Introduction to impact assessment** ▪ the concept (context, rationale, history, architecture) ▪ overview of the framework (conditions and principles) ▪ overview of the method ▪ integration of impact assessment Q&A	 SC DK AC SC
Session 3 25 May 2020 13:30-15:30	**The method for the assessment of impacts in I AM PERSONA (specific aspects)** ▪ Step 5: assessment methods: ○ risk assessment ○ necessity & proportionality assessment ▪ Step 7: public participation (stakeholder involvement) Q&A	 DK AC & NI SC
Session 4 27 May 2020 13:30-15:30	**Practical session: conducting the process of impact assessment on a new border-crossing technology** **Wrap up & conclusion**	 all DK

The training will be provided by J. Peter Burgess, Alessandra Calvi, Simone Casiraghi, Nikolaos Ioannidis and Dariusz Kloza.

2 Reading materials

2.1 Compulsory readings

a) SESSION ONE (18/05/2020): Basic concepts of the IAM PERSONA (benchmark)

- Fundamental rights and border control
  - Arosemena G. (2017) *Human Rights*, In: Hage J., Waltermann A., Akkermans B. (eds.) *Introduction to Law*. Springer, Cham, https://doi.org/10.1007/978-3-319-57252-9_13
  - Council of Europe (nd.), *Human rights teaching resources*, Strasbourg, https://echr.coe.int/Documents/Pub_coe_Teaching_resources_ENG.pdf
  - Galdon Clavell, G. (2017) *Protecting rights at automated borders*, Nature, Vol. 543, https://www.nature.com/news/protect-rights-at-automated-borders-1.21543
- Privacy law and personal data protection law
  - Hildebrandt, M. (2019) *Law for Computer Scientists and Other Folk*. Oxford: Oxford University Press. **Chapter 5**: *Privacy and Data Protection*, pp. 125-196, http://fdslive.oup.com/www.oup.com/academic/pdf/openaccess/9780198860884.pdf
- Ethics of biometrics
  - Fieser, J. (nd.) *Ethics*, Internet Encyclopedia of Philosophy, https://www.iep.utm.edu/ethics/
  - Biometrics Institute (2019) *Ethical Principles for Biometrics*, https://www.biometricsinstitute.org/wp-content/uploads/Biometrics-Institute-Ethical-Principles-Final_1019.pdf
- Social acceptance of technology
  - Taebi, B. (2017). *Bridging the Gap between Social Acceptance and Ethical Acceptability, Risk Analysis,* 37(10), 1817–1827, **Section 2**, https://www.onlinelibrary.wiley.com/doi/10.1111/risa.12734
- Border management law
  - European Parliament. (2019) *Management of the external borders*, https://www.europarl.europa.eu/ftu/pdf/en/FTU_4.2.4.pdf

b) SESSION TWO (20/05/2020): Introduction to impact assessment

- Kloza, D., van Dijk, N., Gellert, R., Böröcz, I., Tanas, A., Mantovani, E. and Quinn, P. (2017) "Data Protection Impact Assessments in the European Union: Complementing the New Legal Framework towards a More Robust Protection of Individuals. *d.pia.lab Policy Brief 1/2017,* VUB: Brussels, https://cris.vub.be/en/publications/data-protection-impact-assessments-in-the-european-union-complementing-the-new-legal-framework-towards-a-more-robust-protection-of-individuals(ce786e1a-75f3-4839-8f82-7f1b2f35a8eb).html (also available in FR, PT)
- Kloza, D., van Dijk, N., Casiraghi, S., Vazquez Maymir, S., Roda, S., Tanas, A., Konstantinou, I. (2019) Towards a method for data protection impact assessment: Making sense of the GDPR requirements. *d.pia.lab Policy Brief No. 1/2019*, VUB: Brussels, https://cris.vub.be/en/publications/towards-a-method-for-data-protection-impact-assessment-making-sense-of-gdpr-requirements(f5c069e6-5c06-48e9-ae07-a244c4b1e3ca).html (also available in FR, DE, PT, CA)

- Kloza, D., van Dijk, N., Casiraghi, S., Vazquez Maymir, S., Tanas, A., Konstantinou, I. *et al.* (2020) Towards a model for the process of data protection impact assessment for the European Union, *d.pia.lab Policy Brief No. 1/2020*, VUB: Brussels (draft)
- Article 29 Working Party (2017) *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, WP248 rev. 01, Brussels, http://ec.europa.eu/newsroom/document.cfm?doc_id=47711

c) SESSION THREE (25/05/2020): Specific aspects of the method for impact assessment:

- **Assessment methods**
  - International Organization for Standardization (ISO), *Risk management – Guidelines*, ISO 31000:2018, Geneva, https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en
  - European Data Protection Supervisor (2020) *The EDPS quick-guide to necessity and* proportionality, https://edps.europa.eu/sites/edp/files/publication/20-01-28_edps_quickguide_en.pdf
- **Public participation**
  - Mays, C. (2004) *Stakeholder Involvement Techniques. Short Guide and Annotated Bibliography*. Organisation for Economic Co-operation and Development (OECD), Paris, **pp. 7-11**, http://www.oecd-nea.org/rwm/reports/2004/nea5418-stakeholder.pdf

d) SESSION FOUR (27/05/2020): Practical session

- Dossier on practical case study (cf. *infra*, Sect. 4)

2.2 Optional readings

a) The concept of impact assessment

- Clarke, R., 2009. *Privacy impact assessment: Its origins and development*. Computer Law & Security Review 25, pp. 123–135: https://www.sciencedirect.com/science/article/abs/pii/S0267364909000302?via%3Dihub
- Reisman D., Schultz J., Crawford K., Whittaker M., (2018) *Algorithmic impact assessments: a practical framework for public agency accountability*, https://ainowinstitute.org/aiareport2018.pdf

b) Benchmark

➢ **Fundamental rights and border control**

- Frontex (2013). *Fundamental Rights Training for Border Guards*, https://frontex.europa.eu/assets/Publications/Training/Fundamental_Rights_Training_for_Border_Guardsl.pdf
- Fundamental Rights Agency (2018). *Under watchful eyes – biometrics, EU IT-systems and fundamental rights.* Luxembourg: Publications Office of the European Union, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-biometrics-fundamental-rights-eu_en.pdf

- Fundamental Rights Agency (2018). *Preventing ulawful profiling today and in the future: a guide*. Luxembourg: Publications Office of the European Union, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-preventing-unlawful-profiling-guide_en.pdf
- Fundamental Rights Agency (2019). *Facial recognition technology: fundamental rights considerations in the context of law enforcement.* Luxembourg: Publications Office of the European Union, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper.pdf
- European Parliament (2019), Briefing, Interoperability between EU border and security information systems, https://www.europarl.europa.eu/RegData/etudes/BRIE/2018/628267/EPRS_BRI(2018)628267_EN.pdf

➢ **Privacy law and personal data protection law**

- Fundamental Rights Agency and Council of Europe (2018). *Handbook on European Data Protection Law*. Luxembourg: Publications Office of the European Union (also available in DE, FR, HU, IT, ES, BG, EL, KA, PL) https://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf
- European Court of Human Rights (2020), Factsheet – New technologies, https://echr.coe.int/Documents/FS_New_technologies_ENG.pdf
- European Court of Human Rights (2020), Factsheet – Personal data protection, https://echr.coe.int/Documents/FS_Data_ENG.pdf

➢ **Ethics of technology**

- High Level Group on Artificial Intelligence (2019). *Ethics Guidelines for Trustworthy AI*, https://ec.europa.eu/futurium/en/ai-alliance-consultation
- European Data Protection Supervisor Ethics Advisory Group (2018). *Towards a digital ethics*, https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf

➢ **Social acceptance of technology**

- Pew Research Center (2019) *More Than Half of U.S. Adults Trust Law Enforcement to Use Facial* Recognition *Responsibly*, https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2019/09/09.05.19.facial_recognition_FULLREPORT_update.pdf
- Venkatesh, V., Morris, M. G., Davis, G. B., Davis, F. D. (2003). User acceptance of information technology. *MIS Quarterly*, *27*(3), 425–478, http://www.vvenkatesh.com/wp-content/uploads/2015/11/2003(3)_MISQ_Venkatesh_etal.pdf

c) Appraisal techniques

➢ **Risk analysis**

- Society for Risk Analysis (SRA) (2018). Society for Risk Analysis Glossary, https://www.sra.org/sites/default/files/pdf/SRA%20Glossary%20-%20FINAL.pdf
- Aven T. (2016) *Risk assessment and risk management: Review of recent advances on their foundation,* European Journal of Operational Research, Volume 253, Issue 1, 16 August 2016, pp. 1-13, https://www.sciencedirect.com/science/article/pii/S0377221715011479

- **Necessity and proportionality**
  - European Data Protection Supervisor (2017) *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A toolkit*, Brussels, https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf
  - European Data Protection Supervisor (2019) *Assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data*, Brussels, https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf

d) Stakeholder involvement

- Creighton, J. L. (2005). The Public Participation Handbook. Making Better Decisions Through Citizens Involvement. New York: Wiley Publisher,: https://smartnet.niua.org/sites/default/files/resources/Public%20Participation%20Handbook.pdf
- Arnstein, S. R. (1969). A Ladder of Citizen Participation. *Journal of American Planning Association*, 35(4), 216-224, https://www.participatorymethods.org/sites/participatorymethods.org/files/Arnstein%20ladder%201969.pdf

3 Case-study

IAM PERSONA practical exercise: iBorderCtrl project

27 May 2020

The context: Horizon 2020 "Secure Societies Programme"[1]

In 2013, the European Commission invested some 1,6 billion euros for the **Research Programme "Secure Societies – protecting freedom and security of Europe and its citizens"**. The objective of this programme is to increase the security and freedom in Europe from threats and challenges that are increasingly affecting its citizens, such as crime, violence, terrorism, illegal trafficking, cyber-attacks or natural disasters. In order to anticipate and prevent these threats, it is considered necessary to understand their causes and develop innovative solutions to ensure individuals' rights and freedoms are respected. Technologies and creative design can be solutions to such problems. However, such solutions should also keep in mind whether the means are necessary and proportional in a democratic society, and whether they are socially acceptable by the larger public.

The actions of the programme have integrated the demands of different end-users, from citizens to businesses, civil society organizations, law enforcement, border guards, etc. One of the focuses has been, among others, on strengthening security through innovative border management technologies.

The specific call[2]

The project **iBorder Ctrl (*Intelligent Portable Control System*, 2016-2019)**[3] has been co-funded in the call **BES-05-2015 Border crossing point topic 1: Novel concepts for land and border security**. The specific challenge of the call has been to secure land borders of the EU/Schengen areas from external threats, where in recent years there has been a significant increase in travellers' flows.

At the same time, there is a need to ensure fast and convenient border crossing of (low-risk) travellers. Since the current infrastructure for land borders is not very flexible, new user friendly and reliable technological solutions need to be developed to maximize security measures (and minimize risks thereof), while facilitating border crossing. Examples of these solutions are mobile devices for border guards for identity checks, both inside vehicles as well as on pedestrians. These devices have to be equipped, to improve accuracy, with **biometric identification** systems (i.e. identification of travellers through the processing of biometric data, like fingerprints or iris).

The objective of the project[4]

The aim of iBorderCtrl was to enable faster and thorough border control for third country nationals crossing the land borders of EU Member States: road, walkway, train stations. Its products to be developed and tested included software and hardware technologies, ranging from portable readers and scanners, various emerging and novel subsystems for automatic controls, highly reliable wireless networking for mobile controls, and secure backend storage and processing.

The projects' specific objectives were:

- To **significantly increase the efficiency in terms of traveller throughput** at the border as well as security in terms of significantly fewer successful illegal crossings;

[1] Cf.: https://cordis.europa.eu/programme/id/H2020-EU.3.7
[2] Cf.: https://cordis.europa.eu/programme/id/H2020_BES-05-2015
[3] https://www.iborderctrl.eu/
[4] Cf.: https://www.iborderctrl.eu/

- To achieve greater comfort, **reduced time at the border** by utilising the portable traveller devices and portable units;
- To utilize **pre-registration step** as a means to better inform travellers of their rights, the procedures they will have to go through for their travel, the data collected and how they are analysed as per EU and national legal requirements and to obtain, were necessary, an informed consent from the traveller;
- To **reduce the subjective control and workload of human agents and to increase the objective control** with automated means that are non-invasive and do not add to the time the traveller has to spend at the border;
- To **create of a fifth tier** for the four-tier[5] access control model of the Integrated Border Management System involving bona fide travellers, especially regular travellers into a Schengen-wide frequent traveller programme including a reward system based on number of successful crossings and trouble-free stay.

In short, the main objective was to employ existing and proven technologies as well as novel ones in a way to **increase both the accuracy** (sensitivity – the ability of border agents to identify problematic crossings that should be halted, and specificity – their ability to identify valid crossings) and **efficiency** (throughput while reducing the average cost to travellers, in terms of time and stress) of border checks.

Public critiques

In the fall of 2018, the project was criticized by the press[6] and some civil society organizations (like Homo Digitalis in Greece).[7] Most criticisms were focused on one particular module, among the many developed, of the project, namely the **Automated Deception Detection System (ADDS)**. In short, the systems follows two stages:

In the first stage, called pre-screening, the system allows travellers (i.e. third-country nationals, who are not residents of EU Member States, crossing the land borders of EU Member States) to use an online application to upload pictures of their passport, visa and proof of funds, then use a webcam to answer questions from a computer-animated border guard, personalised to the traveller's gender, ethnicity and language. The system then analyses the micro-gestures of travellers to figure out if the interviewee is lying.

The second stage happens at the actual border. Travellers who have been flagged as "low risk" during the first stage will go through a short re-evaluation of their information for entry. The travellers flagged as "high-risk" will undergo a more detailed check. Border authorities will then use a handled device to cross check the information obtained during phase 1 with that of phase 2.[8]

Other technological modules of the project included:[9]

- the **Biometrics Module** incorporating **fingerprints and palm vein technologies** (BIO module), for the biometric identity validation of the traveller;
- the **Face Matching Tool (FMT)**, is the tool for performing **facial recognition** for iBorderCtrl during both pre-registration and border crossing phases; and

[5] "European integrated border management, based on the four-tier access control model, comprises measures in third countries, such as under the common visa policy, measures with neighbouring third countries, border control measures at the external borders, risk analysis and measures within the Schengen area and return" (Reg. EU 2019/1896, Recital 11)
[6] https://www.theguardian.com/world/2018/nov/02/eu-border-lie-detection-system-criticised-as-pseudoscience
[7] https://edri.org/greece-clarifications-sought-on-human-rights-impacts-of-iborderctrl/?fbclid=IwAR1sdTQ6nVZSJ7xaMVHRpzD52nUD96Jkl1BaAFJSQbhUadOBOLulyCNye1k
[8] https://ec.europa.eu/research/infocentre/article_en.cfm?artid=49726
[9] For the complete list see: https://www.iborderctrl.eu/Technical-Framework

- the **Document Authenticity Analytics Tool (DAAT)** examine the security features of travel documents (passport, visa) against fraud characteristics.

This "smart" deception detection system (ADDS) **was criticized for its scientific outcomes and possible discriminatory outcomes**. It was labelled as "pseudoscience" by some scientists, who pointed out for instance how micro-expressions do not really say anything about whether a traveller is lying, as there is also no evidence that liars are more stressed, thus leading to subtle facial movements. Therefore, the technology did not seem necessary to detect lies of travellers. Homo Digitalis stressed how it is unlikely that the system will not commit errors in detecting deceptions (leading to a number of false positives and negatives) and might discriminate minorities or third-country national on the basis of the traveller's gender and ethnicity. The organization also filed a petition to demand the Minister in charge in Greece to state whether a Data Protection Impact Assessment and a consultation with the Greek Data Protection Authority (DPA) took place prior to the implementation of this pilot system to the Greek borders.[10] In the report of 2019 on facial recognition technologies, the EU's Fundamental Rights Agency (FRA) pointed out how facial recognition technologies in general can affect not only the fundamental rights of privacy and data protection, but also, more broadly, impact non-discrimination, rights of the child and of the elderly people, freedom of expression and assembly.[11]

Others stressed how the ADDS **is not the only problematic technology of the project**. The whole iBorderCtrl "architecture" processes also other personal data: for example, it compiles a full facial profile of travellers using video and photographs; it checks their social media accounts; it performs document and signature analysis; it creates and stores their digital voice print. In other words, the system would allow surveillance practices on many travellers relying on a comprehensive amount of data.[12]

The project spokespeople did not address publicly the criticisms but mentioned that "the border crossing decision is not based on the single tool (i.e. lie detection) but on the aggregated risk estimations based on a risk-based approach and technology that has been used widely in custom procedures. Therefore, the overall procedure is safe because it is not relying in the risk on one analysis (i.e. the lie detector) but on the correlated risks from various analysis."[13] All the deliverables of the project (except the flyers and the communication material), including three ethics deliverables, remained confidential.[14]

[10] Some of the pilots of iBorderCtrl took place on the Greek land border at the premises of KEMEA and TRAINOSE, two Greek partners of the consortium (see: https://www.iborderctrl.eu/Greek-Scenario).
[11] Fundamental Rights Agency. (2019). *Facial recognition technology: fundamental rights considerations in the context of law enforcement.* Luxembourg: Publications Office of the European Union, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper.pdf
[12] https://thenextweb.com/artificial-intelligence/2018/11/06/the-eus-border-control-lie-detector-ai-is-hogwash/
[13] As reported in: https://www.theguardian.com/world/2018/nov/02/eu-border-lie-detection-system-criticised-as-pseudoscience
[14] See: https://www.iborderctrl.eu/Publications

Questions (please consider all technological modules of iBorderCtrl mentioned in the text)

1. Why (not) to do a DPIA? Why (not) to do other types of impact assessments?
2. How would you define the benchmark for the impact assessment process?
3. What type of expertise should be included in the team of assessors?
4. What types of (personal) data are to be processed?
5. What types of privacy are affected (spatial, informational privacy, etc.)?
6. What are the possible impacts on fundamental rights beyond privacy and data protection?
7. What types of ethical concerns the technologies raise?
8. What could be the issues related to social acceptance of these technologies?
9. Are the technologies necessary? Are they proportionate?
10. What are the risks? How do you assess them?
11. Who, if ever, is to be consulted?
12. What are the possible mitigation measures?
13. When would you revisit the impact assessment? Why?
14. How do you document your process?
15. Who is going to check the quality of the process? How?