

Data Protection Impact Assessments in Public Service and AI Technology

Thomas Marquenie

KU Leuven Centre for IT & IP Law (CiTiP)

2nd Workshop on Artificial Intelligence for NMCAs (27 October 2022)

Outline

- Concept
- Conditions
- Process
- Best practices

Concept



What is a DPIA?

- **Data Protection Impact Assessment**
- **Mechanism to identify and mitigate data protection risks**
 - Overview of the envisioned processing activities
 - Identification of the risks to data subject rights and freedoms
 - Establishment of measures to minimize the potential negative impact
 - Ongoing and circular process
- **Legal requirement under data protection law**
 - General Data Protection Regulation (GDPR)
 - Law Enforcement Directive (LED)
 - National legislation

Article 35

Data protection impact assessment

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

Conditions



When is a DPIA required? (1)

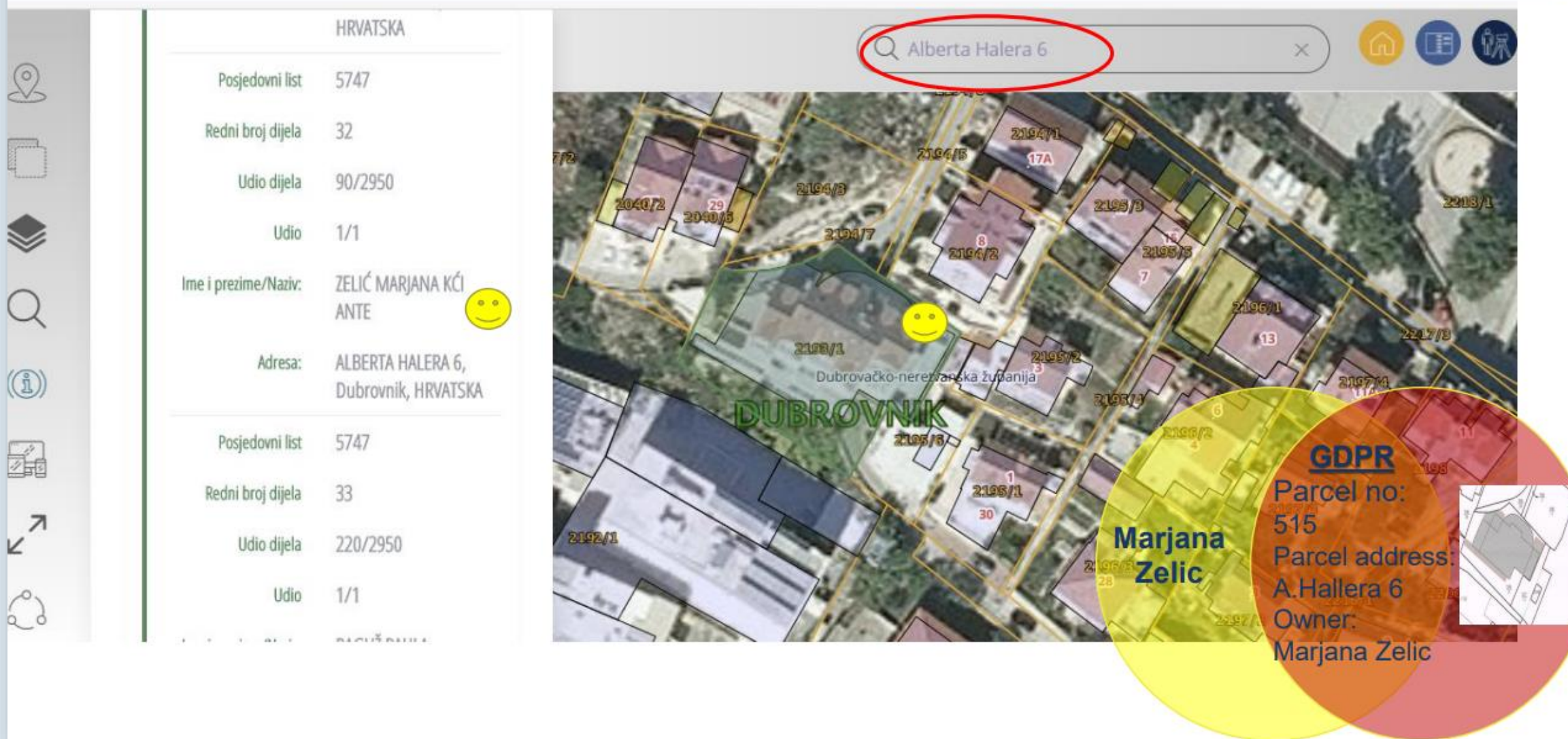
- **Project involves the processing of personal data**

- Processing = collection, analysis, storage, transfer, deletion...
- Personal data = information relating to an identified or identifiable natural person

➡ *Name, identification number, location, address, phone number, IP-address...*

- Cadastral information on property rights and land ownership
- Details on infrastructure and utilities (energy, gas, water, telecommunications...)
- Images and footage (aerial, Streetview-like, roadside / security cameras...)
- Management of national georeferencing networks related to GPS

➡ *Consider that combining data can result in identifiability*



The screenshot displays a web-based cadastral data interface. On the left, a sidebar contains navigation icons. The main content area is divided into two sections. The top section shows property details for a specific parcel, and the bottom section shows a map view of the property.

Property Details:

HRVATSKA	
Posjedovni list	5747
Redni broj dijela	32
Udio dijela	90/2950
Udio	1/1
Ime i prezime/Naziv:	ZELIĆ MARJANA KĆI ANTE
Adresa:	ALBERTA HALERA 6, Dubrovnik, HRVATSKA

Map View:

The map shows a satellite view of the property area in Dubrovnik, Croatia. The property is highlighted in yellow. The search bar at the top right contains the text "Alberta Halera 6". The map includes various labels for parcels and buildings, such as "2194/1", "2194/2", "2194/3", "2194/4", "2194/5", "2194/6", "2194/7", "2194/8", "2194/9", "2194/10", "2194/11", "2194/12", "2194/13", "2194/14", "2194/15", "2194/16", "2194/17", "2194/18", "2194/19", "2194/20", "2194/21", "2194/22", "2194/23", "2194/24", "2194/25", "2194/26", "2194/27", "2194/28", "2194/29", "2194/30", "2194/31", "2194/32", "2194/33", "2194/34", "2194/35", "2194/36", "2194/37", "2194/38", "2194/39", "2194/40", "2194/41", "2194/42", "2194/43", "2194/44", "2194/45", "2194/46", "2194/47", "2194/48", "2194/49", "2194/50", "2194/51", "2194/52", "2194/53", "2194/54", "2194/55", "2194/56", "2194/57", "2194/58", "2194/59", "2194/60", "2194/61", "2194/62", "2194/63", "2194/64", "2194/65", "2194/66", "2194/67", "2194/68", "2194/69", "2194/70", "2194/71", "2194/72", "2194/73", "2194/74", "2194/75", "2194/76", "2194/77", "2194/78", "2194/79", "2194/80", "2194/81", "2194/82", "2194/83", "2194/84", "2194/85", "2194/86", "2194/87", "2194/88", "2194/89", "2194/90", "2194/91", "2194/92", "2194/93", "2194/94", "2194/95", "2194/96", "2194/97", "2194/98", "2194/99", "2194/100".

GDPR Overlay:

GDPR
Parcel no: 515
Parcel address: A. Hallera 6
Owner: Marjana Zelic

When is a DPIA required? (2)

- Processing is “likely to result in a high risk”

- Risk to the rights and freedoms of the data subjects
- Risk is determined by both *likelihood* and *severity* of the potential harm

➡ *Criteria that may indicate a higher risk:*

“...taking into account the nature, scope, context and purposes...”

- “In particular when using **new technologies**”, such as AI systems and tools
- “**Systematic monitoring** of a publicly accessible area”
- “**Evaluation or scoring**”, especially of location, movement, economic situation...
- “**Large scale**”, considering the “geographical extent and number of data subjects”
- “Matching or **combining datasets**”

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

Process



How is a DPIA conducted? (1)

1. **Identify whether a DPIA is needed** *before* the start of the processing
 - Do you process personal data and does this pose a “high risk”?
2. **Describe the scope and nature** of the processing activities
 - Which data will you use? What is the source and purpose?
 - How will you collect, process, store and share data? Who will have access?
 - Which area will it cover? How many individuals are affected? How long will it last?
3. **Examine** whether this is **necessary, proportional and legally compliant**
 - What is your legal basis? Is there a less invasive alternative?
 - Is there a way for data subjects to enforce their rights?

How is a DPIA conducted? (2)

4. **Assess the risks** associated with the processing activities

- Negative impact on privacy? Public distrust?
- Data leaks or data misuse? Function creep?

5. **Present counter-measures** to reduce the risks

- Access controls, anonymization techniques, time limits for storage...
- Data auditing, periodic reviews, supervision, complaints / erasure procedures...
- Exclusion of sensitive information, restrictions on certain processing techniques...

6. **Involvement of the Data Protection Authority**

- If the residual risk remains high

Best Practices



Best practices

- **Do not underestimate the importance of a DPIA**
 - Administrative sanctions, monetary fines, legal liability, project cancellation...
- **When in doubt, seek counsel and advice**
 - Data Protection Officer (DPO) -> legal department -> Data Protection Authority
- **Do not start from scratch but consult templates**
 - CNIL (France), ICO (UK), Privacy International / IAPP (International)...
- **See it as an opportunity with potential benefits**
 - Demonstrating legal compliance, identifying critical issues, proactive planning...

Questions & Contact

Thomas.marquenie@kuleuven.be

This research received support from the Cybersecurity Initiative Flanders – Strategic Research Program (CIF).