The Design of GDPR-Abiding Drones Through Flight Operation Maps: A Win–Win Approach to Data Protection, Aerospace Engineering, and Risk Management

The Design of GDPR-abiding Drones through Flight Operation Maps: A Win-Win Approach to Data Protection, Aerospace Engineering, and Risk Management

Abstract: Risk management is a well-known method to face technological challenges through a win-win combination of protective and proactive approaches, fostering the collaboration of operators, researchers, regulators, and industries for the exploitation of new markets. In the field of autonomous and unmanned aerial systems, or UAS, a considerable amount of work has been devoted to risk analysis, the generation of ground risk maps, and ground risk assessment by estimating the fatality rate. The paper aims to expand this approach with a tool for managing data protection risks raised by drones through the design of flight maps. The tool should allow UAS operators choosing the best air corridor for their drones based on the so-called privacy by design principle pursuant to Article 25 of the EU data protection regulation, the GDPR. Among the manifold applications of this approach, the design of fly zones for drones can be tailored for public authorities in the phase of authorization of new operations, much as for national Data Protection authorities that have to control the lawfulness of personal data processing by UAS operations. The overall aim is to present the first win-win approach to data protection issues, aerospace engineering challenges, and risk management methods for the threats posed by this technology.

Keywords: Data Protection; Data Protection Impact Assessment (DPIA); Design; Drones; GDPR; Risk Management; Unmanned Aerial System (UAS); Unmanned Aerial Vehicle (UAV).

1. INTRODUCTION

The drone sector is flourishing. In Europe, a press released was keen to inform us two years ago, on 16 June 2017, that the EU "Commission is taking the European drone sector to new heights," namely, making "drone use in low-level airspace safe, secure and environmentally friendly." According to the note, the drone services market is going to grow noticeably. "Estimates vary between €10bn by 2035 and €127bn for the coming years. A recent forecast predicts that by 2020 the global drone market size will grow by 42% in precision agriculture, 26% in media and entertainment, by 36% in inspection and monitoring of infrastructures, and by 30% for leisure activities." (European Commission, June 2017).

The expectation of the EU institutions, Member States and authorities, such as the European Union Aviation Safety Agency (EASA), SESAR JU (SESAR Joint Undertakings, November 2016) and JARUS (Joint Authorities for Rulemaking on Unmanned Systems) is high. Still, it seems fair to admit that several legal issues concerning today's regulation of the service market are open (Cifaldi et al., 2018). These problems regard telecommunications and cyber-security breaches, liability and criminal offences, registration and identification of "unmanned aircraft systems" (UASs), including vehicles (UAVs) and Ground Control Stations (GCSs), their pilots and operators, etc. (Bassi, 2019). The Single European sky strategy has thus had to take into account specific sectorial rules of different legal fields, like aviation law and data protection, tortuous liability and e-communication, down to environmental law (European Commission, Directorate-General Enterprise and Industry, November 2014) (European Parliament, Policy Department for Citizen's Rights and Constitutional Affairs, Directorate General for Internal Policy of the Union, November 2018). The regulation of the drone services market concerns also but not only contractors of a delivery service, UAS operators, everyday people walking on streets where UAVs equipped with cameras are flying, whilst a couple discussing in their terrace is intercepted by the sensors of an autonomous little aircraft.

This paper draws the attention to how the use of aircraft with no pilot on board, that is, unmanned aerial vehicles (UAVs), or remotely piloted aircrafts (RPAS), pursuant to Articles 3(30) and (31) of the Regulation (EU) 2018/1139, often entails the processing of personal data in the services market. Remarkably, Article 132 of this regulation includes a safeguard clause for privacy concerns, which refers to the application of the General Data Protection Regulation (GDPR) Reg. (EU) 2016/679. More particularly, the threat is posed by the ways in which sensors, cameras, or geo-positioning systems of UAS and remotely piloted aircrafts may collect "any information relating to an identified or identifiable natural person," that is, the data subject (Finn & Donovan, 2016) (European Data Protection Supervisor, 26 November 2014). According to Article 4 of the GDPR, "an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

The GDPR hinges on the assumption that the processing of personal data is a risky activity. The term risk appears 75 times in the EU legal text. The Regulation thus sets up the list of principles that should be abided by every data processor and moreover, every data

controller. Pursuant to Article 5(1), these principles are (i) lawfulness, fairness, and transparency; (ii) purpose limitation; (iii) data minimization; (iv) accuracy; (v) storage limitation; and, (vi) integrity and confidentiality. It is however up to the decision-making of data controllers as to how to comply with these series of duties. In the phrasing of Article 24(1), "the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation." Moreover, according to Article 25(1), such measures should be pro-active, rather than remedial: data controllers shall abide by the principle of privacy by design, and by default. "Risk assessments on data protection impact do not just regard those directly affected by such data processing, much as privacy by design solutions shall comply with all the requisites of the regulation" (Pagallo et al., 2019).

The European Regulation on Civil Aviation has taken these challenges seriously. On the one hand, Article 132 of Reg. (EU) 2018/1139 adopts all the risk prevention measures set up by the GDPR. On the other hand, the civil aviation regulation hinges on the "application of sound safety management principles... anticipating emerging safety risks and making best use of limited technical resources" (Recital 13 of Reg. 1139 from 2018). Risks are associated with the multiple kinds of aircrafts, operations and activities involved. In the case of unmanned aircraft operations, Recital 27 establishes a degree of flexibility for the Member States that takes into account "various local characteristics, such as population density... in order to implement a risk-based approach and the principle of proportionality." Nevertheless, Article 11 of the Implementing Regulation published on June 2019 (Reg. (EU) 2019/947) provides detailed requirements in order to carry out an operational risk assessment.

Risk management is a well-known method to face new technological challenges and stands as a win-win combination of both protective and proactive approaches, fostering the collaboration of operators, researchers, regulators, and industries for the exploitation of new markets. A considerable amount of papers in this field has been devoted to risk analysis (Washington et al., 2017), ground risk assessment by estimating the fatality rate (Dalamagkidis et al., 2012), or the generation of ground risk maps (Primatesta et al., 2019). Against this framework, which is further explored below in Section 2, the paper aims to present a tool for managing data protection risks raised by autonomous or remotely piloted operations. Data protection safeguards and risk minimization measures should be at work even before the operation starts and a single bit of information has been processed. The tool intends to allow UAS operators choosing the best air corridor for their UAVs based on a data protection map. The service of interactive roadmaps offered by, say, Google can be extended to the flight of city drones and UAS. The tool represents an instance of the so-called privacy by design principle, as set up by Article 25 of the GDPR. It can be tailored for public authorities in the phase of authorization of new operations, e.g. a City officer that has to govern UAS operations, much as a national Data Protection authority that has to control the lawfulness of personal data processing by UAS operations.

Next section introduces the current state of the art in risk management, aerospace engineering, and data protection law. Section 3 sets the level of abstraction of this paper on the design of GDPR abiding drones. The social impact of this technology entails (i) an interdisciplinary approach to safety risk and risks for the protection of personal data; which (ii) has to strike a balance between data protection rights and time operation optimization;

through (iii) the design of personalized fly maps for UAS services. Section 4 illustrates how, pursuant to Art. 25 of the GDPR, the data protection by design principle works in this case, providing the methodology of the research. Section 5 discusses the methodology with a case study, i.e. a flight drone operation performed in an urban context of Turin (Italy). Section 6 illustrates the first experiments and empirical results. Section 7 draws the conclusions.

2. ON RISKY DRONES

In order to ensure security and safety for aircraft operations in the Single European Sky, the EU has adopted a risk-based approach. In the wording of Recital 12 of Reg. (EU) 2018/1139, "the measures taken in accordance with this Regulation to regulate civil aviation in the Union, and the delegated and implementing acts adopted on the basis thereof, should correspond and be proportionate to the nature and risks associated with the different types of aircraft, operations and activities they address. Such measures should also, in as far as possible, be formulated in a manner which focuses on objectives to be achieved, while allowing different means of achieving those objectives." In addition, pursuant to Recital 32, "conditions, rules and procedures should, in particular, take into account the type, scale, and complexity of the operation, including, where relevant, the size and type of the traffic handled by the responsible organisation or person; whether the operation is open to members of the public; the extent to which other air traffic or persons and property on the ground could be endangered by the operation; the purpose of the flight and type of airspace used; and the complexity and performance of the unmanned aircraft involved."

The European Union Aviation Safety Agency has made clear that safeguards, authorizations and limitations should be assessed in a proportional and flexible degree vis-à-vis the level of expected risks (European Aviation Safety Agency, 2015), (European Aviation Safety Agency, 2018). In June 2019, the European Commission published the implementation acts mandated by Articles 57 and 58 of the 2018 Regulation, namely the Implementing Regulation 2019/947 on the rules and procedures for the operation of unmanned aircraft and the Delegated Regulation 2019/945 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems. In particular, Reg. (EU) 2019/947 provides the requirements on how to carry out an operational risk assessment, namely: (a) description of the characteristics of the UAS operation, (b) definition of a "target level of safety," (c) identification of the risks of the operation on the ground and in the air, (d) identification of a range of possible risk mitigating measures; (e) information on the "necessary level of robustness of the selected mitigating measures in such a way that the operation can be conducted safely." All those factors shall be taken into account in order to both reduce uncertainty for risks of a drone flight and minimize them. On the soft side of the law, the European Aviation Safety Agency, or EASA, has adopted the Joint Authorities for Rulemaking on Unmanned Systems (JARUS) guidelines (European Union Aviation Safety Agency, 2017a) (European Union Aviation Safety Agency, 2017b). EASA is a regulatory agency of the EU created in 2002 by Regulation (EC) No. 1592/2002 (now Reg. (EU) 2018/1139) to establish and maintain a uniform level of civil aviation safety in EU. Their

guidelines propose a Specific Operations Risk Assessment (SORA) method, namely, a multi-stage process for safety risk assessment to define the risk of UAS operations. Another safety risk assessment approach is a probabilistic risk assessment quantifying the ground impact fatality rate, commonly used in the literature: see (Dalamagkidis et al. 2012) (Clothier et al., 2007) (la Cour-Harbo, 2018a) (Primatesta et al., 2019). According to some scholars, the probabilistic risk assessment approach aligns with the SORA method (la Cour-Harbo, 2018b). This stance has laid the groundwork for further research. For example, in (Primatesta et al., 2019), authors provide a risk map for the use of drones, in order to quantify the risk for the population on ground over urban areas. Other kinds of research have been devoted to compute the minimum risk path by using a risk-aware path planning (Primatesta, Guglieri, & Rizzo, 2018) (Primatesta, Cuomo, et al., 2018). It thus seems fair to affirm that ground risk models to estimate the risk of UAS operations abound in literature (Washington et al., 2017).

Still, as mentioned above in the introduction, drone operators have to evaluate a further kind of risk, that is, data protection in addition to the safety risks of UAS operations. According to Article 35(1) of the GDPR, which is of course valid law for the use of drones, "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." The data protection impact assessment (DPIA) is a step-by-step review of the processing activity carried out by the data controller, in order to identify all possible risks. It is a method for both building and proving compliance (Wright & Finn, 2016). The DPIA is mandatory when personal data processing entails high risks for the rights and freedoms of natural persons (Art. 29 WP, wp 248 rev01, 2017). The GDPR provides that a DPIA shall specifically be required in case of systematic monitoring of publicly accessible areas on large scale, in particular, via optoelectronic devices, or for other processing activities that national and European authorities, e.g. the European Board, may deem high-risk. Hence, it is likely that (i) most drone flights will require a DPIA (Art. 29 WP, wp231, 2015); (ii) such a DPIA will have to quantify probability of events, consequences, and costs, in order to determine the level of risk; and, (iii) such level of risk should be grasped vis-à-vis the further levels of risk for safety that include e.g. the ground risk models and ground impact fatality rates stressed above in this section.

The versatility of UAS risks depends on the multiplicity of devices that can be loaded: these devices are receptors of data and information of various kinds, including personal data (Finn & Wright, 2016). The most popular UAS device is the camera: when they have particularly high resolution, cameras may allow the collection of personal data and even biometric data (which the GDPR includes in the list of "special categories of personal data" in Article 9, so as to provide for a more robust personal data protection). UAS with high-resolution cameras can accurately capture the facial features of a data subject, whilst UAS equipped with low-resolution cameras may collect no personal data at all. Correspondingly, in accordance with the data minimization principle of the GDPR's Art. 5(1)(iii), a drone flight which needs no personal data for its mission shall be equipped with low-resolution cameras, such as an Obstacle Avoidance Sensor, or as a support to the pilot. The data minimization principle also recommends that data controllers should choose such flight

paths that allow UAS to collect no personal data, or as less personal data as possible. One of our contentions in this paper is that UAS payloads and flight paths can be an effective solution for drone flights complying with data protection principles and provisions of the GDPR. Next section explains why this is the case; then, Section 4 illustrates this approach to the principle of data protection by design, pursuant to Art. 25 of the GDPR.

3. A DATA PROTECTION MAP GENERATOR

We have seen so far how drone flights have to abide by the risk regulation provisions of both the European Regulation on Civil Aviation and the GDPR. The design of legally abiding drones requires an interdisciplinary approach to safety risks and risks for the protection of personal data. In addition to the SORA method and further approaches to risk management and risk evaluation, as e.g. in (Dalamagkidis et al., 2012), attention should be drawn to the data protection impact assessments of the GDPR and how a balance must be struck between data protection rights and further rights and interests, such as in time operation optimization. Data protection is not an absolute but relative right, according to the case law of both the EU Court of Justice in Luxembourg and the European Court of Human Rights in Strasbourg (Pagallo, 2013). It is then crucial to flesh out which further rights and interests are at stake with the use of drones, either for precision agriculture, or media and entertainment, or inspection and monitoring of infrastructures, or simply leisure activities. Depending on which scenario, such as drone delivery of urgent medicals, different forms of balancing follow as a result.

Among the main ingredients of such legal balance, we have a robust tradition in the risk assessment tradition, the impact assessments of data protection, and how to tackle the flexibility of some legal rules, as the GDPR's Article 25 on the principle of privacy by design and by default. Although drone flights in Europe should be compliant with principles and rules of, also but not only, civil aviation and data protection regulations (European Data Protection Supervisor, 26 November 2014), (Cavoukian, 2012) there is room for flexibility and legal imagination. According to the principle of accountability, pursuant to Articles 5(2) and 24(1) of the GDPR, it is up to the decision-making of data controllers as to how to comply with the series of principles listed in Article 5(1). Here, a lot of space for optimization is before us.

Correspondingly, we start imagining a service of interactive roadmaps, such as offered by Google Maps, extended to the flight of city drones and UAS. The design of personalized roadmaps for UAS services consists of software for the dynamic visualization of different kinds of risk, e.g. ground impact fatality rate, while preserving data protection rights and optimizing the operation's time (Dalamagkidis et al., 2012), (Clothier et al., 2007), (Primatesta, et al., 2019). In this context, focus is on the data protection impact assessment, or DPIA, of such drone flights through a data protection map generator. In order to make this scenario more concrete, consider *(i)* a specific urban area, such as, say, some parts of downtown Turin, vis-à-vis *(ii)* a category of UAS; *(iii)* a typology of payload; *(iv)* possible different mission types; and, *(v)* just one kind of processing activity: the data collection. As shown by Figure 1, the first step is to take into account the different types of building and

structures involved, such as universities, hospitals, police offices, cemeteries, schools, etc. The selected area of the city represents a zone rich of different data protection impact evaluations.

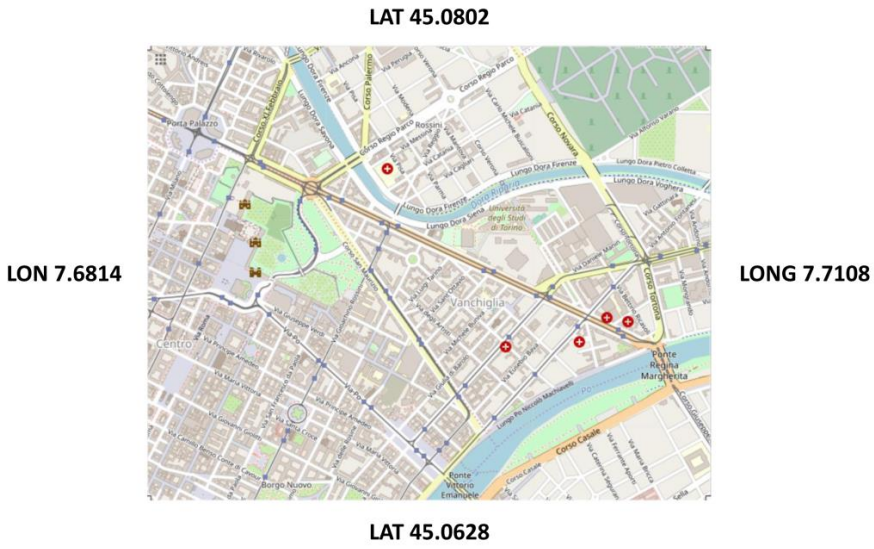

Figure 1: A Sketch of Downtown Turin.

The source data of the map and all related information were extracted from Open Street Map (OSM). OSM is an open source map of the world and data are easily integrated in the simulation. The main advantage in using the OSM is that our approach can be tested everywhere in the world. To test the efficiency of the DPIA, we opted for a quadrotor, namely, a DJI Mavic Pro, a portable and powerful aircraft. The features are illustrated in the following table.

DJI MAVIC PRO	
Size	83x83x198 mm
Weight	743 g
Maximum speed	65 km/h
Endurance	27 min
Camera	4K

Figure 2 - The DJI Mavic Pro aircraft

According to the EASA document, this vehicle is part of the C1 category, i.e. with a mass less than 0.9 kg, and must respect the required property of harmless drone. The latter can be employed in urban areas with higher safety requirements. The payload consists in a 4K camera stabilized by a 3-axis mechanical gimbal, supporting video at 30 fps. Other sensors were not considered in this analysis because we reckon they do not compromise the DPIA. Rather, attention should be drawn to the possible different types of UAS missions in urban environment, such as a leisure mission, or an emergency delivery of first aid kits and

medication. Depending on the use of drones, different kinds of data protection impacts follow as a result.

4. THE DESIGN OF DATA PROTECTION

There are several ways to calculate the level of risk of an activity: the methodology used in this paper entails that the level of risk (LR) for the data protection impact assessment should be calculated on the basis of the probability (P) that a threat can occur, thus infringing rights and freedom of natural persons, and on the basis of the severity of the impact (I). In accordance with (ENISA, 2018), this stance can be summed up as follows:

$$LR= P*I$$

On this basis, the evaluation of the probability of threats due to the processing of personal data has to be sorted out. It depends on the category and amount of the data collected: the probability value is given from 1 (low level) to 3 (high level). Table 2 illustrates this probability of data protection threats.

Level	Value	Probability of negative consequences that derive from the processing of personal data
Low	**1**	The threat is unlikely to materialize.
Medium	**2**	There is a reasonable chance that threat materializes.
High	**3**	The threat is likely to materialize.

Table 2 – Probability of data protection threats

Then, the next step concerns the level of the impact on data subjects. The factors under scrutiny are as different as a possible data breach, discrimination, identity theft, reputation prejudice, or social damage. As shown by a new table (Table 3), four levels of impact are taken into account: low, medium, high, and critical.

Impact level	Impact value	Description
Low	**1**	Individuals may encounter some minor inconveniences, which can be overcome without any problem (annoyances, irritations, etc.).
Medium	**2**	Individuals may encounter considerable unease, which can be overcome despite some difficulties (fear, lack of understanding, stress, minor physical disturbances, etc.).
High	**3**	Individuals may encounter significant consequences that they may overcome despite serious difficulties (property damage, prosecuting, bad health condition, etc.).
Critical	**4**	Individuals can have significant, or even irreversible, consequences that they cannot overcome (long-term psychological or physical disorders, etc.).

Table 3 – Impact levels

We assessed the impact of urban drone flights on the rights of those on the ground, by distinguishing *(i)* the category of data; *(ii)* the critical issues in acquiring such data, *(iii)* some crucial distinctions about data subjects, e.g. minors; and, *(iv)* geolocation.

The level of risk (LR) for data protection (dp) $\mathbf{LR_{dp}}$ is computed using the method described in (ENISA, 2018), and by evaluating different categories of data involved in the risk analysis, namely:

$$\mathrm{LR_{dp}} = P \cdot \left(\sum_{i=0}^{n} D_i \cdot I \right)$$

In the formula, P is the probability that a threat can occur and damage a data subject; I is the severity of the impact; D represents different levels of data protection. Table 4 illustrates five different sets of data, namely, from no personal data at all (value 0) to the protection of highly sensitive data enshrined in Articles 9 and 10 of the GDPR (value 4). We further distinguished between the standard level of protection pursuant to the definition of Article 4 of the GDPR (value 1), particular classes of data in certain legal systems (value 2), and sensitive data (value 3). Since the payload of the aircraft may include more than one sensor, it follows that UAS may collect different categories of data ($i = 1, \ldots n$ with n number of types of data). The equation above includes the sum of all categories of data, according to time of events and their impact.

Value	Categories of data
0	No Personal Data.
1	Personal data pursuant to Article 4 GDPR.
2	Particular protection for certain classes of data in some Member States (e.g. Articles 26 - 27 of the Italian Legislative Decree 14 March 2013, No. 33, on information relating to grants, contributions, subsidies and financial aids, the attribution of economic advantages of any kind to natural persons, such as the amount of the economic advantage paid, the legal basis or the title for the attribution).
3	Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership (Article 9 GDPR); Children data (Article 8 GDPR).
4	Genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation (Article 9 GDPR); Data relating to criminal convictions and offences or related security measures (Article 10 GDPR).

Table 4 – Five different levels of data protection.

Once we have defined the probability of data protection threats (Table 2), impact levels (Table 3), and different types of data protection in EU and Member States law (Table 4), we examined risk factors of the urban drone flight, in accordance with the source map that defines flight altitude, payload, and mission of the flight. The evaluation of the level of risk (LR) exploits a "level of risk factors database" (LRFD) and then, the building extraction processing from the sourced map illustrated above in the previous section. The architecture of the data protection impact assessment (DPIA) is reported in Figure 3.

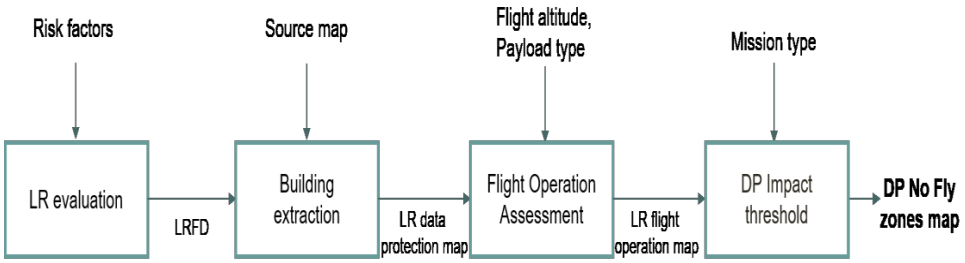

Figure 3 – The Architecture of the Assessment.

The architecture generates three different maps to set up a DPIA over urban areas, namely, the level of risk (LR) data protection map, the LR flight operation map, and the data protection (DP) No Fly zones map. Each is a two-dimensional location-based map, in which every cell represents a square area centered in a location with a value defined according to the map type. Hence, each map is represented as a matrix of dimension NxM.

The inputs of the proposed methodology are the *Risk Factors* that were used to generate the aforementioned *Level of Risk Factors Database* (LRFD). The LRFD stores all the data protection impact values defined according to the building type, the activity done inside it and, of course, the data which might be found and collected inside those buildings. As shown by a new table (Table 5), the related Level of Risk, or "Raw Level," is defined in the LRFD for each building type and activity, according to the different categories of data in Table 4, to the probability of data protection threats in Table 2, and to the impact value of Table 3. For example, we assigned to hospitals the values of 4, 2, 4, respectively, whereas churches were given 3, 1, 2, and universities 1, 1, 1. The "raw level" of risk is then quantified in accordance with the formulas below in Section 5.

Building	Data 1	Data n	Probability	Impact Value	Raw Level of risk
Police office	4	-	2	2	16
Kindergarten	3	-	2	2	12
Hospital	4	-	2	4	32
Prison	4	-	2	2	16
Consulate	4	-	2	2	16
Pharmacy	4	-	2	2	16
Church	3	-	1	2	3
University	1	-	1	1	1
Museum	1	-	1	1	1
Library	1	-	1	1	1

Table 5 – The Raw Level of Risk

We admit that the final outputs of Table 5 are open to discussion and may even vary over time. Still, they represent a good enough approximation to assess the data protection impact of drone flights in urban areas. Next sections illustrate how we quantified different levels of risk through data protection abiding maps.

5. A CASE STUDY

Let's go back to Open Street Map (OSM). We extracted the building list from data about the building type and the geo-location of each building in the portion of downtown Turin under scrutiny. Two different maps on the level of risk (LR) on data protection and the LR flight operation followed as a result.

The first map, namely $\mathbf{LR_{dp}}$ assumes that each element $\mathbf{LR_{dp}}(x, y)$ of the map has a value determined by the Level of Risk defined by the LRFD, based on the building type placed in the associated area. The area is represented by the element centered in the location (x, y). Thus,

$$\mathbf{LR}_{\boldsymbol{dp}}(x, y) = \mathrm{LR}(b, x, y),$$

with b being the building type. The Level of Risk LR_{dp} is computed for each cell of the map, considering the building characteristics located in the area represented by the cell. The LR of a specific flight operation hinges on a DPIA. Figure 3 above has shown that such impact assessment consists of two processes: the flight operation assessment and the use of a threshold. The flight operation assessment evaluates the Level of Risk when the aircraft performs a particular flight operation, i.e. with a predefined flight altitude and with a specific payload. The assumption is that the Level of Risk decreases with the distance between the data subject and the aircraft, depending on the type of the payload. In particular, we determined the Level of Risk using a function f(·), obtaining the level for a specific flight operation. On this basis, a second map $\mathbf{LR_{fo}}$ is defined as follows:

$$\mathbf{LR_{fo}}(x, y) = \mathbf{LR_{dp}}(x, y) \cdot f(d, p)$$

with f(·) as function of the distance between the data subject and the aircraft (d), and the type of payload (p).

$\mathbf{LR_{fo}}$ is thus the map containing the Level of Risk (LR) referred to a particular flight mission. When the UAV flies over a location (x, y), the aircraft is able to collect data from all the neighbour locations. By defining a set **L** as the set of all neighbour locations near the aircraft, the value $\mathbf{LR_{fo}}(x, y)$ is defined as the maximum level of risk involved by all neighbor locations:

$$\mathbf{LR_{fo}}(x, y) = \max[\, \mathbf{LR_{dp}}(x_i, y_i) \cdot f(d_i, p), \qquad \forall\, (x_i, y_i) \in \mathbf{L}]$$

Here, d_i is the distance between the aircraft and the location at (x_i, y_i). In particular, the distance is computed considering both vertical and horizontal distances between the UAV and a location, where the vertical distance is the flight altitude.

In addition, we assumed the use of a camera with a 4K resolution. The camera is able to acquire personal data (as defined in the GDPR, i.e. data about an identified or identifiable person), when it frames a subject. The risk to collect personal data appears as proportional to the effective resolution of the image of the data subject. For instance, a person's face reported in an image of 200 pixels is recognizable. This is not the case when the same face is represented by 10 pixels. As a result, the Level of Risk defined as $\mathbf{LR_{fo}}$ is proportionate to the resolution of the image of the data subject. However, it is not easy to determine the resolution of a camera, because the quality of an image depends on the camera sensor's type, such as the lens focal length and the field of view. In this work, we used the method described in (Theia Technologies, 2009), in which the resolution of an image is defined in accordance with the distance between camera and subject, and with the camera parameters. The resolution is computed with the following formula:

$$res = \frac{h_{px} \cdot l_{focal}}{d \cdot w_{chip}}$$

In the formula, d is the distance between the camera and the subject; w_{chip} is the width of the chip of the camera sensor; h_{px} is the number of pixels of the entire image on the horizontal axis; and l_{focal} is the lens focal length. The resulting resolution is expressed in pixel/m and refers to the resulting resolution of the image vis-à-vis a plane at distance d. According to the results reported in (Theia Technologies, 2009), we identify two thresholds to evaluate the resolution of an image: *(i)* with a resolution greater than 200 pixel/m, the data subject is completely recognizable; *(ii)* with a resolution lower than 70 pixel/m, subjects are not recognizable. When the image has a resolution between 70 and 200 pixel/m, the risk decreases exponentially with the resolution according to the following equation

$$f(d,p) = \begin{cases} 0 & if\ res < res_{min} \\ \left(\frac{res - res_{min}}{res_{max} - res_{min}}\right)^{0.5} & if\ res_{min} \leq res \leq res_{max} \\ 1 & if\ res > res_{max} \end{cases}$$

with res_{min} the minimum resolution defined at 70 pixel/m, and res_{max} the maximum resolution defined at 200 pixel/m.

Figure 4 illustrates the function f(·) in respect of the resolution of the image.

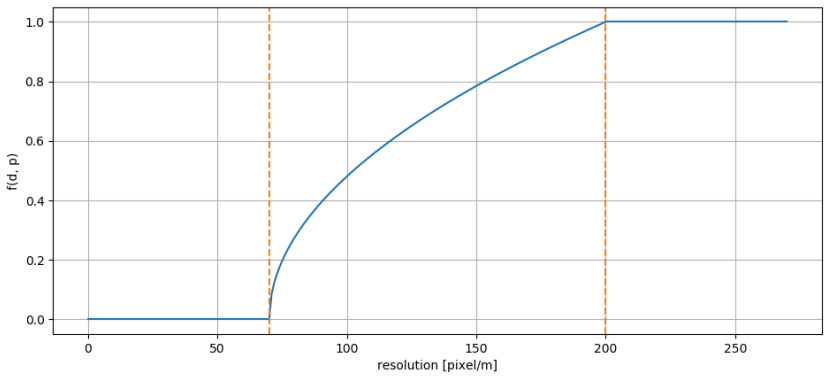

Figure 4: The domain of the function f(d, p).

The Level of Risk for a specific flight operation is finally computed for each cell in the map $\mathbf{LR}_{fo}$. Accordingly, depending on the mission type, the last step defines the output map. It determines in which areas the flight is allowed due to the Level of Risk and the mission type. If the Level of Risk of the flight operation of a cell $\mathbf{LR}_{fo}(x, y)$ exceeds the threshold, the flight in the area is not allowed. Otherwise, if the risk involved is lower, the flight is permitted.

The threshold is illustrated with Figure 5. A delivery mission at 50 m of flight altitude should allow a drone to fly only over the school, an emergency delivery drone could flow over the school and the hospital.

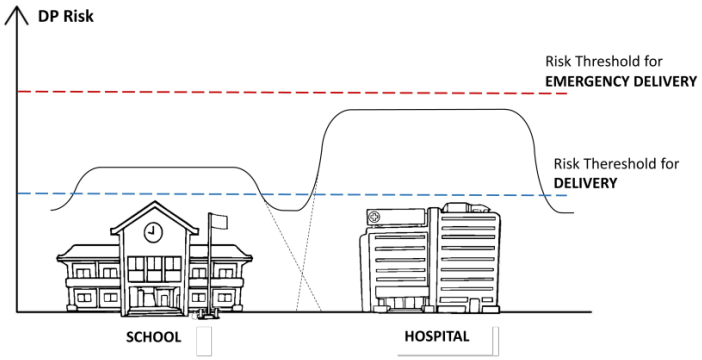

Figure 5: Simplified example

Regardless of whether drone missions are more or less urgent, our Data Protection Map Generator fleshes out the no-fly zones over urban areas. UAS should be designed in such a way that maps instruct them as to their best corridor, or in which areas flying is not permitted. In particular, the idea to plan a sort of data protection aware flight mission is implemented in C++ as an executable process in the Robot Operating System (ROS) (Quigley et al., 2009). ROS is an open-source framework for developing robotics applications. Each map is constructed using the Grid Map library (Fankhauser & Hutter, 2016), a C++ library interfaced with ROS able to manage two-dimensional grid maps with multiple data layers.

6. FIRST EXPERIMENTS

The aim of this section is to graphically represent the architecture of our data protection assessment introduced above with Figure 3. We can further appreciate on this basis how data protection safeguards may impact the fly corridors of drones. Once again, OSM provides data for all buildings and their topology. By taking into account the level of risk (LR) Impact Database, a new figure (Figure 6) shows how the different maps on the LR for data protection, flight operations, and No Fly Zones (NFZ) look like.

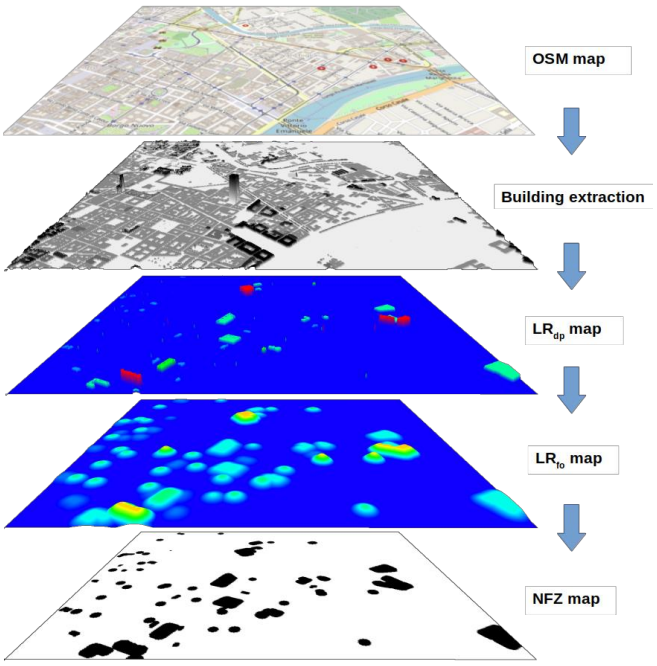

Figure 6: Graphical representation of the proposed methodology.

After the "building extraction" of Figure 6, the map on the level of risk for data protection posed by a drone flight, or $\mathbf{LR_{dp}}$ map, represents the sketch of downtown Turin introduced above in Section 3. The blue areas correspond to streets, rivers and buildings that do not trigger particular data protection issues, whereas the building with higher Level of Risk is a hospital (value 32). The granularity of this picture can of course be augmented. For example, Figure 7 colors the levels of risk from 1 (in blue) up to 32 (in red).

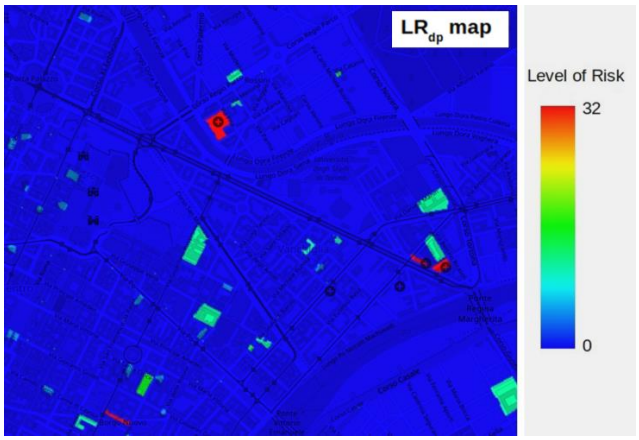

Figure 7: Flying over downtown Turin with $\mathbf{LR_{dp}}$ *maps.*

In addition to such values for each element of the $\mathbf{LR}_{dp}(x, y)$ map, namely the Level of Risk defined by the building type placed in the associated area, a second representation takes into account the Flight Operation Assessment (FOA) and the characteristics of the flight operation through a $\mathbf{LR}_{fo}$ map, which includes flight altitude, camera(s), payload and mission of the drone under scrutiny. As further discussed below in Appendixes 1 and 2, on the one hand, these experiments cast light on crucial differences between maps. At the altitude of 15 m., for instance, the threshold values applied to an $\mathbf{LR}_{fo}$ map end up with several no-fly zones in the case of a drone's delivery mission, whilst rare no-fly zones pop up for an emergency delivery case. On the other hand, a **NFZ** (no-flight zone) map can be used as a path-planning algorithm to plan a flight mission in urban areas. Figure 8 reports an example of such a path in the NFZ map. The path is computed with the RRT* (Optimal Rapidly-exploring Random Tree) algorithm, able to seek for a near-optimal path in the map, avoiding no-fly zones and obstacles in the map. The map of Figure 8 includes both no-fly zones of Figure 10 below in Appendix 1, and obstacles at the flight altitude of 15 m. The resulting path can be executed by the UAS, so as to avoid no-fly zones and any kind of obstacle.

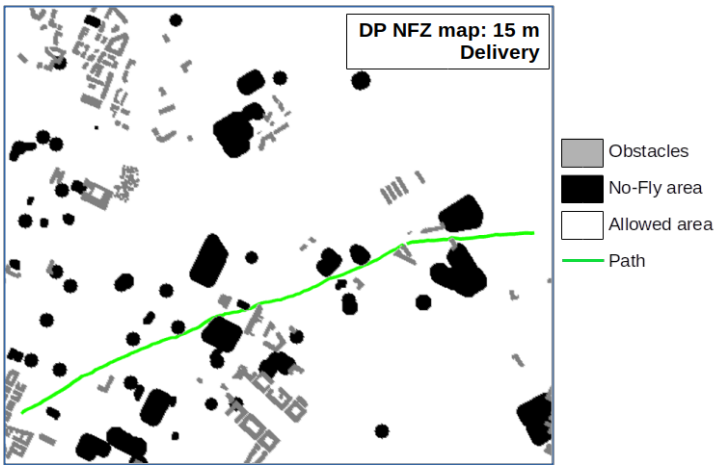

Figure 8: The path planning of a delivery mission at 15 m.

Our Data Protection Map Generator thus provides a smart way in which we can tackle the threats of drone flights in urban areas. This technology can be designed to fly hand-in-hand with the protection of data protection rights, in a flexible and proportionate manner. A personalized fly map for UAS follows as a result of the topological features of urban areas and taking into account the specific kind of drone, payload, and mission to be carried out. The time is ripe for the conclusions of this paper.

7. CONCLUSIONS

We mentioned that ground risk and safety models to estimate the threat of UAS operations abound in literature. Still, drone operators and authorities have to evaluate a further kind of risk, that is, data protection. Our analysis has aimed to fill a gap in current research, by providing a first model of fly zones for GDPR-abiding drones. In particular, Section 3 drew the attention to *(i)* a specific urban area, such as some parts of downtown Turin, vis-à-vis *(ii)* different categories of UAS; *(iii)* the typology of payload; and, *(iv)* possible different mission types, e.g. an emergency delivery mission of food, or drugs. Section 4 illustrated the architecture of the principle of data protection by design. The focus was on the probability of data protection threats (i.e. Table 2), impact levels (Table 3), and different kinds of data protection (Table 4), in order to determine the "Law Level" of risk for a drone's fly zone (Table 5). Then, Section 5 provided two different maps on the level of risk (LR) for data protection and the LR flight operation, namely, the $\mathbf{LR_{dp}}$ and $\mathbf{LR_{fo}}$ maps. $\mathbf{LR_{dp}}$ assumes that each element $\mathbf{LR_{dp}}(x, y)$ of the map has a value determined by the Level of Risk defined by the building type placed in the related area. $\mathbf{LR_{fo}}$ is the map containing the Level of Risk (LR) referred to a particular flight mission. Section 6 showed crucial differences between such maps, that is, how principles and rules on today's data protection safeguards may affect the flight of a drone, much as how additional parameters, such as camera(s), payloads, and missions under scrutiny, further define the balance between data protection and flight optimization. The Data Protection Map Generator suggests, or even determines, what is the best corridor for UAVs, or in which areas flying is not permitted. The stance can be tailored for public authorities in the phase of authorization of new operations, e.g. a City officer that has to govern UAS operations, much as a national Data Protection authority that has to control the lawfulness of personal data processing by UAS operations.

Some issues, however, remain open to further work and discussion. First, we should develop our 2Dmodels into 3D to improve scalability, interoperability, and optimization. Second, we should mix our previous research on drone security and safety maps with our new GDPR-abiding maps for drones in urban contexts, i.e. the $\mathbf{LR_{dp}}$ map, the $\mathbf{LR_{fo}}$ map, and the **NFZ** map of Appendix 2. Third, we may further distinguish between data protection and privacy impacts brought about the use of UAS technology: all in all, data protection aims to protect the transparency of personal data processing; privacy aims to protect the "opaqueness" of individuals. Fourth, we may address this complex mix of interdisciplinary issues with current research on machine learning and generative adversarial networks. We should accordingly distinguish between maps for remote piloted drones and growingly autonomous aerial systems.

Yet, for the time being, we filled a gap. We've got the first kind of flight operation maps for GDPR-abiding drones in the EU market, namely, a sound example of a win-win approach to data protection, aerospace engineering, and risk management for UAS technology.

8. BIBLIOGRAPHY

Article 29 Data Protection Working Party. (2015). *Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones, WP231, Adopted on 16 June 2015*.

Article 29 Data Protection 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, as last Revised and Adopted on 4 October 2017*.

Bassi, E. (2019). European Drones Regulation: Today's legal Challenges. *2019 International Conference on Unmanned Aircraft Systems (ICUAS)*, 443-450.

Cavoukian, A. (2012). *Privacy and Drones: Unmanned Aerial Vehicles*. Ontario, Canada: Information and Privacy Commissioner.

Cifaldi, C., Mascarello, L. N., & Quagliotti, F. (2018). Regulations: The European Way. In K. P. Valavanis, & G. J. Vachtsevanos, *Handbook of Unmanned Aerial Vehicles*. Springer.

Clothier, R. A., Walker, R. A., Fulton, N., & Campbell, D. A. (2007). A casualty risk analysis for unmanned aerial system (UAS) operations over inhabited areas. *AIAC12, Twelfth Australian International Aerospace Congress, 2nd Australasian Unmanned Air Vehicles Conference*, (p. 1-15).

Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems.

Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft.

Dalamagkidis, K., Valavanis, K. P., & Piegl, L. A. (2012). *On integrating unmanned aircraft systems into the national airspace system: issues, challenges, operational restrictions, certification, and recommendations*. Springer.

ENISA. (2018). *Handbook on Security of Personal Data Processing*.

European Commission. (2017, June 16). *Press Release. Aviation: Commission is taking the European Drone Sector to new Heights*. Retrieved from http://europa.eu/rapid/press-release_IP-17-1605_en.htm#_ftn2..

European Commission, Directorate-General Enterprise and Industry. (November, 2014). *Study on the Third-Party Liability and Insurance Requirements of Remotely Piloted Aircraft Systems (RPAS)*.

European Data Protection Supervisor. (26 November 2014). *Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on "A new era for aviation - Opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner"*.

European Parliament, Policy Department for Citizen's Rights and Constitutional Affairs, Directorate General for Internal Policy of the Union, Study for the JURI Committee. (November, 2018). *Artificial Intelligence and civil law: liability rules for drones, PE608.848*.

European Union Aviation Safety Agency. (2015). *Concept of Operations for Drones, A risk based approach to regulation of unmanned aircraft*.

European Union Aviation Safety Agency. (2017a). *Notice of proposed amendment 2017-05 (a) - introduction of a regulatory framework for the operation of drones*.

European Union Aviation Safety Agency. (2017b). *Notice of proposed amendment 2017-05 (b) - introduction of a regulatory framework for the operation of drones*.

European Union Aviation Safety Agency. (2018). *Opinion 01/2018, Introduction of a regulatory framework for the operation of unmanned aircraft systems in the 'open' and 'specific' categories.*

Fankhauser, P., & Hutter, M. (2016). A Universal Grid Map Library: Implementation and Use Case for Rough Terrain Navigation. In A. Koubaa, *Robot Operating System (ROS) – The Complete Reference (Volume 1)*. Springer.

Finn, R. L., & Donovan, A. (2016). Big Data, Drone Data: Privacy and Ethical Impacts of the Intersection Between Big Data and Civil Drone Deployments. In B. Custers, *The Future of Drone Use. Opportunities and Threats from Ethical and Legal Perspectives* (p. 47-70). Springer.

Finn, R. L., & Wright, D. (2016). Privacy, data protection and ethics for civil drone practice: A survey of industry, regulators and civil society organisations. *Computer Law & Security Review, 32*, 577-486.

la Cour-Harbo, A. (2018a). Quantifying ground impact fatality rate for small unmanned aircraft. *Journal of Intelligent & Robotic Systems*, 1–18.

la Cour-Harbo, A. (2018b). The Value of Step-By-Step Risk Assessment for Unmanned Aircraft. *ICUAS 2018, International Conference on Unmanned Aircraft Systems*. IEEE.

Pagallo, U. (2013). On the Principle of Privacy by Design and its Limits: Technology, Ethics and the Rule of Law. In S. Gutwirth et al., *European Data Protection: In Good Health?* (p. 331-346). Springer.

Pagallo, U., Casanovas, P., & Madelin, R. (2019). The Middle-out Approach: Assessing Models of Legal Governance in Data Protection, Artificial Intelligence, and the Web of Data, *Theory and Practice of Regulation*, Forthcoming.

Primatesta, S., Cuomo, L. S., Guglieri, G., & Rizzo, A. (2018). An innovative algorithm to estimate risk optimum path for unmanned aerial vehicles in urban environments. *International Conference on Air Transport - INAIR 2018*, (p. 1-10).

Primatesta, S., Guglieri, G., & Rizzo, A. (2018). A risk-aware path planning strategy for UAVs in urban environments. *Journal of Intelligent & Robotic Systems*, 1-15.

Primatesta, S., Rizzo, A., & la Cour-Harbo, A. (2019). Ground risk map for unmanned aircraft in urban environments. *Journal of Intelligent & Robotic Systems*, 1-21.

Quigley, M., Gerkey, B. P., Conley, K., Faust, J., Foote, T., Leibs, J., Bergert, E., Wheeler, R.., Ng, A. Y. (2009). ROS: an open-source Robot Operating System. *ICRA Workshop on Open Source Software*.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91.

SESAR Joint Undertakings, European Union. (2016, November). *European Drones Outlook Study*. *Unlocking the Value for Europe*.

Theia Technologies. (2009). *Theia Technologies*. *How to calculate the image resolution*.

Washington, A., Clothier, R., & Silva, J. (2017). A review of unmanned aircraft system ground risk models. *Progress in Aerospace Sciences*.

Wright, D., & Finn, R. (2016). Making Drones more Acceptable with Privacy Impact Assessment. In B. Custers, *The Future of Drone Use*. *Opportunities and Threats from Ethical and Legal Perspectives* (p. 325-352). Springer.

APPENDIX 1 – ON LR_{fo} Maps

In addition to the **LR_{dp}** map presented in Section 6, a **LR_{fo}** map can be created, in order to take into account the Flight Operation Assessment (FOA) and the characteristics of the flight operation. We used the DJI Mavic Pro with a 4k camera. The **LR_{fo}** map is computed using a flight altitude of 15 m and 25 m. The resulting maps are reported in Figures 8 and 9.

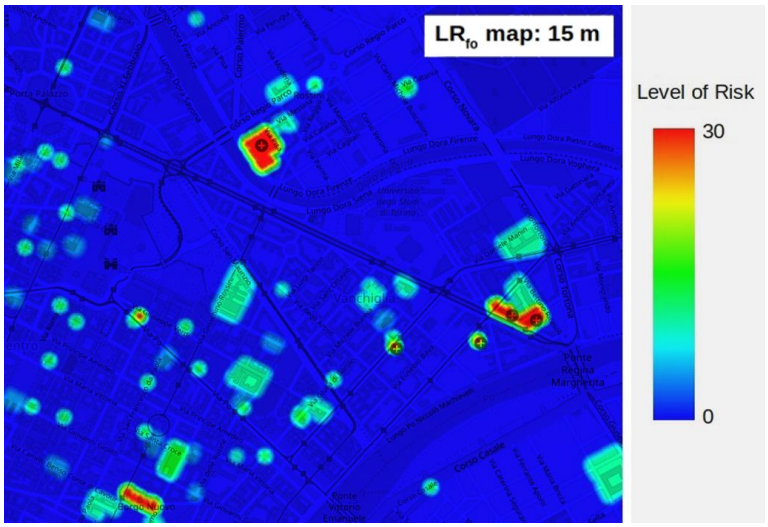

Figure 8: The **LR_{fo}** *map of the same area of Figure 6. The map assumes the use of an UAV at the altitude of 15 m and a 4k camera.*

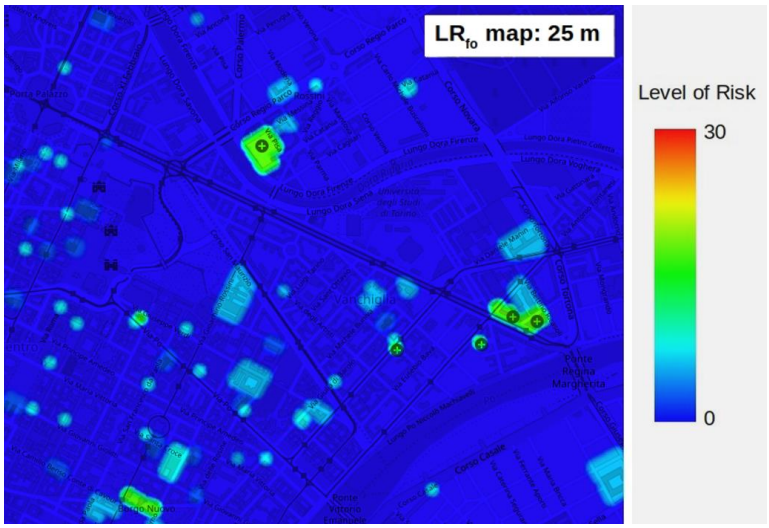

Figure 9: The **LR_{fo}** *map of the same area of Figure 6. The map assumes the use of an UAS at the altitude of 25 m and a 4k camera.*

Flight altitude affects the Level of Risk in the **LR_{fo}** map. The Level of Risk lowers because the distance between the camera, i.e. the UAV, and the data subject increases. The Level of Risk of 32 defined by the hospital of Figure 7 decreases to 30.13 with the flight altitude of

15 m. An altitude of 25 m decreases the Level of Risk to a value of 23.05. Accordingly, we may say that the Flight Operation Assessment (FOA) reshapes the Level of Risk LR_{dp}. FOA softens the peak value and inflates risk distribution. Figure 6 of the paper in Section 6 illustrated this step using a three-dimensional view of both $\mathbf{LR_{dp}}$ and $\mathbf{LR_{fo}}$ maps.

The $\mathbf{LR_{fo}}$ map evaluates the Level of Risk of a flight operation with a specific flight altitude and payload. According to the mission type, a DPIA threshold determines the areas in which a drone flight is allowed. The case study of Section 6 introduced two types of mission: delivery and emergency with threshold values set at 5 and 30, respectively.

APPENDIX 2 – ON NFZ (NO FLY ZONES)

In addition to the $\mathbf{LR_{dp}}$ and $\mathbf{LR_{fo}}$ maps, our Data Protection Map Generator casts light on the areas in which flying is not permitted. In particular, Figures 10 and 11 illustrate two No-Fly Zones (NFZ) maps. They correspond to the altitude of 15 m. Threshold values are applied to the $\mathbf{LR_{fo}}$ map of Figure 8 accordingly. A crucial difference emerges as a consequence: in the map of the delivery mission, there are several no-fly zones; in the map of the emergency delivery mission, there are rare no-fly zones.

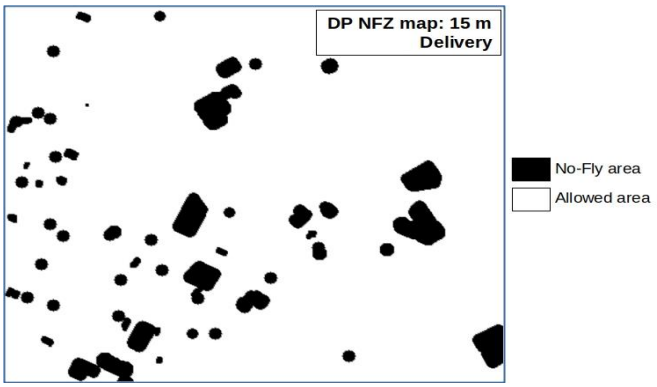

Figure 10: The NFZ map considering a delivery mission and flight altitude of 15 m.

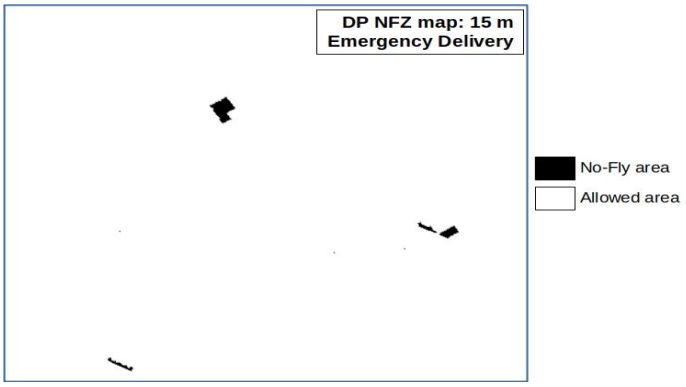

Figure 11: The NFZ map considering an emergency delivery mission and flight altitude of 15 m.

Yet, how about the same parameters of Figure 10 under a delivery mission, but flight altitude of 25 m.? Figure 12 reports this scenario. Again, no fly zones areas decrease. By considering mission and altitude at 25 m, in the case of emergency delivery, the UAS can fly all over the map because all areas have a Level of Risk lower than the DPIA threshold.

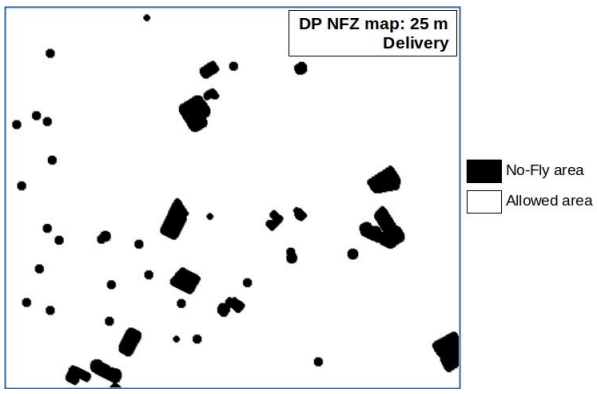

Figure 12: The NFZ map considering the delivery mission and a flight altitude of 25 m.

Among the manifold applications of this approach to drones and personal data protection, we mentioned in the paper that a NFZ map can also be used as a path-planning algorithm to plan a flight mission in urban areas. Figure 8 above illustrated an example of such a path in the NFZ map, so that UAS can avoid all no-fly zones and every kind of obstacle.