“NOVEL INTEGRATED SOLUTION OF OPERATING A FLEET OF DRONES WITH MULTIPLE SYNCHRONIZED MISSIONS FOR DISASTER RESPONSES”

RespondDrone

D12.2 “Legal, ethics, privacy & security framework”

Project Deliverable Report

Deliverable Number: 12.2
Deliverable Title: Legal, ethics, privacy & security framework
Author(s): Jos Dumortier, Niels Vandezande
Work Package Number: 12
Work Package Title: Innovation Management, Exploitation & Business Planning

This project is funded by the European Union’s H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

RESPONDRONE Project Information	
Project full title	Novel Integrated Solution of Operating a Fleet of Drones with Multiple Synchronized Missions for Disaster Responses
Project acronym	RESPONDRONE
Grant agreement number	833717
Project coordinator	Max Friedrich, DLR
Project start date and duration	1st May 2019, 36 months
Project website	https://respondroneproject.com/

Deliverable Information	
Work package number	12
Work package title	Innovation Management, Exploitation & Business Planning
Deliverable number	12.2
Deliverable title	Legal, ethics, privacy & security framework
Description	Analysis of legal requirements applicable to ResponDrone
Lead beneficiary	Timelex
Lead Author(s)	Jos Dumortier, Niels Vandezande
Contributor(s)	Jos Dumortier, Niels Vandezande
Revision number	1.0
Revision Date	30/12/2019
Status (Final (F), Draft (D), Revised Draft (RV))	F

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

Dissemination level (Public (PU), Restricted to other program participants (PP), Restricted to a group specified by the consortium (RE), Confidential for consortium members only (CO))	PU

Document History			
Revision	**Date**	**Modification**	**Author**
0.1	20/09/2019	Initial draft	Niels Vandezande
0.2	30/11/2019	Review	Jos Dumortier
1.0	30/12/2019	Final Version	Menelaos Chatziapostolidis

Approvals				
	Name	**Organisation**	**Date**	**Signature (initials)**
Coordinator	Max Friedrich	DLR	31/12/2019	MF
WP Leaders	Nir Tel Oren	IAI	31/12/2019	NTO

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

Disclaimer

Copyright message

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

Table of Contents

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

1. Executive Summary

Legal and ethical issues are core aspects for the successful implementation of drone-based first responses – both as potential barriers, but also as strong facilitators when providing a trustworthy, reliable framework for complex ICT-enabled emergency responses. These must be addressed as part of the innovation process to enable a sustainable implementation and successful, compliant usage of the emergency response applications to be developed. Therefore, it is the goal of Task 12.2 to support RESPONDRONE in being fully compliant with all legal, regulatory, certification and ethics requirements both at the European and at the respective national level.

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

2. Introduction

This deliverable focuses on a number of core issues. First, it looks at the regulation of drones, where the EU has in 2019 adopted a new legal framework that supersedes earlier national rules. Second, it looks at the use of drones by emergency services, particularly within the framework of civil protection in the EU. National legislation of a few select Member States has been taken into account here as well. Third, it looks at the privacy and data protection issues that can be raised through the use of drones, which form pressing ethical and legal concerns that must be appropriately addressed within the project. Fourth, it looks at the use of radio spectrum by first responders. Fifth, it looks at the use of drones for the transport of particular goods, in this case blood and medicinal products. Last, it looks at a number of potential security aspects.

After this introduction (section 2), this deliverable provides the results of the main legal analysis into the legal frameworks applicable to RESPONDRONE. First, we look at the EU and national regulations with regard to the use of drones (section 3). Second, we look at the legal framework applicable to emergency services and the use of drones therein (section 4). Third, we turn to the fields of privacy, data protection and image rights, which will be important legal and ethical matters when drones are equipped with audio-visual tools and when they can be used for surveillance purposes (section 5). Fourth, we look at the use of the radio spectrum by first responders, in order to establish how they can receive radio spectrum usage rights to deploy drones as mobile antennas for electronic communications networks (section 6). Fifth, we look at the legal framework applicable to the transport of medicinal products and blood (section 7). Sixth, we look at the legal framework regarding the security of network and information services (section 8). This deliverable is closed off with summary conclusions (section 9).

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

3. Regulation of drones

3.1. At the international level

International air travel is principally regulated through the 1944 Chicago Convention on International Civil Aviation. This international treaty also established the International Civil Aviation Organization (ICAO), which commenced operations in 1947 and became an agency of the United Nations under the Economic and Social Council. The treaty, which has been amended several times, provides the main rules with regard to airspace, the registration and safety of aircraft, and air travel rights. Important to note is that this treaty only applies to civil aircraft and not state aircraft.[1] Military, customs and police aircraft are considered state aircraft.

Article 8 of this Convention refers to 'pilotless aircraft'. These can only be over the territory of a State with authorization of that State and according to the principles of the Convention. Flying pilotless aircraft in areas open to civil aviation must obviate danger to civil aircraft.

While the Convention itself does not provide further information on what constitutes a 'pilotless aircraft', there is an additional circular by ICAO on Unmanned Aircraft Systems (UAS).[2] This circular provides definitions for notions such as autonomous aircraft and operations, remote piloting, and unmanned aircraft. Generally, unmanned aircraft are all aircraft without a pilot on board. They can either be piloted remotely (remote piloting) or without pilot intervention (autonomous aircraft). Overall, this circular provides a first assessment of the further framework needed to regulate UAS.

A 2012 amendment to the Chicago Convention's Annex 2 'Rules of the air' included a definition for Remotely piloted aircraft system (RPAS). Generally, RPAS must be operated in such a way as to minimize hazards to people, property and other aircraft. The amendments reiterate the need to State authorization. Also amended were Annexes 7 'Nationality and registration marks' and 13 'Accident investigation'.

In 2015, ICAO adopted the 'Manual on Remotely Piloted Aircraft Systems (RPAS)'.[3] This manual serves RPAS used for other than recreational purposes. It provides guidance on applying the existing aviation legal framework to RPAS. It applies to "*commercial air transport and general aviation, including aerial work, operations conducted by RPAS*". Generally, this manual provides guidance to legislators on how to handle RPAS. Rather than fully going through all principles of this manual, we will – in the following sections – discuss how the EU and EU Member States have implemented these rules with regard to RPAS.

[1] Article 3 Chicago Convention on International Civil Aviation.
[2] Cir 328 AN/190.
[3] Doc 10019 AN/507.

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

3.2. At the EU Level

3.2.1. Basic Regulation

According to article 100(2) of the Treaty on the Functioning of the European Union, the EU has the competence to adopt appropriate rules for sea and air transport. To this end, a new basic Regulation for the safety of civil aviation was adopted in 2018.[4] This Regulation implements at the EU level the main principles of the aforementioned Chicago Convention. It repeals and replaces earlier regulations in this field.[5]

According to article 3(30) of the Regulation, an unmanned aircraft is "*any aircraft operating or designed to operate autonomously or to be piloted remotely without a pilot on board*". The Regulation sets out the essential requirements for the design, production, maintenance and operation of unmanned aircraft (article 55). This may be subject to certification (article 56). Annex IX to the Regulation provides more rules on unmanned aircraft. They must be designed fit for purpose and to avoid putting persons at risk. Their operators must be aware of applicable rules. Data protection rules must be respected. They must display adequate airworthiness and be piloted by sufficiently skilled and trained pilots. Safety of their operations must be ensured. However, further rules are to be determined by the European Commission by means of implementing and delegated acts. Those acts were adopted in 2019. They entered into force 1 July 2019 and become applicable 1 July 2020. The European Union Aviation Safety Agency (EASA) is expected to publish further guidance material and predefined risk assessments later in 2019.

The most important change brought by the new EU rules is a move toward risk-based regulation of UAS. As a result, recreational use and professional use of drones can be subjected to the same rules, depending on the type of UAS and their operations. The registration duty will ensure that all UAS operators are identified. Only the use of small UAV without cameras – <250g – will be exempted from registration. Higher classes of UAV have more stringent requirements with both theoretic and practical tests and require certification.

[4] 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, *OJ* L 212 of 22 August 2018, 1-122.

[5] E.g. Regulation (EC) No 216/2008 of the European Parliament and of the Council of 20 February 2008 on common rules in the field of civil aviation and establishing a European Aviation Safety Agency, and repealing Council Directive 91/670/EEC, Regulation (EC) No 1592/2002 and Directive 2004/36/EC, *OJ* L 79 of 19 March 2008, 1-49; Regulation (EC) No 552/2004 of the European Parliament and of the Council of 10 March 2004 on the interoperability of the European Air Traffic Management network (the interoperability Regulation), *OJ* L 96 of 31 February 2004, 26-42.

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

None of the three regulations specify whether a single pilot can operate multiple drones at the same time. It is expected that this will be further addressed in the guidance material to be adopted by the EASA.

3.2.2. Implementing Regulation

First, there is an Implementing Regulation.[6] This Regulation establishes a risk-based approach, determining three categories of operations: open, specific and certified (article 3). Risk mitigation measures must be commensurate to the risk posed by a particular category of operations.

The open category is not subject to prior operational authorization or an operational declaration. Aircraft in this category must have a take-off mass of less than 25kg and maintain visual line of sight at all times. They can in principle only be flown up to a height of 120m and not over assemblies of people. Further requirements can be found in Part A of the Annex to the Regulation.

The specific category does require an operational authorization and operational declaration. Operations are subject to a risk assessment. The operational declaration must state the specifics of the operation – e.g. whether it intends to fly over assemblies of people or controlled ground area – and appropriate risk mitigation measures. The risk assessment can be made according to one particular operation, or standard scenarios can be used. Operational authorization must be obtained from the competent authority. In any case, the operator of the unmanned aircraft is subjected to a number of rules, mainly relating to limiting operational risks.

The certified category requires certification and possibly licensing of the remote pilot. This category includes operations over assemblies of people, involving the transport of people, or involving the carriage of dangerous goods, in other words the most high-risk operations. Part C of the Annex holds provisions for obtaining a light UAS operator certificate (LUC). Those holding a LUC do not have to submit the operational declaration, nor receive operational authorization. Each LUC holder must have an appropriate safety management system in place.

3.2.3. Delegated Regulation

Second, there is a Delegated Regulation.[7] This Regulation focuses more on the design and manufacture of the UAS themselves. It follows the three categories defined in the Implementing Regulation.

[6] Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft, *OJ* L 152 of 11 June 2019, 45-71.
[7] Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems, *OJ* L 152 of 11 June 2019, 1-40.

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

UAS in the open category can be marketed as toys, in which case they must follow product safety rules for toys.[8] When they are not toys, they must comply with general rules on machinery[9] and additional rules on UAS. UAS complying with these rules can be marketed freely in the EU. Manufacturers must document this compliance and apply the relevant CE-marking. Member States must designate notifying bodies and conduct market surveillance to ensure compliance.

UAS in the specific and certified categories can be designed to transport people or dangerous goods, to have dimensions of over 3m or to be used in the specific category of operations. When subject to certification, UAS in this group must comply with general requirements for the airworthiness of aircraft.[10]

The Annex to the Regulation defines different classes of UAS, depending on their risk. For instance, there is C0, with UAS weighing up to 250g. C1 UAS can weigh up to 900g and transfer less than 80J upon impact with a human head. C2 UAS can weigh up to 4kg. C3 weighs less than 25kg. C4 is restricted to 25kg as well and cannot be capable of automatic control modes.

3.3. At the national level

Before the adoption of the EU framework regarding drones, several Member States had already adopted their own rules in this field. Unlike a directive – which needs to be transposed into the national law of the Member States – a regulation is directly applicable. As a result, and following the adoption of the new EU regulations, Member States will have to bring their national legal framework in line with those new rules. Some implementing legislation will be needed, which at this stage is still to be adopted.
In future iterations of this deliverable, we will look at how Member States have conducted this exercise. According to recital 1o of the Basic Regulation, it is possible for Member States to apply the EU framework to aircraft carrying out military, customs, police, search and rescue, firefighting, border control and coastguard or similar activities and services undertaken in the public interest. It will therefore need to be followed up to what extent Member States will use this option.

[8] Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the safety of toys, *OJ* L 170 of 30 June 2009, 1-37.
[9] Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC, *OJ* L 157 of 9 June 2006, 24-86.
[10] E.g. Commission Regulations (EU) No 748/2012, (EU) 2015/640, and (EU) No 1321/2014.

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

4. Drones for emergency services

4.1. At the EU level

4.1.1. Civil protection

Civil protection – or civil defence – originated as a mechanism to protect a State's citizens from military attacks and natural disasters. Nowadays, the focus has mostly shifted toward disaster and emergency prevention, mitigation and response. Civil protection is included in title XXIII of the Treaty on the Functioning of the European Union in its article 196.

> *1. The Union shall encourage cooperation between Member States in order to improve the effectiveness of systems for preventing and protecting against natural or man-made disasters.*
> *Union action shall aim to:*
> *(a) support and complement Member States' action at national, regional and local level in risk prevention, in preparing their civil-protection personnel and in responding to natural or man-made disasters within the Union;*
> *(b) promote swift, effective operational cooperation within the Union between national civil-protection services;*
> *(c) promote consistency in international civil-protection work.*
> *2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure shall establish the measures necessary to help achieve the objectives referred to in paragraph 1, excluding any harmonisation of the laws and regulations of the Member States.*

From this, it follows that civil protection in itself remains a competence of the Member States. The EU will only play a role in fostering cross-border cooperation between Member States to better respond to disasters.

Member States can request assistance from other Member States through the EU Civil Protection Mechanism.[11] The Mechanism pools expertise and capacities of first responders, in order to ensure swift and efficient assistance where needed. Capacities are included in the European Civil Protection Pool.[12] Moreover, the Mechanism supports training and the development of standards to ensure a higher level of preparedness and prevention. In 2019, the Mechanism was expanded with the rescEU reserve in order to provide a higher reserve of capacities.

From an operational perspective, the Emergency Response Coordination Centre (ERCC) coordinates the actual mobilization and monitors events.[13] Additionally, the Copernicus Emergency Management Service produces up-to-date satellite maps that provide first responders with the necessary geospatial information.

[11] https://ec.europa.eu/echo/what/civil-protection/mechanism_en.
[12] https://ec.europa.eu/echo/what/civil-protection/european-civil-protection-pool_en.
[13] https://ec.europa.eu/echo/what/civil-protection/emergency-response-coordination-centre-ercc_en.

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

4.1.2. Drones in civil protection

The Basic Regulation does not apply to "*aircraft, and their engines, propellers, parts, non-installed equipment and equipment to control aircraft remotely, while carrying out military, customs, police, search and rescue, firefighting, border control, coastguard or similar activities or services under the control and responsibility of a Member State, undertaken in the public interest by or on behalf of a body vested with the powers of a public authority, and the personnel and organisations involved in the activities and services performed by those aircraft*" (article 2(3)(a)).

The operation of drones for civil protection purposes can therefore be considered to fall outside of the scope of the EU drone regulations. Nevertheless, and as noted before, Member States can decide to apply these rules in such situations as well.

4.1.3. Defence procurement

Drones are already widely used in military and defence operations. The EU has adopted the EU Defence and Security Procurement Directive to foster cross-border defence procurement.[14] The reason for this directive is that defence markets in the EU were mainly a matter of national law, which hindered the creation of a cross-EU defence manufacturing market. Defence procurement operated in a sphere of national protectionism, which resulted in a very low degree of competition on this market. The directive therefore aims to open up this market and to create an EU-wide defence market. Being a directive, this framework needed to be transposed into the national law of the Member States. While the directive sets the main provisions, some national differences are still possible.

The directive applies to the procurement of military equipment, being "*equipment specifically designed or adapted for military purposes and intended for use as an arm, munitions or war material*", and sensitive equipment, being "*equipment, works and services for security purposes, involving, requiring and/or containing classified information*" (article 1(6) and (7)). According to recital 10 to the directive, this also includes equipment designed for civilian use that has been adapted for military purposes. Civil purchases are contracts falling out of the scope of the directive, covering the procurement of non-military products, works or services for logistical purposes.

According to Annex I to the directive, defence services includes both military defence services and civil defence services. As a result, the procurement of equipment for civil defence purposes also falls under the scope of this directive. The directive is a *lex specialis* to the general

[14] Directive 2009/81/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of procedures for the award of certain works contracts, supply contracts and service contracts by contracting authorities or entities in the fields of defence and security, and amending Directives 2004/17/EC and 2004/18/EC, *OJ* L 216 of 20 August 2009, 76-136.

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

procurement framework – set by Directive 2014/24/EU – which excludes civil defence, civil protection, and danger prevention services that are provided by non-profit organisations or associations, except patient transport ambulance services (article 10(h)).[15]

However, on the basis of article 346(1) of the Treaty on the Functioning of the European Union, Member States may exempt certain procedures from the scope of this deliverable – be it that such should be exceptionally. Moreover, the directive lists a number of exclusions, in article 10, such as contracts for intelligence services.

The basic principle of defence procurement is to treat economic operators equally and in a non-discriminatory manner and to act in a transparent way (article 4). Article 8 establishes the thresholds above which the framework applies. These are (a) EUR 412 000 for supply and service contracts, and (b) EUR 5 150 000 for works contracts – both excluding VAT. Article 9 provides methods for calculating the estimated value of the contracts. Member States are, however, free to also conduct procedures for lower values under this framework.

Contracts for the services listed in Annex I to the directive are subject to the provisions of articles 18 to 54. This includes civil defence services. Annex III to the directive defines a number of technical specifications for the procedure aimed to create equal access to all tenderers – such as referring to existing standards. Conditions for the performance must be in compliance with EU law and be described in the procedure (article 20). Articles 22 and 23 provide details on the security of information and supply. Contracts can be awarded according to national procedure as adjusted for this framework (article 25). In some cases, a negotiated procedure without publication of a contract notice may be allowed (article 28). Member States can allow framework contracts (article 29).

Contract notices must be published on beforehand (Article 30). Annex IV to the directive provides detailed requirements on the publication of prior information, contract notices and award notices. Annex VI provides how notices must be provided to the Publications Office of the EU. Generally, a time limit for responses to the procedure of 37 days must be observed, although derogations are possible (article 33). Article 36 provides the rules on communication, with Annex VIII holding requirements for electronic receipts. Procedures must be documented in reports (article 37). Specific requirements apply to electronic auctions (article 48).

The directive provides criteria for the selection of tenderers (articles 39 *et seq.*). This must take into account the personal situation of the candidate and their suitability for the tasks. Economic and financial standing, as well as technical and/or professional capability must be taken into account too. Member States may adopt lists of approved candidates (article 46). Subcontracting

[15] Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC, *OJ* L 94 of 28 March 2014, 65-242.

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

can be allowed, and subcontractors must be treated in an equal and non-discriminatory manner (article 51).

4.2. At the national level

Given that civil protection is mainly a competence of the Member States, it must be assessed which rules have been implemented in a select number of EU Member States and how those rules relate to the use of drones. Moreover, those rules may provide an indication to what extent such Member State is likely to apply the EU rules on drones to the use of drones in civil protection.

4.2.1. Belgium

The main rules with regard to drones can be found in the Royal Decree of 10 April 2016.[16] This decree defines remote piloted aircraft (RPA) as weighing less than 150kg (article 1, 4°). It defines two classes of flights. Class 1 flights present moderate or increased risk for airspace safety and/or persons and goods on the ground because flights are either conducted where the safety of third parties on the ground would be endangered in case of emergency or could give rise to a serious risk due to their nature or location (article 1, 18°). Class 2 flights are any RPA flight with a maximum take-off mass of less than 5kg for activities such as aerial photography, geography and observation with low risk for airspace safety and/or persons or goods on the ground (article 1, 17°). Class 2 flights must remain 50m removed from buildings, people and animals.

The Royal Decree does not apply to the use of drones in military, customs, police, search and rescue, firefighting, coastguard, or similar operations (article 3 §1, 2°).

The operation of RPA must be compliant with the EU and Belgian rules regarding airspace safety (article 5). Certain operations are prohibited, including the transport of passengers or goods using RPA (article 6). Visual line-of-sight must be maintained at all times (article 12). Article 13 defines areas in which RPA class 2 operations are not permitted. Title 4 of the decree defines the pilot certification scheme as well as the permit to operate RPA. Pilots must pass theoretical and practical training. The certificate only serves class 2 operations, while the permit allows class 1 operations. This also requires RPA to have an unique registration identifier (article 16). To this end, a register of RPA registrations is created (article 53). Flights must be preceded by a risk analysis (article 68). If the risk analysis shows a higher risk, the flight is subjected to prior authorization (article 73). Class 1 flights require an operational manual (article 78).

[16] Royal Decree of 10 April 2016 regarding the use of remote piloted aircraft in the Belgian airspace, *Belgian State Gazette* 15 April 2016.

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

On 7 December 2017, a Ministerial circular was adopted on the use of drones by police and first responders.[17] The Circular applies to the use of drones by all state actors such as police, firefighters and civil protection services – regardless of whether or not the drone is owned by such state actor. The Circular confirms that some of the basic rules on drones do apply – such as the prohibition of passenger transport using RPA. The drone operator must continuously remain in control of the drone. General drone operations must maintain visual line-of-sight. Beyond line-of-sight operations may only be conducted by pilots specifically licensed to do so. Also, the licensing and registration requirements of the Royal Decree apply, as do the risk analysis and operational manual.

The conclusion of this is that while the Royal Decree principally excludes the use of drones for civil protection purposes, the Circular states that many of the principles of that legal framework do in fact apply.

In June 2019, the 2017 Circular was replaced with a new version.[18] It contains an important restriction in that all flights – regardless of whether they are within or beyond visual line-of-sight – in controlled and non-controlled airspace are limited to 300ft. Under the previous Circular, flights in controlled airspace did not have an upper limit and only required notification by telephone to air traffic control before the flight. Flights within controlled airspace limited to a range of 500m around a stationary pilot can be allowed if prior authorization by air traffic control is obtained and following certain procedures and conditions. If the drone is owned by an external operator, this operator must receive a written confirmation from civil protection services authorizing its use within the operation.

Directive 2009/81/EC has been transposed in the Belgian Act of 13 August 2011.[19] Annex 1 to the Act includes civil defence services as being subjected to this legal framework. The thresholds above which the European notification duty applies have been amended to EUR 5.548.000 for works and EUR 443.000 for services.[20] A Belgian notification duty may apply even below those thresholds. Generally, the directive has been transposed fairly faithfully into Belgian law. There are no major deviations from the EU directive.

[17] Ministerial Circular of 7 December 2017 on the use of drones by police and first responders, *Belgian State Gazette* 28 March 2018.
[18] Ministerial Circular of 25 June 2019 on the use of drones by police and first responders, *Belgian State Gazette* 8 July 2019.
[19] Act of 13 August 2011 concerning public procurement and certain contracts for works, deliveries and services in the fields of defence and security, *Belgian State Gazette* 1 February 2012.
[20] Article 33 Royal Decree of 23 January 2012 concerning public procurement and certain contracts for works, deliveries and services in the fields of defence and security, *Belgian State Gazette* 1 February 2012.

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

4.2.2. France

The main legal texts in France with regard to drones are two Orders of 17 December 2015.[21]

The first Order distinguishes three categories of operation: aeromodelling, experiments and private use – which can also include commercial activities (article 3). Each of these operations is subjected to specific conditions listed in the Annexes to the Order (article 4). Drone operations presenting higher risks can be limited or prohibited (article 6). Specific authorizations can be given when not all of the conditions listed in the Annexes are met (article 7).

Drones operated on behalf of the State for the purposes of rescue missions, emergencies, customs, police or civil security may derogate from the rules set by the two Orders when the circumstances of the operation and the public order and security justify it (article 8).

Annex III to the first Order applies to private use of drones. It defines four scenarios based on proximity to people and distance from the pilot. These scenarios determine the type of drone that can be used in them. Each drone must display the name and contact details of its operator. Certain drones require a design certificate. An operational manual must be maintained. Specific safety measures – depending on the scenario used – are applicable. Drone operations must be notified on beforehand and can only go through when an acknowledgment of receipt of such notification has been obtained.

The second Order defines the airspace in which drone operations can or cannot be conducted. For instance, flights in populated areas are subject to prior notification. Also, flights beyond line-of-sight and flights above 50m are subjected to notification. Prior authorization is required for some flight operations, such as those in controlled airspace.

A third Order determines the necessary qualifications for pilots.[22] Pilots for flights in scenarios 1, 2 and 3 must be above 16 years old, have followed theoretical training and have a certificate proving their aptitude for flights in those scenarios. For flights in scenario 4, the minimum age is 18 years and a pilot license is required. Requirements for the theoretical and practical tests are listed in the Annexes to the Order. Military credentials or those obtained in other EU Member States can be taken into account. Drone pilots must maintain a flight log.

[21] Arrêté du 17 décembre 2015 relatif à la conception des aéronefs civils qui circulent sans personne à bord, aux conditions de leur emploi et aux capacités requises des personnes qui les utilisent, *JORF* n°0298 du 24 décembre 2015 page 23897; Arrêté du 17 décembre 2015 relatif à l'utilisation de l'espace aérien par les aéronefs qui circulent sans personne à bord, *JORF* n°0298 du 24 décembre 2015 page 23890.

[22] Arrêté du 18 mai 2018 relatif aux exigences applicables aux télépilotes qui utilisent des aéronefs civils circulant sans personne à bord à des fins autres que le loisir, *JORF* n°0129 du 7 juin 2018 texte n° 32.

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

Drones are already being used by civil protection services. The most well-known example of such use occurred during the fire at the Notre-Dame de Paris cathedral, where images captured by the drone helped firefighters to prioritize and to mount a more effective response to the fire.[23] Drones are also being used to combat forest fires or to map flooding.[24]

Directive 2009/81/EC was transposed by the Act of 22 June 2011.[25] The Act inserted a number of provisions with regard to the import and export of military goods to or from EU Member States into the French Defence Code and the Public Markets Ordinance[26]. These provisions are in line with the EU Directive. A further Decree of 14 September 2011 amended the Public Markets Code with the procedures prescribed by the EU Directive.[27] The Public Markets Code was later replaced by a new Public Markets Ordinance.

4.2.3. Germany

New drone rules were adopted in 2017.[28] According to article 1 of the Regulation, drones weighing more than 250g must be equipped with a fireproof plaque displaying the name and address of the operator. Drones weighing over 5kg require special permission, as does the operation of any drone within a 1,5km range around airports and nightly flights. Drones weighing below 5kg cannot be operated beyond line-of-sight. Neither can drones be operated closer than 100m from people gatherings, disaster areas, or industrial or military installations. Drones heavier than 250g or equipped with video, audio or radio equipment cannot be flown over residential houses, unless the owner has permitted so. Flights above 100m are only allowed in certain cases, as are flights below 50m in controlled areas. Operation of drones above 25kg is prohibited, unless for certain agricultural purposes. Operation of drones above 2kg requires training and proof of qualification.

No permission is needed for done flights by or under the supervision of authorities in the fulfilment of their duties or by organizations tasked with matters of emergencies, disasters or accidents. This provision thus exempts civil protection services from compliance with these rules. Furthermore, they are not subjected to the licensing requirements.

[23] https://www.numerama.com/tech/481413-notre-dame-de-paris-le-drone-precieux-allie-des-pompiers.html.
[24] https://www.interieur.gouv.fr/Archives/Archives-des-dossiers/2016-Dossiers/Les-drones-au-service-de-la-securite/Identifier-en-temps-reel-les-contours-d-un-sinistre.
[25] Loi n° 2011-702 du 22 juin 2011 relative au contrôle des importations et des exportations de matériels de guerre et de matériels assimilés, à la simplification des transferts des produits liés à la défense dans l'Union européenne et aux marchés de défense et de sécurité, *JORF* n°0144 du 23 juin 2011 page 10673.
[26] Ordonnance n° 2015-899 du 23 juillet 2015 relative aux marchés publics, *JORF* n°0169 du 24 juillet 2015 page 12602.
[27] Décret n° 2011-1104 du 14 septembre 2011 relatif à la passation et à l'exécution des marchés publics de défense ou de sécurité, *JORF* n°0214 du 15 septembre 2011 page 15450.
[28] Verordnung zur Regelung des Betriebs von unbemannten Fluggeräten, *BGBl*. I 2017 S. 683.

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

Drones have been used in civil protection in Germany for quite some time. Already a decade ago the AirShield project was launched, in which drones were equipped with lightweight gas sensors. Civil protection falls under the ambit of the Federal Office of Civil Protection and Disaster Assistance. It was this government agency that advocated the use of drones by civil protection services, as included in the 2017 drone regulation.[29]

Defence procurement is subject to the general rules on public procurement. In 2011, an Act was adopted implementing the essential elements of Directive 2009/81/EC into German competition law – which also governs public procurements.[30] The more procedural rules of the Directive were implemented into a 2012 Regulation.[31] The German legislator has lowered the thresholds for applicability of this legal framework to EUR 80.000 for goods and services, and to EUR 1.000.000 for construction works. For the services to which the framework applies, the German Regulation refers directly to the Annex to the EU Directive.

[29] German Federal Office of Civil Protection and Disaster Assistance (2017) Services for modern civil protection, Rheinbach: WM Druck + Verlag, 30.
[30] Gesetz zur Änderung des Vergaberechts für die Bereiche Verteidigung und Sicherheit, *BGBl.* I 2011 S. 2570.
[31] Vergabeverordnung für die Bereiche Verteidigung und Sicherheit (VSVgV), *BGBl.* I S. 1509.

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

5. Use of drones for surveillance

One of the uses for drones envisioned within RESPONDRONE is surveillance. Indeed, drones can be equipped with video and audio equipment in order to allow first responders to assess a particular situation. In the case of forest fires, for instance, this can give first responders a better view over the spread of the fire and the affected area. When dealing with a building fire – such as for instance the 2019 fire in the Notre-Dame de Paris – drones can provide a much closer view that allows first responders to prioritize their actions.

However, the same technology can also pose a privacy risk. When using a drone to capture images, video and/or audio, it will almost inevitably also capture private persons. In such case, there will be a processing of personal data as to be understood under the EU's data protection framework. Moreover, it will affect a person's right to image. In this section, the relevant frameworks for these issues will be explored, and it will be assessed how RESPONDRONE can handle such situations.

5.1. The General Data Protection Regulation

5.1.1. From privacy to data protection

The right to privacy started to emerge at the end of the 18th century as a protection of personal communication and the inviolability of the personal home. In the second half of the 20th century, the right to privacy became enshrined in the major human rights instruments adopted in the frameworks of the United Nations and the Council of Europe, such as article 8 of the European Convention on Human Rights (ECHR).[32] Later on, the Organization for Economic Co-operation and Development (OECD) published guidelines on the protection of privacy and cross-border data flows.[33] This would lead to the idea of informational privacy.

On 24 October 1995, the European Union adopted Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.[34] With this directive, the EU implemented informational privacy in its data protection framework. Being a directive, this text had to be transposed by the Member States into national law by late 1998. Additional texts were adopted for privacy in the field of telecommunication

[32] Convention for the Protection of Human Rights and Fundamental Freedoms signed at Rome, 4 November 1950.
[33] OECD, Recommendation of the Council of 23 September 1980 concerning guidelines governing the protection of privacy and transborder flows of personal data.
[34] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data , *OJ* L 281 of 23 November 1995, 31-50.

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

(Directive 2002/58/EC[35]) and in the field of data retention (Directive 2006/24/EC[36]). The rights to privacy and data protection were also included in the Charter of Fundamental Rights of the European Union.[37]

However, the growth of the Internet and the rise of new business models – such as those used by Google and Facebook – have shown that the data protection framework had become insufficient in its existing form. The European Commission therefore proposed to replace the legal framework by a regulation. The main benefit is that a regulation can apply directly in all Member States, therefore not requiring national – and often deviant – implementation. This regulation, the General Data Protection Regulation, or GDPR, was adopted on 27 April 2016 and became applicable on 25 May 2018.[38]

5.1.2. Personal data

The GDPR applies to the processing of personal data. Article 4(1) defines such personal data as "*any information relating to an identified or identifiable natural person („data subject")".* An identified or identifiable natural person for the purposes of the GDPR 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 Article 29 Working Party – the current European Data Protection Board – has provided more guidance on this topic, which will be summarized here. [39]

First, '*any information*' is not tied the nature of the information and must be understood in the broadest sense. Any statement regarding a natural person can qualify, whether it be an objective statement – e.g. remarking on physical traits of a person – or a subjective one – e.g. remarking on a person's behavior. The content of the information can not only include the person's personal life but any situation – such as social or work-related settings. Last, the medium or format of the

[35] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *OJ* L 201 of 31 July 2002, 37-47.
[36] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, *OJ*. L 105 of 13 April 2006. 54-63. This directive was in 2014 annulled by the Court of Justice of the European Union.
[37] *OJ*. C 83 of 30 March 2010, 393.
[38] 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), *OJ* L 119 of 4 May 2016, 1-88.
[39] Article 29 Working Party (2007) "Opinion 4/2007 on the concept of personal data", *WP136*.

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

information is irrelevant, meaning that any kind of paper, electronic of magnetic information – such as video or computer code – can satisfy this element of the definition. Audio and video recordings are also information in this sense.

Second, the information must '*relate to*' a person. This means that it must be about that person and, therefore, there must be a relationship between the information and an individual. In some cases, this is fairly straightforward, for instance in the case of a HR-file of an employee. It can, however, also be less obvious, for instance where the value of a house does not directly say anything about a person but does provide insight in the financial status of its owner. According to the Article 29 Working Party, there must be clear content – in the sense that the information is obviously about a person – purpose – meaning that the information could be used to evaluate a person or to influence his status or behavior – or result – meaning that the information could have an impact on a person's rights and interests. Information can also relate to multiple persons, in which case only the elements relating to one person are personal data to that particular person and not the elements relating to another person.

Third, the information must make a person '*identified or identifiable*'. An identified person is distinguishable from other members in a group. An identifiable person has not been identified yet but could be identified. Identification can occur directly – meaning that it is made possible by information directly relating to that person – or indirectly – meaning that multiple pieces of information which do not directly relate to a person can be put together to identify that person. The threshold for putting together such information is any "*means reasonably likely to be used*".[40] That reasonableness is assessed by taking account "*of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments*".[41] One example is a dynamic IP address, which according to the Court of Justice of the European Union (CJEU) can be considered as personal data, since Internet service providers have the means that can reasonably be used to identify which person was using a particular dynamic IP address at a given time.[42] Such reasonableness can also evolve over time.[43] When, for instance, processed information is stored for a longer duration, technology may become available that does make identification reasonably likely. In that case, the threshold of personal data has been attained and the legal framework will apply. Given the rapid developments in data mining and machine learning, it is quite likely that data previously not considered as personal data may sooner or later become personal data.

Fourth, personal data concerns a '*natural person*'. Information on a company will therefore not be considered as personal data. Of course, in cases such as one-person companies, information on such company will include personal data on the owner of that company. A natural person

[40] Recital 26 GDPR.
[41] *Id.*
[42] CJEU, Breyer *v.* Bundesrepublik Deutschland, C-582/14, para. 31-49.
[43] Article 29 Working Party (2007) "Opinion 4/2007 on the concept of personal data", *WP136*, 15-17.

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

must furthermore be alive, meaning that information on deceased or yet unborn people does principally not qualify as personal data.

Fifth, pseudonymized information may still be considered as personal data. Article 4(5) GDPR defines pseudonymization as "*the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person*". Pseudonymization is normally reversible, meaning that upon reversal is will be possible to identify a natural person. Only when the pseudonymization is completely irreversible will it no longer be reasonably likely to identify a natural person. However, also here time is of the essence, as some techniques thought of as irreversible today, could later be proven to be reversible after all. Hashing has been recognized by the Article 29 Working Party as a pseudonymization technique.[44] Hashed personal data can therefore still be considered as personal data, since hashed data can still be linked to a natural person.[45]

Last, according to recital 26, the GDPR does not apply to anonymous information, "*namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable*". This means that any kind of information should be assessed on a case-by-case basis to ascertain whether it renders a natural person identified or reasonably likely to be identifiable. Only when the threshold of personal data is not met it be concluded that there is anonymous data falling outside of the scope of the GDPR. However, as shown in another opinion by the Article 29 Working Party, true anonymization is rare.[46] Many anonymization techniques can be reversed and can thus result in information that could make a natural personal reasonably identifiable. And again, technical evolutions must be taken into account.

5.1.3. Processing

The GDPR concerns the processing of personal data. Processing "*means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*".[47] This broad definition can cover practically anything that could be done with personal data. One example can

[44] Article 29 Working Party (2014) "Opinion 05/2014 on Anonymization Techniques", *WP 216*.
[45] Maxwell, W., Salmon, J. (2017) "A guide to blockchain and data protection", *Hogan Lovells,* 9.
[46] Article 29 Working Party (2014) "Opinion 05/2014 on Anonymization Techniques", *WP 216*.
[47] Article 4(2) GDPR.

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

be found in the *Google Spain* case, where the CJEU held that web-scraping by a search engine constitutes a processing operation.[48]

5.1.4. Data controller and processor

5.1.4.1. Notions

The data controller holds the final responsibility over the personal data processing operation. A controller is "*the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law*".[49]

A processor is "*a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*".[50] This is a party that can be used by the data controller to conduct the actual personal data processing. Also here the Article 29 Working Party has provided further guidance, which will be summarized in the following paragraphs.[51]

A data controller is either a natural or a legal person. When an employee processes personal data on behalf of its employer, the company will serve as the data controller.

The main task of the data controller is to determine the means and purposes of the personal data processing. The purpose provides the reason why personal data is to be processed, and the means determine how that should be done. Purpose and means of the processing are principally determined by the data controller. While the controller can delegate the non-essential aspects of the means to a processor, only the controller can decide on the purposes.

In a more complex personal data processing, there may be multiple co-controllers that jointly determine the means and purposes of that processing. Those co-controllers hold joint and equal responsibility over the processing, which is to be determined in a joint controller agreement.[52] However, when multiple controllers each determine their own means and purposes, they are sole data controllers for their own processing rather than joint controllers over a single processing.[53] Each processing must therefore be distinguished from one another, particularly when they appear to form a single processing.

---

[48] CJEU, Google Spain *v*. Agencia Española de Protección de Datos, C-131/12, para. 28.
[49] Article 4(7) GDPR.
[50] Article 4(8) GDPR.
[51] Article 29 Working Party (2010) "Opinion 1/2010 on the concepts of controller and processor", *WP 169*.
[52] Article 26 GDPR.
[53] See: Van Alsenoy, B. (2016) "Regulating Data Protection: The Allocation of Responsibility and Risk among Actors Involved in Personal Data Processing", *Doctoral thesis KU Leuven*, 53-62.

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

The GDPR assumes that the processor acts under delegation by the controller, which is to be determined in a controller-processor agreement. This agreement must show to what extent the processor can determine the means of the processing.[54] All processing activities must be recorded.[55]

5.1.4.2. Obligations

The GDPR determines a number of responsibilities of the data controller.

5.1.4.2.1. General obligations

The data controller must ensure that the general principles of personal data processing are respected. When consent is used as a processing ground, it must be proven that consent was freely obtained. The data controller must ensure that the free exercise of the rights of the data subject. Article 24 GDPR summarizes this as having to "*implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation*".

5.1.4.2.2. Data protection by design

According to article 25 GDPR, the data controller must implement appropriate technical and organizational measures designed to implement data protection principles in an effective manner and to implement safeguards to meet the requirements of this legal framework. In doing so, the data controller must consider the state of the art, the cost of implementation and the nature, scope, context and purposes of the processing, the risks of the processing and their likelihood to materialize and their potential impact on the rights and freedoms of the data subject. Such assessment must be made both when planning the processing and at the time of the processing itself.

Additionally, the data controller must implement appropriate technical and organizational measures to ensure that only the necessary personal data are processed by default. This relates to the principle of data minimization. Personal data may also not be made available to an indefinite amount of people without the data subject's intervention.

5.1.4.2.3. Security of the processing

Article 32 GDPR concerns the security of the processing. Appropriate technical and organizational measures must be implemented to ensure an appropriate level of security according to the risks

[54] Article 28 GDPR.
[55] Article 30 GDPR.

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

posed by the processing. The data controller must consider the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. As an example, such measures can include:

(a) the pseudonymization and encryption of personal data;
(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; or
(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

The appropriateness of a security level depends on the precise risks presented by a processing operation. Risks range from accidental or unlawful destruction, loss and alteration, to unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. Data controllers and processors must ensure that their employees handle personal data as instructed.

5.1.4.2.4. Data breach notification

A new principle under GDPR is the data breach notification. A data breach is a "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed*".[56]

Article 33 GDPR prescribes the procedure for data breach notifications. The notification duty does not apply when the breach is unlikely to result in a risk to the rights and freedoms of natural persons. Any personal data breach where there is such risk must be notified to the competent supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it. Later notifications must be reasoned. A processor should notify its controller without delay after becoming aware of a personal data breach. Any notification should at least:

(a) describe the nature of the personal data breach including, where possible, the categories and approximate number of involved data subjects and the categories and approximate number of personal data records concerned;
(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
(c) describe the likely consequences of the personal data breach; and
(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

[56] Article 4(12) GDPR.

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

When needed, this information can be provided in phases. Documentation must be maintained on data breaches, their effects and the remedial actions.

According to article 34, a data breach must be communicated to the data subject without undue delay when it is likely to result in a high risk to the rights and freedoms of those data subjects. Such communication must describe in clear and plain language the nature of the data breach and information on the breach and measures taken. Notification to the data subject is not needed when:

(a) the data controller has implemented appropriate technical and organizational protection measures, and if those measures were applied to the personal data affected by the data breach, particularly those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption;
(b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialize; or
(c) the communication would involve disproportionate effort. In such a case, a public communication or similar measure can be made whereby the data subjects are informed in an equally effective manner.

5.1.4.2.5. Data protection impact assessment

The impact of the processing operation on the protection of personal data must be subjected to a prior assessment, particularly when new technologies are used and when the processing – taking into account its nature, scope, context and purposes – is likely to result in a high risk to the rights and freedoms of natural persons. Article 35 GDPR provides that a data protection impact assessment (DPIA) is required when the processing concerns an automated processing providing systematic and extensive evaluation of personal aspects relating to natural persons and on which decisions are based that produce legal effects concerning the natural person; when conducting large-scale processing of special categories of data; or when systematically monitoring a publicly accessible area on a large scale. A public list of these operations is maintained by the supervisory authority.

A DPIA must contain:

1. a systematic description of the envisaged processing operations and the purposes of the processing;
2. an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
3. an assessment of the risks to the rights and freedoms of data subjects; and
4. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance, taking into account the rights and legitimate interests of data subjects and other persons concerned.

When the processing is required by law and if a general impact assessment was already conducted in adopting that legal basis, a DPIA is not necessary.

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

If the processing will result in a high risk, the controller should contact the supervisory authority. If the authority finds that the processing would infringe upon GDPR, or that the risks are insufficiently mitigated, it may provide a negative advice to the processing. Member States may allow authorities to require controllers to obtain prior authorization.

5.1.4.2.6. Data Protection Officer

When the processing is conducted by a public authority or body; when the core activities of the controller or the processor consist of 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 when the core activities of the controller or the processor consist of processing on a large scale of special categories of data and personal data relating to criminal convictions and offences, article 37 GDPR requires the designation of a data protection officer (DPO). A single DPO can be assigned at group level. Also, when not required by law, a DPO can be designated.

The DPO must demonstrate adequate professional qualities and knowledge of data protection law. A staff member or someone working through an external service contract can be designated as DPO. The contact details of the DPO must be communicated to the supervisory authority.

According to article 38 GDPR, the DPO must be involved – properly and timely – in all issues relating to the processing of personal data. He is supported by the data controller and processor and must work without instructions. Data subjects may contact the DPO with issues and for the exercise of their rights.

Article 39 GDPR provides that the DPO informs and advises the data controller or the processor; monitors compliance; provides advice where requested; cooperates with the supervisory authority; and acts as the contact point for the supervisory authority. The DPO minds the risk associated with processing operations, considering the nature, scope, context and purposes of processing.

5.1.4.2.7. Codes of conduct and certification

Codes of conduct or certification mechanisms can according to article 24(3) GDPR be used as elements to demonstrate compliance with the data controller's obligations. Certification mechanisms can also serve to prove compliance with the requirement of data protection by design, as well as with the security requirement and the DPIA requirement.

Article 40 GDPR encourages Member States, supervisory authorities, the European Data Protection Board and the European Commission to draft codes of conduct, minding the specific

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

features of various processing sectors and the specific needs of micro, small and medium-sized enterprises.

Associations and other bodies representing categories of data controllers or processors may prepare codes regarding fair and transparent processing; the legitimate interests of the data controller; the collection of personal data; the pseudonymization of personal data; the information provided to the public and to data subjects; the exercise of the rights of data subjects; the information provided to children and how parental consent is obtained; the data protection-by-default measures and procedures and the measures to ensure security; the notification of personal data breaches and the communication thereof to data subjects; the transfer of personal data to third countries; or out-of-court proceedings and other dispute resolution procedures. When associations draft their own codes, they must submit them to the competent supervisory authority. When approved, the supervisory authority will register and publish the code.

Data controllers and processors outside of the EU may also adhere to codes to provide appropriate safeguards for personal data transfers to third countries. They are required to make binding and enforceable commitments to apply appropriate safeguards. If the code relates to processing activities in multiple Member States, the code must be put before the European Data Protection Board. The European Commission may subsequently approve the code and publish it.

Supervisory authorities may, according to article 41 GDPR, accredit bodies to monitor compliance with a code of conduct. Such bodies must function independently, demonstrate expertise for their tasks, adopt procedures to carry out those tasks, be able to handle complaints about infringements of codes, and be free of conflicts of interests. Bodies may also take corrective measures, such as suspending or excluding a data controller or processor.

Article 42 GDPR provides that Member States, supervisory authorities, the European Data Protection Board and the European Commission encourage the establishment of data protection certification mechanisms and of data protection seals and marks, particularly for micro, small and medium-sized enterprises. Data controllers and processors outside of the EU can make binding and enforceable commitments to adhere to certifications or seals, in order to demonstrate adequate safeguards. Certification is voluntary and must be available via a transparent process. Certification does not reduce the responsibilities of the data controller or the processor. The European Data Protection Board publishes certification mechanisms and data protection seals and marks in a register. Certification is awarded through a certification body approved by the competent supervisory authority. Accreditation of certification bodies is regulated by article 43 GDPR.

Data controllers and processors must provide all information and access to their processing activities which are necessary to conduct the certification procedure. Certificates can be issued

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

for up to three years and can be renewed, under the same conditions, provided that the relevant requirements are still met. Certification can be withdrawn if the requirements for the certification are not or are no longer met.

5.1.5. Territorial scope

Article 3 GDPR determines that the legal framework "*applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not*". The data controller notion is therefore important to the territorial scope of GDPR. In determining whether there is an establishment in the EU "*both the degree of stability of the arrangements and the effective exercise of activities* […] *must be interpreted in the light of the specific nature of the economic activities and the provision of services concerned*".[57] To determine which local data protection authority is competent, the GDPR provides that the Member State where the main or single establishment is located will become the lead supervisory authority.[58]

If the data controller or processor is not established in the EU, GDPR can still apply if personal data of EU data subjects is processed, and if the processing activities are related to either the offering of goods or services to EU data subjects – for free or paid – or when the behavior of EU citizens within the EU is monitored. Factors to be taken into account in this assessment include the use of an official EU language, the display of prices in a European currency, and potential references to EU users or customers.[59] According to recital 24 GDPR, monitoring can include the tracking of Internet users. If there is no establishment within the EU, every national supervisory authority will have competence over the processing activities concerning its territory. According to article 27 GDPR, if the controller has no establishment in the EU, a representative within the EU must be designated.

5.1.6. General principles to process personal data

5.1.6.1. General principles

Every processing must comply with certain basic principles.[60]

5.1.6.1.1. Lawfulness, fairness and transparency

Personal data processing must in the first place be lawful. This means that any processing must be able to rely on one of the exhaustively listed processing grounds.

[57] CJEU, Weltimmo *v*. Nemzeti Adatvédelmi és Információszabadság Hatóság, C-230/14, para. 29.
[58] Article 56 GDPR.
[59] Recital 23 GDPR.
[60] Article 5 GDPR.

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

A fair balance to be struck between the data controllers and the data subjects. Fairness therefore aims to correct any power asymmetry between them. Additionally, any processing must meet the reasonable expectations of the data subject.

Last, transparency requires data subjects to be informed clearly and adequately about the processing of their personal data. Particularly the purposes of the processing and the applicable processing ground must be explicated. Such information enables the data subject in the exercise of its rights.

5.1.6.1.2. Purpose limitation

Personal data can only be "*collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes*". Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is not considered to be incompatible with the initial purposes.

Purpose limitation requires the data controller to establish *a priori* the purposes for which the personal data will be processed. Those purposes need to be sufficiently delineated in order to be specific. The purposes must be clearly communicated in order to be explicit. And to be legitimate, they must correspond with the legal expectations of the data subject.

Purpose limitation also aims to limit further processing. An example of further processing is when a company collects personal data on its clients for invoicing purposes, and later wants to use those contact details for marketing purposes. Further processing is only allowed if the purpose of the second processing operation is compatible with the purpose of the initial processing operation. When the purpose of the further processing is incompatible with the purpose of the initial processing, the further processing is considered as a fully separate processing operation, thus requiring its own purpose, processing ground, etc. According to recital 50 GDPR, the controller should, after having met all the requirements for the lawfulness of the original processing, "*take into account, inter alia: any link between those purposes and the purposes of the intended further processing; the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations*".

5.1.6.1.3. Data minimization

Personal data must be "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*". The assessment of necessity is made according to whether the processed personal data is suitable to achieve the purposes of the processing, and

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

whether the processing is reasonable to achieve those purposes. If the intended purpose could be attained with lesser amounts of personal data, or without personal data altogether, the processing fails the necessity test. The collected personal data must also be proportionate to the purposes of the processing. This means that no more data can be collected than is necessary and the data may also not be stored longer than is necessary. Article 11 GDPR provides that if the purposes of the processing are met, no further personal data should be kept solely for the purposes of GDPR-compliance.

5.1.6.1.4. Accuracy

Personal data must be "*accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay*". The data controller must therefore ensure that the processed personal data is accurate. When inaccuracies are found, these must be corrected.

5.1.6.1.5. Storage limitation

Personal data must be "*kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed*". Longer storage can be allowed if the personal data is processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes and subject to implementation of appropriate technical and organizational measures adopted in the margin of GDPR to safeguard the rights and freedoms of the data subject.

The data controller must therefore clearly state, in advance to the processing, for how long the personal data must be stored to achieve the purposes of the processing. Once those purposes are achieved, the data should be deleted or fully anonymized. However, legislation may require certain data to be kept longer than needed for the purposes of the processing. For instance, VAT law requires invoices to be kept for seven years. As invoices may contain personal data, their longer storage is therefore justified for the entire legally mandated retention period.

5.1.6.1.6. Confidentiality and integrity

Personal data must be "*processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures*". The data controller must therefore adopt a certain security strategy.

5.1.6.1.7. Accountability

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

The data controller holds the final responsibility over the processing, including the responsibility to demonstrate compliance with the abovementioned principles. This requires a proactive attitude to comply with the principles of the GDPR and to document such compliance.

5.1.6.2. Processing grounds

As noted, personal data can only be lawfully processed when one of the processing grounds applies. Article 6 GDPR list six grounds.

First, personal data can be processed upon consent of the data subject. Consent is defined as "*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*".[61] Article 7 GDPR further specifies consent. Consent must be documented, as it must be proven that consent was given. When consent is asked in writing, the request thereto must be intelligible and easily accessible, distinguished from other matters, and in plain and clear language. Consent can be withdrawn, without invalidating any processing based on that consent prior to withdrawal. Most importantly, consent must be freely given. A service for which consent is not necessary may therefore not be made conditional on granting consent. Doing so would limit the freedom with which the data subject provides consent. In the case of obvious power asymmetries – such as an employer-employee relationship – it may be questioned whether consent can truly be freely given. Minors under the ages of between 13 and 16 years, depending on the Member State, must be authorized by the holder of parental responsibility.[62]

Second, personal data can be processed when necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering into such contract.

Third, personal data can be processed when necessary for compliance with a legal obligation to which the controller is subject.

Fourth, personal data can be processed to protect the vital interests of the data subject or of another natural person.

Fifth, personal data can be processed when necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

Sixth, personal data can be processed when necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the

[61] Article 4(11) GDPR.
[62] Article 8 GDPR.

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

interests or fundamental rights and freedoms of the data subject, particularly where the data subject is a child. This processing ground is a more nuanced one, as it requires a prior assessment balancing the interest of the controller against the potential impact of the processing on the data subject, taking into account additional safeguards and measures to limit that impact.[63] Therefore, having a legitimate interest alone is not sufficient to be able to use this processing ground, the balancing exercise is always required.

5.1.6.3. Sensitive personal data

Apart from regular personal data, there is also sensitive personal data – or special categories of personal data –which is subjected to stricter requirements. Article 9 GDPR principally prohibits the processing of such sensitive personal data, defined as "*revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of 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*".

There are, however, deviations to the principal prohibition. As under article 6, there are a number of processing grounds under which sensitive personal data can be processed:

(a) When the data subject has given explicit consent, unless prohibited by a certain Member State;
(b) When processing is necessary for carrying out obligations and specific rights of the controller or data subject in the field of employment and social security;
(c) When necessary to protect the vital interests of the data subject or another natural person where the data subject is physically or legally incapable of giving consent;
(d) When carried out for legitimate activities by a foundation, association or another non-profit body with political, philosophical, religious or trade union aims and if the processing relates to their members or former members;
(e) When processing relates to personal data manifestly made public by the data subject;
(f) When processing is necessary for the establishment, exercise or defence of legal claims or when courts act in their judicial capacity;
(g) When processing is necessary for reasons of substantial public interest and when it respects the essence of the right to data protection and provides suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
(h) When processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services or pursuant to contract with a health professional;
(i) When processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices and with suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

[63] For guidance on this matter, see: Article 29 Working Party (2014) "Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC", *WP 217.*

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

(j) When processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes and is proportionate to the aim pursued, respects the essence of the right to data protection and provides for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Member States may also further limit the processing of health, genetic and biometric data. Processing of data relating to criminal convictions and offences is limited as well and can only be conducted under the control of official authorities or when authorized by Member State law.[64]

5.1.7. Data subject's rights

Chapter III of the GDPR determines the data subjects' rights. According to article 23 of the GDPR, these rights can be restricted by law, as long as the essence of fundamental rights and freedoms is respected and the restriction is necessary and proportionate to safeguard matters such as national and public security, defence, crime prevention, the public interest, etc.

5.1.7.1. Right to information

Article 12 GDPR provides that the data controller must take appropriate measures to ensure transparency of the processing, in a concise, transparent, intelligible and easily accessible form, using clear and plain language, particularly for information addressed to a minor. The exercise of the data subject's rights must be ensured by the data controller. A response must be provided within one month of receipt of a request, which can be extended by another two months where needed. Absent any action, the data subject must be informed within one month. When an information request is manifestly unfounded or excessive, in particular because of its repetitive character, a reasonable fee may be charged, or the request may be refused. When reasonable doubts exist on the requesting person's identity, the data controller may request additional identifying information.

When personal data is collected from the data subject, article 13 GDPR will apply. The data subject must be provided with the identity and the contact details of the controller; contact details of the data protection officer; the purposes of the processing and their legal basis; the legitimate interests, if the processing is based thereon; the data storage period; the recipients or categories of recipients of the personal data; and any potential transfer to third countries, unless that information is already known. Additionally, the data subject must be informed on applicable rights, such as the right to access, to rectification, to erasure, to restrict the processing, and to data portability. When the processing ground is that of consent, it must be communicated how consent can be withdrawn. A complaint can be filed with the competent supervisory authority. The existence of automated decision-making processes, including profiling, and any further processing must be communicated too.

[64] Article 10 GDPR.

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

When the personal data is not obtained from the data subject, article 14 GDPR applies. Here, similar information must be provided, together with an overview of the processed personal data and its origins. This information must be provided within one month after obtaining the personal data at the latest. When this personal data is used to communicate with the data subject, the information must be provided at the latest at the time of the first communication. When the personal data will be disclosed to another recipient, this must be communicated at the latest when the personal data is first disclosed. When the data subject already has this information; when the provision of such information proves impossible or would involve a disproportionate effort – in which case appropriate measures to protect the data subject's rights and freedoms and legitimate interests must be taken – when obtaining or disclosure is expressly laid down by law; or when the personal data must remain confidential subject to an obligation of professional secrecy, this notification duty will not apply.

5.1.7.2. Right of access

The right of access is defined by article 15 GDPR. The data subject has the right to obtain confirmation as to whether personal data concerning him or her is being processed. If so, the data subject receives access to the data. Information must also be provided on the purposes of the processing, which data is processed, to whom it is disclosed, how long the data will be stored, the data subject's rights, and legal recourses. A copy of the processed data must be provided. Further copies may be subject to a reasonable fee.

5.1.7.3. Right to rectification

A right to rectification is provided by article 16 GDPR. The data subject has the right to obtain without undue delay the rectification of inaccurate personal data. This also covers the right to demand completion of incomplete personal data, including by means of providing a supplementary statement.

5.1.7.4. Right to erasure

The right to erasure, more popularly known as the right to be forgotten, can be found in article 17 GDPR. The data subject can demand any personal data processed to be erased without undue delay. This right only applies in the following circumstances:

(a) When the personal data are no longer necessary for the purposes of their processing;
(b) When the data subject withdraws consent if the processing was based on consent;
(c) When the data subject objects to the processing and there are no overriding legitimate grounds for the processing;
(d) When the personal data have been unlawfully processed;
(e) When the personal data are to be erased for compliance with a legal obligation; or
(f) When the personal data have been collected in relation to the offer of information society services.

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

When personal data have been made public, the controller must take reasonable steps to inform other controllers that the data subject has requested the erasure of any links to, or copy or replication of, that personal data.

The right to erasure does not apply when the processing is necessary:

(a) for exercising the right of freedom of expression and information;
(b) for compliance with a legal obligation which requires processing or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(c) for reasons of public interest regarding public health;
(d) for archiving purposes in the public interest, for scientific or historical research or statistical purposes; or
(e) for the establishment, exercise or defence of legal claims.

5.1.7.5. Right to restriction of processing

The data subject can demand the processing to be restricted according to article 18 GDPR. This applies when the accuracy of the personal data is contested, when the processing is unlawful, when the personal data is no longer needed for the purposes of the processing but still required for the establishment, exercise or defence of legal claims, and when the data subject has objected to processing pending verification whether the legitimate interests of the controller override those of the data subject. After a restriction, the data can only be stored. Any other processing requires the data subject's consent, or must be deemed necessary for the establishment, exercise or defence of legal claims, for the protection of the rights of another person, or for reasons of important public interest. The data subject must inform the controller when the restriction is lifted.

Additionally, a notification obligation is provided by article 19 GDPR. This means that any rectification, erasure, or restriction must be notified to each recipient of the personal data, unless such proves impossible or involves disproportionate effort.

5.1.7.6. Right to data portability

The right to data portability is provided by article 20 GDPR. A data subject can receive in a structured, commonly used and machine-readable format all relevant personal data in order to transmit that data without hindrance to another data controller.

Data portability is possible when the processing is based on consent, or when the processing is conducted by automated means. If technically feasible, the data subject has the right to transmit the personal data directly from one data controller to another. Data portability does not preclude the right to erasure, nor can it adversely affect the rights and freedoms of others.

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

5.1.7.7. Right to object

The right to object can be found in article 21 GDPR. A data subject can object, for reasoned grounds, to the processing of personal data when that processing is based on the public interest or the legitimate interests of the data controller. As a result, the data controller can no longer process that personal data, unless it can be proven that compelling legitimate grounds override the interests, rights and freedoms of the data subject.

When processing personal data for direct marketing purposes, an objection can be filed at any time. Following such objection, personal data may no longer be processed for direct marketing purposes. When using information society services, the data subject can also object to automated processing using technical specifications.

Processing for scientific or historical research purposes or statistical purposes can be objected to as well, on reasoned grounds, unless such processing is necessary for the performance of a task carried out for reasons of public interest.

5.1.7.8. Automated decision-making

The data subject should not to be subjected to a decision based solely on automated processing, including profiling, if such processing produces legal effects or similarly significantly affects the data subject, according to article 22 GDPR. This does not apply when such processing is necessary for entering into or the performance of a contract, when such processing is authorized by law, and when the processing is based on the data subject's explicit consent.

Suitable measures must be implemented to safeguard the data subject's rights and freedoms and legitimate interests, including the right to obtain human intervention and to express the data subject's point of view and to contest the decision. Automated decisions cannot be based on special categories of personal data, unless suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

5.1.8. Transfers to third countries

Processed personal data concerning EU citizens must remain at a jurisdiction offering sufficient guarantees to safeguard the rights and freedoms of those citizens. Transfers to third countries, being data transfers outside the EU, are possible when the level of protection of natural persons guaranteed by the GDPR is not undermined.[65]

According to article 45 GDPR, such level of data protection can be ensured by adequacy decisions. These let the European Commission decide whether a third country ensures an adequate level of

[65] Article 44 GDPR.

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

protection. The European Commission assesses that adequacy by taking into account elements such as the rule of law and respect for human rights and fundamental freedoms, local data protection laws, the presence and effectiveness of local independent supervisory authorities, and international commitments of that third country. If a third country is found to offer an adequate level of data protection, the European Commission may adopt an adequacy decision by means of an implementing act. Such decision is subject to periodic review. Developments that can affect its decisions will be monitored, and decisions can be amended, suspended or repealed. Consultations with a third country can be held to remedy a situation that would lead to such action.

Transfers to a third country can still be allowed even without an adequacy decision if the data controller or processor has provided appropriate safeguards, and on the condition that enforceable data subject rights and effective legal remedies for data subjects are available.[66] Appropriate safeguards can be offered through legally binding and enforceable instruments between public authorities or bodies, binding corporate rules, standard data protection clauses, approved codes of conduct, or approved certification mechanisms. Appropriate safeguards can also be provided through contractual clauses between the data controller and processor, or by provisions inserted into administrative arrangements between public authorities that include enforceable and effective data subject rights.

Article 47 GDPR governs binding corporate rules. These can be allowed if they are legally binding, if they expressly confer enforceable rights on data subjects, and if they fulfil certain requirements. Those requirements include specifying a structure and contact details of a group of undertakings engaged in a joint economic activity, the data transfers or set of transfers, their legally binding nature, the application of the general data protection principles, the rights of data subjects, the acceptance of liability for any breaches of binding corporate rules, how information on the binding corporate rules is provided, the tasks of any data protection officer, the complaint procedures, mechanisms for ensuring verification of compliance with binding corporate rules, mechanisms for reporting and recording changes to the rules, cooperation and reporting mechanisms with supervisory authorities, and appropriate data protection training to personnel. The European Commission can further specify the format and procedure for information transfers under binding corporate rules.

Court judgments requiring transfers or disclosures of personal data can only be recognized or enforced if based on an international agreement, such as a mutual legal assistance treaty, between the requesting third country and the EU.[67]

[66] Article 46 GDPR.
[67] Article 48 GDPR.

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

There are, however, a number of derogations.[68] Transfers to a third country are possible – even without adequacy decision, binding corporate rules or appropriate safeguards – if the data subject has explicitly consented to the proposed transfer, if the transfer is necessary for the performance of a contract, if the transfer is necessary for important reasons of public interest, if the transfer is necessary for the establishment, exercise or defence of legal claims, if the transfer is necessary in order to protect the vital interests of the data subject or of other persons, or if the transfer is made from a register which according to law is intended to provide information to the public and which is open to consultation either by the public or by anyone who can demonstrate a legitimate interest. When these derogations are not applicable, transfers are only possible if the they are not repetitive, if they concern only a limited number of data subjects, if they are necessary for the purposes of compelling legitimate interests pursued by the controller, and if the data controller has assessed all circumstances surrounding those data transfers and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The supervisory authorities must be informed of such transfers.

The European Commission and supervisory authorities must take appropriate steps to develop international cooperation mechanisms, provide international mutual assistance in the enforcement of data protection legislation, engage relevant stakeholders, and to promote the exchange and documentation of personal data protection legislation and practice.[69]

5.2. Image rights and security cameras

Apart from the rights to privacy and data protection, there is also the right of the citizen relating to the depiction of the person. The right to depiction provides that every natural citizen retains all rights regarding depictions of that person, thus requiring consent in order to use any of such depictions. However, in certain cases – such as filming at a public location – and under certain conditions, consent can be assumed. This individual right can also be extended to the closest relatives of the protected person in order to preserve the privacy and integrity of the family against unauthorized use of the depiction of the protected person.

The right to depiction protects the image of the person and certain characteristics of that person's looks, such as a specific style of hair and clothing. Note that this protection only extends to external features and does not cover internal features such as the person's character. In order for a person's right to depiction to be violated, the depiction that is used without authorization needs to depict the person in a recognizable manner. While the threshold for 'recognizable' is not clearly defined and left open to the discretion of the judge, reference can be made here to the concepts of 'identified' and 'identifiable' within data protection.

[68] Article 49 GDPR.
[69] Article 50 GDPR.

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

The right to depiction is not limited to a particular form, which means it includes all photographic images, video and even sculptures and statues. The precise techniques used for producing or storing the depiction are irrelevant, which means that also live video streams – as can be used by drones – that are not permanently stored are also included under the scope of this protection.

The right to depiction can be invoked against everyone, thus applying *erga omnes*. Generally, this means that all use of a natural person's depiction requires this person's consent. Important is that only the 'use' of such depictions require the protected person's consent. When there is no 'use', there is also no need for consent. As reproduction can be considered as a form of use, it requires the consent of the protected person. Even if this person has already given consent to produce an image, the later reproduction will thus require additional consent. Publishing and sharing a depiction on the Internet can also be considered as a form of use, which can easily lead to unauthorized reproduction.

As is the case for the informed consent in the context of data protection, the protected person's prior consent for the use or reproduction of a depiction needs to be given explicitly and out of free will. This consent also needs to be certain and cannot be dubious. In case of doubt, consent cannot be assumed. However, this consent is not bound to any formalities and therefore does not need to be provided in writing, although for probative purposes written consent may be preferred. Consent can be retracted, thus stopping all future uses or reproductions.

When the audio and video equipment on a drone is used for security purposes, being the surveillance and monitoring of areas, specific legislation may apply. In Belgium, for instance, there is the Camera Act[70] which regulates the use of fixed and mobile security cameras. A drone can be considered as a mobile security camera.[71] More specifically, the Act applies to the use of such security cameras to prevent, to establish or to track down crimes against people or goods, or public nuisance (article 3). Public authorities can use mobile security cameras for certain purposes of license plate recognition in public spaces (article 7/1). Access to the captured images is highly restricted (article 9). This Act does not apply when specific legislation foresees in the use of cameras by public authorities.

5.3. Privacy, GDPR and drones

There are several ways in which the operation of drones can affect citizens' privacy or entail a processing of personal data. The most obvious is the equipment of a drone with a camera. This camera will often not only be able to record videos and sound, it may also be capable to zoom in on images, to recognize faces or number plates, or to detect movement.[72] Also other types of

[70] Act of 21 March 2007 regulating the placement and usage of security cameras, *Belgian State Gazette* 31 May 2007.
[71] As confirmed by the Belgian Data Protection Authority:
[72] European Data Protection Supervisor (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 -

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

sensors that can be used in drones could reveal information on a natural person that could identify that person or make that person identifiable. For instance, a drone could detect Wi-Fi networks, read IP addresses, have biometric sensors, provide GPS tracking, etc. According to the European Data Protection Supervisor (EDPS), a drone could process more personal data than a manned flight could, as its sensors are more advanced than the human eye and given that drones have added discreetness and mobility.[73] As a result, drones must be operated with respect to the fundamental rights of citizens, including that of data protection.

5.3.1. Privacy

According to established case law, the right to privacy can also apply in a public context.[74] Therefore, even when an individual is in a public space, there can still be a reasonable expectation of privacy. This would protect the individual from being targeted by drones, for instance by being tracked. Also the right to data protection applies in a public space, whenever there is a processing of personal data. These rights therefore protect the individual from possible intrusion by drones, whether it be in their own home or in public spaces.

On the other hand, the privacy risks when first responders operate drones in the specific scenarios that they encounter are not the same as when drones are used on a wide scale for police and surveillance purposes. A study conducted for the European Commission found that drones operated by first responders pose a low risk for chilling effect, body privacy, data minimisation, proportionality, purpose limitation, accountability, data security, data subjects' rights and dehumanization, and a medium risk for transparency, visibility, location privacy, privacy of association and function creep.[75] The main reason for these findings is that first responders will normally only operate drones in specific scenarios that require their use, and that such operations will be in the public interest. Only for consent a high risk was identified, as data subjects involved cannot consent to the operation.

5.3.2. GDPR

With regard to data protection, it is clear that when the use of a drone involves the processing of personal data, that the principles of the GDPR will have to be complied with. This has consequences for both drone manufacturers and drone operators.

Opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner"", *edps.europa.eu*, 4.

[73] *Ibid.*, 5.

[74] ECHR, Von Hannover *v* Germany, 40660/08 and 60641/08, §95.

[75] Finn, R., Wright, D., Jacques, L., De Hert, P. (2014) "Study on privacy, data protection and ethical risks in civil Remotely Piloted Aircraft Systems operations - Final Report", *ec.europa.eu,* 231-.

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

When manufacturing a drone, the principles of data protection-by-design and data protection-by-default should be taken into account. This means that the drone should be fit to purpose. A drone that only needs to map forest fires does not necessarily need a high-resolution camera that can identify people or license plates.[76] Sensors need to be able to be switched on and off, so that they are used only when needed. Automatic pixelation of faces could be foreseen if identification of people is not needed.

Also, the operation of drones must comply with GDPR. For first responders, the most likely processing ground to be used will be that of necessity of the processing for the public interest. Before the use of drones with a potential high impact on the rights of data subjects, a DPIA will be needed to determine what the drone needs to accomplish. It then needs to be decided how the drone can be operated with respect to the rights of the data subjects involved. The principles of necessity and proportionality must be preserved. The operator of the drone will in most cases serve as data controller, which in the context of RESPONDRONE will be first responders. It is, however, also possible that a third party operates a drone on behalf of first responders. In such case, the operator will be the processor and a suitable controller-processor agreement must be in place.

The data controller must ensure that the data subjects involved can exercise their rights. However, article 23 GDPR allows for Member States to restrict those rights as "*a necessary and proportionate measure in a democratic society to safeguard*", amongst others, national security and defence, public security, and other important objectives of general public interest of the Union or of a Member State. Where a drone operation by first responders is planned, it must therefore be assessed whether the Member State in which the operation takes place has indeed adopted such restrictions and whether any of those restrictions can apply to that particular operation.

[76] European Data Protection Supervisor (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"", *edps.europa.eu*, 15.

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

6. Use of radio spectrum

RESPONDRONE aims to equip drones with wireless communication technology. This allows the drones to provide network coverage in areas where the network has been disabled due to disaster. The goal is to provide first responders with wireless access to LTE, 5G-NR and other technologies. This is described in section 1.3.2.4.2 of the DoA [DoA]. The use of broadband technologies will provide numerous advantages over the existing Terrestrial Trunked Radio (TETRA) communication used by first responders.

The use of the radio spectrum is closely regulated. The reason for this is that the radio spectrum is a rival good, meaning that it cannot be depleted, but overuse can result in interference. To limit such interference, the radio spectrum has been divided into bands, with each band being allocated to a particular use. Mobile communication technologies – such as LTE and 5G-NR – are therefore confined to a predefined number of bands. This high-level division of the radio spectrum has been agreed to within the framework of international organizations such as the International Telecommunication Union (ITU), having 193 Member States, and at the regional European level, through the European Conference of Postal and Telecommunications Administrations (CEPT), with 48 Member States. Within the EU, telecommunications rules are mainly provided by the recently adopted Electronic Communications Code, replacing the former patchwork of several directives in the field of telecommunications.

Access to those radio spectrum bands is mainly regulated by the Member States. There are several options to allow access to a radio spectrum band. One is that of the general authorization. In this system, access to the radio spectrum band is in principle open to everyone, be it that certain conditions will apply to limit interference. Second, there is the individual authorization. In this system, access to a (part of a) radio spectrum band will be possible only for those that obtained a license thereto. There are several ways in which such a license can be granted. It could be granted on a first-come-first-serve basis, using a lottery or beauty contest, etc. However, the option used mostly by governments today – for instance in granting 5G licenses – is that of the auction, in which the highest bidder will be granted the license. Several EU Member States have already conducted their 5G auctions, resulting in significant revenues for those Member States.

The result of this background for RESPONDRONE is that there are three main possibilities for first responders to gain access to radio spectrum usage rights using existing commercial technologies such as LTE and 5G-NR. These possibilities are detailed in the following subsections.

6.1. Band reservation

First, Member States can reserve part of the radio spectrum to first responders, something which is already a well-established practice. In the US, for instance, the Federal Communications Commission (FCC) has reserved several frequencies to first responders, such as police, fire

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

fighters and Emergency Medical Service (EMS) providers.[77] Some of these frequencies are licensed to the First Responder Network Authority (FirstNet), which is tasked with building and operating a nationwide broadband public safety network. Similarly, the UK's Ofcom has reserved some frequencies to first responders.[78] This is a practice followed all over the EU. Furthermore, within Europe first responders can use the TETRA network, generally found in the 380MHz - 430MHz range.

However, the frequencies reserved to first responders are generally the frequencies used by specialized trunked radio equipment used by first responders – such as those needed under TETRA. Commercial mobile technologies, such as LTE and 5G-NR, require different frequencies to operate. The frequencies traditionally reserved to first responders can therefore not provide them with access to mobile technologies such as LTE and 5G-NR.

There is some practice with regard to providing first responders with access to commercial mobile networks. In Belgium, for instance, the national operator for emergency and security communications services, ASTRID, is now operating a mobile virtual network (MVN) called Blue Light.[79] Users of Blue Light – first responders – get access to the traditional commercial mobile communications networks. Normally Blue Light uses the network of commercial operator Proximus but can automatically switch to the other two mobile networks – Orange and Base – when needed. Furthermore, Blue Light receives priority on the Proximus network, in order to ensure its use by first responders in situations of network disruption or congestion.

While such initiatives can indeed provide first responders with access to commercial mobile communications technologies, the status of a MVNO does still, in principle, not allow first responders to start operating their own broadcasting equipment, as would be the case with a drone equipped with a radio antenna. For such use, additional measures are required. There are two main options here.

First, the first responder MVNO could negotiate with the commercial network operators with which it is affiliated the right to operate mobile network equipment through the use of drones in a particular operation. This is, of course, subject to the license of that mobile network operator including the use of mobile antennas.

Second, separate permissions could be foreseen by law to first responders to operate mobile networks using drones in their operations. This could be an extension of the rights foreseen in the current allocation of certain frequencies to first responders.

[77] https://www.fcc.gov/public-safety/public-safety-and-homeland-security/policy-and-licensing-division/public-safety-spectrum.
[78] https://www.ofcom.org.uk/__data/assets/pdf_file/0021/103296/fat-emergency-services.pdf.
[79] https://www.astrid.be/nl/diensten/blue-light-mobile.

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

6.2. Primary market

Second, first responders could obtain radio spectrum usage rights on the primary market. In this scenario, first responders would gain radio spectrum usage rights – including the right to operate their own radio antennas – in the same way any commercial network operator does.

The main benefit of this approach is that it would give first responders the widest possibilities, as they can gain full radio spectrum access rights, as well as the rights to operate the necessary mobile equipment.

However, this would put first responders in direct competition with commercial network operators in license auctions. Given the significant sums paid by those network operators and given the non-profit nature of first responders, this option can be considered as financially unfeasible.

6.3. Secondary market

Third, first responders could obtain radio spectrum usage rights on the secondary market. Article 51 of the EU Electronic Communications Code[80] allows the holders of radio spectrum usage rights to transfer or lease (part of) their rights to other actors.

Essentially, this would mean that first responders could negotiate such transfer or lease – according to their specific needs – with incumbent mobile network operators. This transfer or lease can include the rights to operate their own (mobile) network equipment.

This option goes further than the aforementioned example of the Belgian Blue Light network. With Blue Light being an MVNO, the usage rights remain fully with the network operator – *in casu* Proximus. Blue Light's usage rights are therefore fully regulated by its agreement with that operator. The actual prioritization of its communications will thus still be up to whether the mobile network operator fulfils its side of the bargain. A lease or transfer could, in this example, give Blue Light full rights to a section of the frequency bands to which it would need access to operate a drone establishing a LTE or 5G-NR network. Prioritization would therefore be ensured, as only Blue Light users – being first responders – would be able to use that segment.

Such lease or transfer would, of course, be more financially feasible to negotiate than having first responders launch a bid on the primary market, as discussed in section 6.2. It would furthermore ensure that first responders gain usage rights themselves, rather than being subject to a more limited arrangement such as a MVNO. Last, it would allow first responders to operate their own mobile communications antennas, such as those envisioned by RESPONDRONE.

[80] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, *OJ* L 321 of 17 December 2018, 36-214.

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

7. Transport of medical goods

The transport of medicinal products and blood is subject to certain rules, particularly with regard to the storage duration and temperature. When using these products as payload to a drone, they will have to be stored in a container suitable for such products, according to EU law.

7.1. Medicinal products

In 2001, the EU adopted a directive on medicinal products for human use.[81] Article 1(2) of the directive defines medicinal products as *"(a) any substance or combination of substances presented as having properties for treating or preventing disease in human beings; or (b) any substance or combination of substances which may be used in or administered to human beings either with a view to restoring, correcting or modifying physiological functions by exerting a pharmacological, immunological or metabolic action, or to making a medical diagnosis*".

According to article 1(3), such substance may include human blood and human blood products. However, according to article 3(6), the directive does not apply to "*whole blood, plasma or blood cells of human origin, except for plasma which is prepared by a method involving an industrial process*". Medicines that include or are derived from blood are therefore covered by this directive, while blood in itself is not.

Title IV regulates the manufacture and importation of medicinal products. According to article 40, the general principle of that the manufacture of medicinal products is subject to prior authorization. Article 46b provides that Member States must "*take appropriate measures to ensure that the manufacture, import and distribution on their territory of active substances, including active substances that are intended for export, comply with good manufacturing practice and good distribution practices for active substances*". Importers, manufacturers and distributors of active substances established in the EU must be registered with the competent authority of the Member State in which they are established (article 52a). Competent authorities may hold inspections.

Title VII regulates the wholesale distribution and brokering of medicinal products. According to article 76, any import must be notified. Article 84 authorizes the European Commission to adopt guidelines on good distribution practices.

[81] Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community code relating to medicinal products for human use, *OJ* L 311 of 28 November 2001, 67-128. Note that this directive has been amended several times. Our findings are therefore based on the at the time of writing consolidated version: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02001L0083-20190128.

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

In 2013, the European Commission adopted guidelines Good Distribution Practice of Medicinal Products for Human Use.[82] With regard to transport, it is determined in article 9.2 that the required storage conditions for medicinal products should be maintained during transportation within the defined limits as described by the manufacturers or on the outer packaging. The wholesale distributor must ensure that vehicles and equipment used to distribute, store or handle medicinal products are suitable for their use and appropriately equipped to prevent exposure of the products to conditions that could affect their quality and packaging integrity. When non-dedicated vehicles and equipment are used, procedures must be in place to ensure that the quality of the medicinal product will not be compromised. Written procedures must be in place to document and arrange this. Article 9.3 provides that medicinal products must be transported in containers that have no adverse effect on the quality of the products, and that offer adequate protection from external influences, including contamination. In 2015, additional guidelines were provided for the distribution of active substances for medicinal products.[83] While these principles only apply to wholesale distributors, they do provide information on what the EU expects from transport and storage of medicinal products.

Apart from direct legislation, industry norms may apply as well. One example is the DIN 58345 norm for pharmaceutical refrigerators. Such refrigerators must have an operating temperature between +2°C and +8°C, in ambient temperatures between +10°C and +35°C. Noise emission must remain below 60dB. Optical and acoustic alarms must warn when operating temperature thresholds are crossed, or when there is a power failure. Operating temperatures must be recorded. A safety thermostat must prevent freezing temperatures. Internals must have a load capacity of 100kg/m^2. The door must be lockable. Remote maintenance must be possible through a potential-free contact.

7.2. Blood

A 2002 directive regulates the collection, testing, processing, storage and distribution of human blood and blood components.[84] Article 5 provides that blood establishments must be accredited. With regard to storage, transport and distribution, article 22 provides that the European Commission can adopt further technical requirements.

[82] Guidelines of 7 March 2013 on Good Distribution Practice of Medicinal Products for Human Use (2013/C 68/01), *OJ* C 68 of 8 March 2013, 1-14.

[83] Guidelines of 19 March 2015 on principles of Good Distribution Practice of active substances for medicinal products for human use (2015/C 95/01), *OJ* C 95 of 21 March 2015, 1-9.

[84] Directive 2002/98/EC of the European Parliament and of the Council of 27 January 2003 setting standards of quality and safety for the collection, testing, processing, storage and distribution of human blood and blood components and amending Directive 2001/83/EC, *OJ* L 33 of 8 February 2003, 30-40.

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

Those technical requirements were included in a 2004 Commission directive.[85] Annex IV of that directive lays down the requirements for storage, transport and distribution of blood. This Annex provides storage durations and temperatures for blood and different blood components:

- Red cell preparations and whole blood (if used for transfusion as whole blood) | + 2 to + 6 °C | 28 to 49 days according to the processes used for collection, processing and storage
- Platelet preparations | + 20 to + 24 °C | 5 days; may be stored for 7 days in conjunction with detection or reduction of bacterial contamination
- Granulocytes | + 20 to + 24 °C | 24 hours.

[85] Commission Directive 2004/33/EC of 22 March 2004 implementing Directive 2002/98/EC of the European Parliament and of the Council as regards certain technical requirements for blood and blood components, *OJ* L 91 of 30 March 2004, 25-39.

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

8. Security aspects

The EU has adopted a directive on the security of network and information systems (NIS) in 2016.[86] Recognizing the societal and economic importance of network and information systems, and the growing magnitude, frequency and impact of attacks on such systems, the directive aims to establish a minimum level of security for such systems across the EU, particularly for those operating essential services and digital service providers. Member States can further add entities to the list provided by the directive (recital 19). Member States may adopt stricter rules as well, given that the directive only aims at minimal harmonization (article 3).

The main goals of this legal framework are established in article 1(2):

1. Establishing obligations on the Member States to adopt a national strategy on the security of network and information systems;
2. Coordination and cooperation between Member States through a Cooperation Group and a CSIRT Network; and
3. Creating a culture of security for essential services and for digital service providers through national competent authorities, single points of contact and CSIRTs (Computer Security Incident Response Teams) with tasks related to the security of network and information systems.

Where personal data is processed, the principles of GDPR must be taken into account (article 2).

The NIS Directive defines network and electronic information systems as:

> *"(a) an electronic communications network within the meaning of point (a) of Article 2 of Directive 2002/21/EC;*
> *(b) any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data; or*
> *(c) digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance"* (article 4(1)).

Security, in turn, means "*the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems*" (article 4(2)). Digital services relate to online marketplaces, online search engines, and cloud computing services (Annex III).

[86] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, *OJ* L 194 of 19.7.2016, 1-30.

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

Annex II of the directive defines the operators of essential services (article 5(1)). These include air transport authorities and healthcare providers, as defined in Directive 2011/24/EU. It is therefore possible for a Member State to apply this framework to certain services of first responders, or to certain drone services. In deciding on this, Member States must take into account that essential services are services essential for the maintenance of critical societal and/or economic activities, the provision of those service depending on network and information systems, and an incident having significant disruptive effects on the provision of those services (article 5(2)). Article 6 provides criteria to determine the significance of a disruptive effect.

Each Member State must adopt "*a national strategy on the security of network and information systems defining the strategic objectives and appropriate policy and regulatory measures with a view to achieving and maintaining a high level of security of network and information systems*" (article 7). This includes the definition of objectives, a governance framework, measures for preparedness, response and recovery, and programs for education and training. Article 8 requires the identification of a national competent authority and a single point of contact. This authority will monitor national compliance and cross-border coordination. CSIRTs are responsible for risk and incident handling processes, covering all of the essential sectors listed in Annex II (article 9).

EU Member States, the European Commission and ENISA form a Cooperation Group (article 11). The goal is to foster strategic cooperation and information exchange between the Member States in order to raise the common level of NIS security. The Group can provide guidance to CSIRTs and develop best practices (article 12). Also, cooperation with non-EU countries can be set up (article 13).

Operators of essential services must implement appropriate technical and organizational measures to manage their security risks with a view on securing the continuity of those services (article 14). When confronted with an incident with significant impact on continuity, the competent authority or CSIRT must be notified. Where needed, cross-border coordination can be initiated. Communication to the public may be required as well. In implementing the required measures, the NIS Directive encourages standards (article 19).

The Member States had to implement the NIS Directive by 9 May 2018 (article 25). The European Commission developed a 'NIS Toolkit' to help Member States with the swift and efficient implementation of the directive.[87] Moreover, the EU Cybersecurity Act[88] establishes ENISA as the main body for certification in this field.

[87] European Commission (2017) "Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union", *COM/2017/0476 final.*

[88] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), *OJ* L 151 of 7 June 2019, 15-69.

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

9. Conclusions

In this deliverable, we have analysed six legal framework that are important to the implementation of the RESPONDRONE project results. In this section, we briefly summarize our main conclusions.

With regard to drones and their operation, the EU has recently adopted a new legislative package. A Basic Regulation sets the main rules regarding the design, production, maintenance, certification and operation of unmanned aircraft. An additional implementing and delegated regulation deepen these rules. Generally, this framework defines three categories of drone operations: open, specific and certified. Each of these is subject to particular rules, commensurate to the risks they pose. Manufacture and certification of drones is also subject to specific requirements for each category. Several EU Member States had already adopted their own national rules with regard to drones before the new EU legislative package. These rules will have to be brought in line with the new EU framework. While the EU framework in principle does not apply to drones carrying out military, customs, police, search and rescue, firefighting, border control and coastguard or similar activities and services undertaken in the public interest, the Member States do have the option to apply the framework to such operations. This matter will therefore require more follow-up throughout the project.

With regard to civil protection, it was found that this is mainly a national competence of the Member States. The EU itself is only involved at the level of cooperation between Member States, including mutual assistance. Civil defense procurement falls under the scope of the EU rules on military procurement. This framework – as implemented by the Member States – will therefore be applicable to the procurement of drone equipment as part of civil defense operations.

With regard to the use of drones for surveillance purposes, principles such as data protection and image rights should be taken into account. Data protection is mainly regulated by the GDPR, which applies to the processing of personal data obtained through the use of audio-visual equipment on drones. Section 5 of this deliverable has detailed the different responsibilities applicable to data controllers, as well as the rights of data subjects whose personal data is processed. Since first responders will operate the drones – or have a third party operate it for them – they will be considered as data controllers. Where a processor – the third party operating the drone – is used, a suitable controller-processor agreement must be in place. This means that the first responders will have to ensure compliance of their processing with the GDPR. With regard to image rights, it can be held that images that identify natural persons cannot be used – in the sense of being reproduced – without the consent of the persons involved.

With regard to the use of radio spectrum by first responders' drone operations, it must be assessed how they can gain radio spectrum usage rights. While there are some reserved frequencies they can use, these do not include the frequencies needed for commercial electronic communications networks, such as LTE and 5G-NR. Access to those networks can be achieved by

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

operating as a MVNO – as is already the case in Belgium. Alternatively, radio spectrum usage rights can be gained at the primary market or the secondary market. For obvious financial reasons, the secondary market seems more feasible, insofar as it can give first responders the necessary rights to operate their drones as mobile antennas.

With regard to the transport of medicinal goods and blood, there are a number of rules to be taken into account, mainly with regard to the temperature at which such goods must be transported and stored. While most of these rules mainly apply to distributors, they do provide an indication of what is considered as best practices in this field.

With regard to security aspects, attention must be given to the EU's NIS-Directive. This directive applies to essential services, which includes healthcare providers. Also aviation authorities are covered by this framework. As a result, it must be assessed to what extent Member States apply their national implementations of this framework to the use of drones by first responders.

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

10. Bibliography

10.1. International law

- Article 3 Chicago Convention on International Civil Aviation.
- Convention for the Protection of Human Rights and Fundamental Freedoms signed at Rome, 4 November 1950.

10.2. EU law

- Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft, *OJ* L 152 of 11 June 2019, 45-71.
- Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems, *OJ* L 152 of 11 June 2019, 1-40.
- Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), *OJ* L 151 of 7 June 2019, 15-69.
- 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, *OJ* L 212 of 22 August 2018, 1-122.
- 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), *OJ* L 119 of 4 May 2016, 1-88.
- Regulation (EC) No 216/2008 of the European Parliament and of the Council of 20 February 2008 on common rules in the field of civil aviation and establishing a European Aviation Safety Agency, and repealing Council Directive 91/670/EEC, Regulation (EC) No 1592/2002 and Directive 2004/36/EC, *OJ* L 79 of 19 March 2008, 1-49; Regulation (EC) No 552/2004 of the European Parliament and of the Council of 10 March 2004 on the interoperability of the European Air Traffic Management network (the interoperability Regulation), *OJ* L 96 of 31 February 2004, 26-42.
- Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, *OJ* L 321 of 17 December 2018, 36-214.
- Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, *OJ* L 194 of 19.7.2016, 1-30.

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

- Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC, *OJ* L 94 of 28 March 2014, 65-242.
- Directive 2009/81/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of procedures for the award of certain works contracts, supply contracts and service contracts by contracting authorities or entities in the fields of defence and security, and amending Directives 2004/17/EC and 2004/18/EC, *OJ* L 216 of 20 August 2009, 76-136.
- Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the safety of toys, *OJ* L 170 of 30 June 2009, 1-37.
- Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC, *OJ* L 157 of 9 June 2006, 24-86.
- Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, *OJ*. L 105 of 13 April 2006. 54-63.
- Commission Directive 2004/33/EC of 22 March 2004 implementing Directive 2002/98/EC of the European Parliament and of the Council as regards certain technical requirements for blood and blood components, *OJ* L 91 of 30 March 2004, 25-39.
- Directive 2002/98/EC of the European Parliament and of the Council of 27 January 2003 setting standards of quality and safety for the collection, testing, processing, storage and distribution of human blood and blood components and amending Directive 2001/83/EC, *OJ* L 33 of 8 February 2003, 30-40.
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *OJ* L 201 of 31 July 2002, 37-47.
- Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community code relating to medicinal products for human use, *OJ* L 311 of 28 November 2001, 67-128.
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data , *OJ* L 281 of 23 November 1995, 31-50.

10.3. Belgian law

- Act of 13 August 2011 concerning public procurement and certain contracts for works, deliveries and services in the fields of defence and security, *Belgian State Gazette* 1 February 2012.
- Act of 21 March 2007 regulating the placement and usage of security cameras, *Belgian State Gazette* 31 May 2007.

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

- Royal Decree of 10 April 2016 regarding the use of remote piloted aircraft in the Belgian airspace, *Belgian State Gazette* 15 April 2016.
- Royal Decree of 23 January 2012 concerning public procurement and certain contracts for works, deliveries and services in the fields of defence and security, *Belgian State Gazette* 1 February 2012.
- Ministerial Circular of 25 June 2019 on the use of drones by police and first responders, *Belgian State Gazette* 8 July 2019.
- Ministerial Circular of 7 December 2017 on the use of drones by police and first responders, *Belgian State Gazette* 28 March 2018.

10.4. French law

- Loi n° 2011-702 du 22 juin 2011 relative au contrôle des importations et des exportations de matériels de guerre et de matériels assimilés, à la simplification des transferts des produits liés à la défense dans l'Union européenne et aux marchés de défense et de sécurité, *JORF* n°0144 du 23 juin 2011 page 10673.Arrêté du 18 mai 2018 relatif aux exigences applicables aux télépilotes qui utilisent des aéronefs civils circulant sans personne à bord à des fins autres que le loisir, *JORF* n°0129 du 7 juin 2018 texte n° 32.
- Arrêté du 17 décembre 2015 relatif à la conception des aéronefs civils qui circulent sans personne à bord, aux conditions de leur emploi et aux capacités requises des personnes qui les utilisent, *JORF* n°0298 du 24 décembre 2015 page 23897.
- Arrêté du 17 décembre 2015 relatif à l'utilisation de l'espace aérien par les aéronefs qui circulent sans personne à bord, *JORF* n°0298 du 24 décembre 2015 page 23890.
- Ordonnance n° 2015-899 du 23 juillet 2015 relative aux marchés publics, *JORF* n°0169 du 24 juillet 2015 page 12602.
- Décret n° 2011-1104 du 14 septembre 2011 relatif à la passation et à l'exécution des marchés publics de défense ou de sécurité, *JORF* n°0214 du 15 septembre 2011 page 15450.

10.5. German law

- Verordnung zur Regelung des Betriebs von unbemannten Fluggeräten, *BGBl*. I 2017 S. 683.
- Gesetz zur Änderung des Vergaberechts für die Bereiche Verteidigung und Sicherheit, *BGBl.* I 2011 S. 2570.
- Vergabeverordnung für die Bereiche Verteidigung und Sicherheit (VSVgV), *BGBl*. I S. 1509.

10.6. Case law

- CJEU, Breyer *v.* Bundesrepublik Deutschland, C-582/14, para. 31-49.
- CJEU, Weltimmo *v*. Nemzeti Adatvédelmi és Információszabadság Hatóság, C-230/14, para. 29.
- CJEU, Google Spain *v*. Agencia Española de Protección de Datos, C-131/12, para. 28.
- ECHR, Von Hannover *v* Germany, 40660/08 and 60641/08, §95.

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/

10.7. Literature

- Article 29 Working Party (2014) "Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC", *WP 217.*
- Article 29 Working Party (2014) "Opinion 05/2014 on Anonymization Techniques", *WP 216*.
- Article 29 Working Party (2010) "Opinion 1/2010 on the concepts of controller and processor", *WP 169*.
- Article 29 Working Party (2007) "Opinion 4/2007 on the concept of personal data", *WP136*.
- European Commission (2017) "Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union", *COM/2017/0476 final.*
- European Data Protection Supervisor (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"", *edps.europa.eu*, 4.
- Finn, R., Wright, D., Jacques, L., De Hert, P. (2014) "Study on privacy, data protection and ethical risks in civil Remotely Piloted Aircraft Systems operations - Final Report", *ec.europa.eu,* 231 *et seq*.
- Guidelines of 7 March 2013 on Good Distribution Practice of Medicinal Products for Human Use (2013/C 68/01), *OJ* C 68 of 8 March 2013, 1-14.
- Guidelines of 19 March 2015 on principles of Good Distribution Practice of active substances for medicinal products for human use (2015/C 95/01), *OJ* C 95 of 21 March 2015, 1-9.
- Maxwell, W., Salmon, J. (2017) "A guide to blockchain and data protection", *Hogan Lovells,* 9.
- OECD, Recommendation of the Council of 23 September 1980 concerning guidelines governing the protection of privacy and transborder flows of personal data.
- Van Alsenoy, B. (2016) "Regulating Data Protection: The Allocation of Responsibility and Risk among Actors Involved in Personal Data Processing", *Doctoral thesis KU Leuven*, 53-62.

This project is funded by the European Union's H2020 Research and Innovation Programme and the Korean Government under Grant Agreement No. 833717
https://respondroneproject.com/