Data Protection: Drone User Handbook

Comhairle Cathrach Bhaile Átha Cliath
Dublin City Council

Our Public Service

SMART DUBLIN

Contents

Part 1: Background and Context

Part 2: Putting Things into Practice

Part 3: Best Practice Recommendations

Disclaimer

This handbook has been prepared for information purposes based on the contributions provided by Dublin City Council (DCC) and the various stakeholder groups involved in the use of drones and drone-mounted technology. It has considered research, legislation, legal precedent, and regulatory guidance in place as of the time of writing.

As data protection law and sensor technologies are both rapidly evolving areas, readers are advised to check with their legal advisors and their data protection officers before adopting or implementing any measures based on the information in this handbook.

Executive Summary

Drones and drone-mounted sensors have a multitude of potential uses for local authorities and municipalities. While early-adopters have piloted and tested the use of drones for specific scenarios, widespread adoption and implementation requires appropriate planning and development of relevant governance, oversight, and controls to ensure that data protection rights and other fundamental rights are respected, and data protection laws complied with in the gathering and processing of data using drone-mounted sensors and associated technologies.

This handbook provides an overview of the evolution of drone use scenarios and a snapshot of the current state of the art in respect of the balancing of the utility of drone-mounted sensors against the data protection and privacy impacts of these technologies, with reference to the fundamental concepts of Data Protection by Design and by Default.

Drawing on interviews with stakeholders, we set out a taxonomy of use case scenarios for drones and drone mounted sensors. It is recommended that this taxonomy is developed as a structure framework to support scalable and repeatable processes for assessing and mitigating data protection risks in the operation of drones and drone-mounted sensors. This taxonomy provides a basis for data protection impact assessments to be carried out on categories of scenarios rather than on specific instances of drone operations.

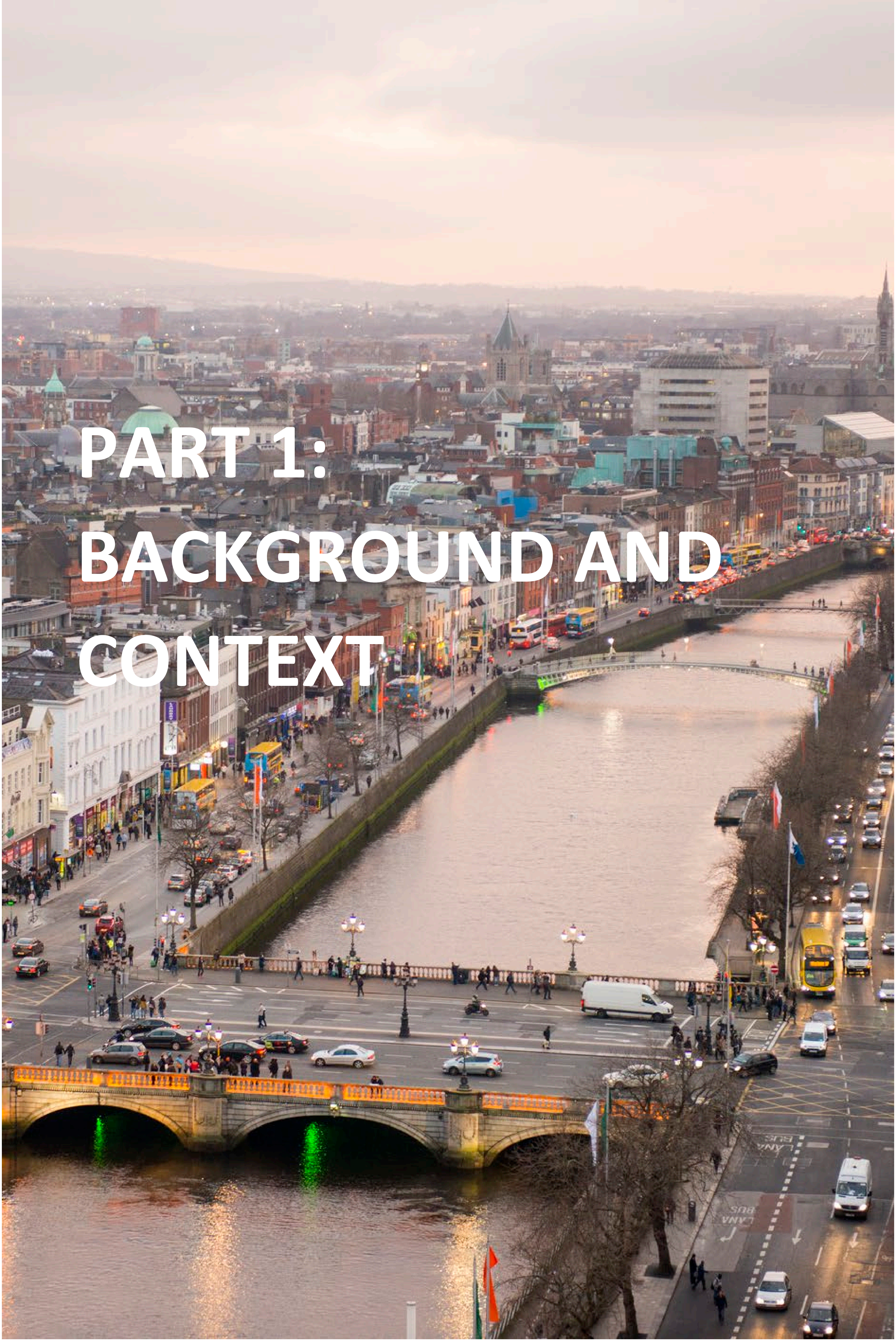
This handbook then sets out core data protection principles and map them to issues arising in the planning and execution of data gathering using drone-mounted sensors and associated technologies. As part of this the handbook sets out four key decision points for stakeholders who are planning the use of drones and drone-mounted sensors. It is important to note that these decision points do not replace any defined Data Protection Impact Assessment methodology that may be in use in a Local Authority but are intended to support and supplement these methodologies.

This handbook sets out ten recommendations for the use of drones and drone-mounted sensors in a way that is compliant from a data protection perspective and is responsible with respect to the impact of processing on fundamental rights of individuals. Among these recommendations is the development of a library of DPIAs, ensuring that Registers of Processing Activities are kept updated, and to improve transparency through the publication of information about planned drone operations.

The WERLA DPIA framework for the use of drones and drone-mounted sensors for Waste Management enforcement is considered as a reference example for the development of DPIAs and appropriate safeguards, mitigations, and controls. This DPIA and Use Case Scenario is mapped to the defined taxonomy of Use Cases to illustrate how the development of a taxonomy of Use Cases and an associated library of DPIAs and standardised safeguards, mitigations, and controls can support an effective framework for responsible and compliant drone operations.

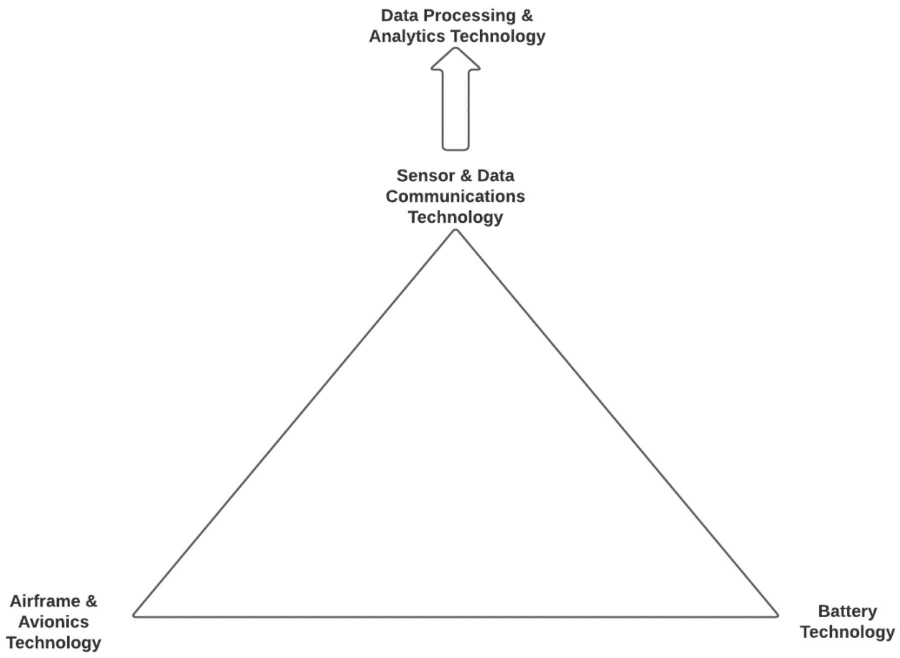
Appendix 1 to this handbook sets out a taxonomy of use cases which can be built on by stakeholders.

PART 1: BACKGROUND AND CONTEXT



The State of the Art in Drone use and Data Protection

Unmanned Aerial Vehicles, more commonly known as “drones” have been used in various forms for almost two centuries[1]. But the modern revolution in the use of drones, particularly by local government and municipalities has taken off in recent years due to technological advances in the manufacture of drone airframes, evolution in battery technologies and communications technology, and innovation in the development of both sensor technologies and software for data analytics.


Data Processing & Analytics Technology
Sensor & Data Communications Technology
Airframe & Avionics Technology
Battery Technology

These factors have resulted in an increase in the potential utility of unmanned vehicles to local authorities in line with a reduction in the relative cost of acquisition of the technology. And, with the continued development of improvements in sensor technology and data analytics capabilities, the potential scenarios for drone use in municipalities continue to evolve.

However, many local authorities have found themselves struggling to identify and mitigate the potential issues and risks associated with the use of drone-based technologies to help improve the efficiency and effectiveness of local government operations. And, as with the early adoption of drones for military applications, local authority deployment of drones has resulted in some clear wins as well as some self-inflicted wounds.

[1] As a point of historic reference, the first use of drones in a military context was by the Austrian Army in the 19th Century. It is worth noting that this was considered a failure as they had failed to account for risks in the use of the new technology arising from the weather conditions and the drones inflicted as much damage to their own forces as their enemies. This highlights the long-standing need for good risk management in drone operations.

Regulation of Drone Use

The first challenge in establishing a legal and ethical framework for drone use in the public sector is that of terminology.[2] Five overlapping terms may be relevant under the general category of drone usage:

- UAV (*Unmanned Aerial Vehicle*)
- UA (*Unmanned Aircraft*)
- UAS (*Unmanned Aerial System*)
- RPA (*Remotely Piloted Aircraft*)
- RPAS (*Remotely Piloted Aircraft System*)

In general usage the term "drone" may be said to apply to the categories of unmanned aerial vehicles (UAV) and Unmanned Aircraft (UA). Researcher Joaquín Sarrion Esteve explains that the term "*RPA refers to a drone, —UAV or UA—, which, in addition to be an aircraft or unmanned aerial vehicle, is also characterized by its ability to be piloted remotely… in other words, all RPAs are drones, but not all drones are RPAs*."[3] The terms UAS and RPAS refer to the entire system including the control system for piloting.

In general, all terms are covered by European Regulation under the broad category of "drones." In this handbook we adopt a similar general approach.

Regulation of Drone Flight

Prior to 2018, the regulation of small aircraft within the EU was the responsibility of member states. However, per Regulation 2018/1139, The European Aviation Safety Agency established in 2018 now holds regulatory responsibility for drone use.

The harmonized rules for drone usage may be found in Commission Delegated Regulation 2019/945, and Commission Implementing Regulation 2019/947. These regulations provide specific rules for manufacturers, pilots, and operators.

The Irish Aviation Authority (IAA) supervises and implements these Regulations in Ireland. Commission Implementing Regulation 2019/947 additionally outlines the need for drone usage to comply with privacy legislation including the General Data Protection Regulation[4] and the Data Protection Act 2018.

[2] Sarrión Esteve, Joaquín, *Actual Challenges for Fundamental Rights Protection in the Use of Drone Technology* (August 27, 2018). Available at SSRN: https://ssrn.com/abstract=3239562

[3] Ibid. 3

[4] Regulation (EU) 2016/679, 27 April 2016, General Data Protection Regulation, OJ L 119.

Data Protection and Drones

It is important to note data protection legislation applies not to the aerial vehicle platform (the drone) but to the processing of personal data by any sensor technologies, for example a camera or a microphone, which may be mounted on a drone and any processing of data captured by that sensor for analytics or other processes. **Given the breadth of the definition of "processing" in data protection law, this includes both the viewing of the drone's cameras in real time, as well as any recordings of the data (e.g. video files) which are made**.

In short, a drone that does not have sensors for data capture mounted to it is unlikely to give rise to data protection risks. However, a drone which has data capture sensors mounted to it may give rise to data protection risks and these risks must be assessed. In certain circumstances it will be sufficient to implement mitigations, however in other instances the risks will simply outweigh the benefits and thus the intended use will not be lawful.

The use to which a drone is employed will necessitate that it be equipped with different types of sensor technologies. The overall processing purpose for which the drone is being deployed may also require the use of different types of analytics technologies or integration with other which in turn will have differing impacts on privacy and data protection.

Common types of sensor equipment include:

- Optical sensors capable of capturing photographic images and recording video surveillance.
- Thermal sensors measuring heat
- Humidity sensors
- Wind strength and direction sensors
- Audio sensors and microphones capable of recording audio, including directional microphones.
- LiDAR[5] or similar sensor technologies

Other types of sensors that can be mounted on a drone platform include proximity sensors (to measure distance from objects or other drones), GPS (to identify the location of the drone at a point in time or to manage navigation or set boundaries on the flightpath of the drone), or optical gas imagery (to detect the presence of hazardous gases), and gas sensors to measure air quality. In addition, technologies such as Automatic Number Plate Recognition (ANPR), biometric facial recognition, or similar machine learning analytics or data processing tools can further enhance the capability of drone mounted sensors to support additional use cases.

However, the **combination** of different sensor types with information processing technologies in different **contexts** or locations can give rise to a range of potential privacy and data protection challenges that need to be balanced against the benefits that might arise from the use of a drone-mounted sensor technology to perform a task.

[5] Laser Imaging, Detection, and Ranging. A technology which involves the targeting of distances from above with lasers and measuring the time taken for the reflected light to return to the receiver. These readings can be used to create three-dimensional representations of an area

Understanding Privacy and Data Protection

The right to Privacy and the right to Data Protection are two distinct rights enshrined in EU law in Article 7 and Article 8 of the Charter of Fundamental Rights. Both are relevant to the use and operation of drones, drone mounted sensors, and associated technologies.

> **Article 7 Charter of Fundamental Rights – The Right to Privacy**
>
> Everyone has the right to respect for his or her private and family life, home, and communications.

This means that the use of optical sensors (e.g., cameras), audio sensors (e.g., directional microphones) in areas that overlook homes or areas where people might enjoy a presumption of privacy needs to be carefully planned and executed to mitigate the risks to this right.

> **Article 8 Charter of Fundamental Rights – The Right to Data Protection**
>
> 1. Everyone has the right to the protection of personal data concerning him or her.
>
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
>
> 3. Compliance with these rules shall be subject to control by an independent authority.

This means that when personal data of any living individual is obtained and processed by an organisation, it must be done for specific purposes with a clear legal basis. This right is given effect through legislation such as the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

> **What is Personal Data?**
>
> The GDPR defines personal data as:
>
> *"Any information relating to an identified or identifiable natural person"*

This definition is quite broad, and the key test is whether an individual can be identified of is identifiable from the data and any other data that the Data Controller would legally have access to (e.g., a car license plate number becomes personal data of an identifiable natural person if the Data Controller can link that license plate to the name of an individual through some lawful means).

What is Processing?

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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

Processing therefore includes the capture and recording of personal data but also the consultation or use of the data, and the onward transmission or publication of data. Particular attention should be paid to the risk that arises when sensor data from drones is combined with other data which could give rise to personal data being processed.

In the case of cameras and recording technology connected to drones processing would include **both the viewing of the drone's cameras in real time, as well as any recordings of the data (e.g. video files) which are made.**

The UK's Information Commissioner's Office provides the following guidance in relation to the use of drones:

> The use of UAS have a high potential for collateral intrusion by recording images of individuals unnecessarily and therefore can be highly privacy intrusive, ie the likelihood of recording individuals inadvertently is high, because of the height they can operate at and the unique vantage point they afford. Individuals may not always be directly identifiable from the footage captured by UAS, but can still be identified through the context they are captured in or by using the devices ability to zoom in on a specific person. As such, it is very important that you can provide a strong justification for their use.

The Irish Data Protection Commission does not have specific guidance on the use of drones at this time, but they echo the guidance of the ICO:

> "…users should consider the location in which they use these devices and the possibility of identifying any individuals recorded…"

The Data Protection Implications of Drone Use

In the context of Drone usage personal data may processed when:

- Clear footage of a person's face is recorded.
- An individual can be identified in another manner such as through the GPS location, visible address, car registration, and personal items including clothing.
- Information about an individual's private life, behaviour, bodily characteristics are revealed through the footage or images.

- Recordings are made of an individual's voice or conversation
- A person's heat signature can be identified revealing behaviour.
- Intimate imagery exposing home life is recorded.

It is also important to consider the risk of a drone-mounted sensor capturing data which could be categorised as "Special Category Data" under GDPR and which carries with it a higher standard of protection from interference. Drone use monitoring home life as well as religious, political or trade union buildings may reveal personal information about these types of special category data in a manner that can be associated to an identifiable person.

Special Category Data is data which

- Can reveal
    - Racial or Ethnic Origin
    - Political Opinions
    - Religious or philosophical beliefs
    - Trade Union Membership
- Is
    - Genetic Data
    - Biometric data
- Is concerning
    - An individual's health
    - An individual's sexual history or sexual orientation

The European Union's DroneRules.EU[6] project outlined the risks to privacy associated with different technologies used with drones. We have expanded on their classification slightly for this handbook to align with the classification of different sensor types and to clearly differentiate between the sensors used and the processing of sensor data either on-device or off-device after data transfer.

[6] DroneRules.eu is an awareness campaign tool that aims to inform and educate the drone user community and the general public how to fly legally in the different EU member states, and Norway and Switzerland. The project is co-financed by the European Commission under the COSME Programme. See https://dronerules.eu/en/faq

Category of Sensor /Processing	Payload / Capability	Potential Privacy Impacts	Consideration for Mitigation
Optical Sensor (Camera)	High-Definition Camera	• Privacy of image and data • Privacy of behaviour and action • Privacy of association • Privacy of beliefs (political/religious/philosophical) • Privacy of home	• Is the resolution necessary for the purpose? • Can camera be kept off until needed? • Retention period for recordings and control of access
	Camera with zoom capability	• Privacy of image and data • Privacy of behaviour and action • Privacy of association • Privacy of beliefs (political/religious/philosophical) • Privacy of home	• Is the resolution necessary for the purpose? • Can camera be kept off until needed? • Retention period for recordings and control of access
	Multi-spectrum NDVI	• Potential impacts if normal optical camera capability is employed as well • Combination with other data could result in data protection/privacy risk	• Can normal optical camera be kept turned off? • What controls/safeguards are in place re combining data?
	Thermal Sensor	• Privacy of image and data • Privacy of behaviour and action • Privacy of association • Privacy of beliefs (political/religious/philosophical) • Privacy of home	• Consider purpose for processing and potential safeguards • Is sensor targeting people or environment? • Retention period for recorded data / access controls

Category of Sensor /Processing	Payload / Capability	Potential Privacy Impacts	Consideration for Mitigation
Audio Sensors	Directional Microphone	• Privacy of voice/spoken word and data • Privacy of behaviour and action • Privacy of association • Privacy of beliefs (political/religious/philosophical) • Privacy of Communications	• Can purpose be met through live 'sampling' of audio and on-device measurement? (e.g., decibel measurement vs recorded sound) • Retention period for recordings and control of access
Environmental Sensor	Gas Sensor	• Privacy of home	• What gases are being tested for/measured? • Is this a point in time sample or will data be retained?
	Humidity Sensor	• Privacy of home	• What gases are being tested for/measured? • Is a drone the best / least invasive way of carrying out the measurement? • Is this a point in time sample or will data be retained?
	Air Quality Sensor	• Privacy of home	• As above - what is being detected/Is drone-based sensors the least invasive way of carrying out measurement?
	GPS/Geolocation Sensors	• Privacy of location and space	• Is it necessary to combine GPS with other data that might enable people to be identified or data relating to them to be inferred?
	LiDAR	• Privacy of home	• Consider flight path and necessity of mapping areas that may include private residences.

Category of Sensor /Processing	Payload / Capability	Potential Privacy Impacts	Consideration for Mitigation
AI matching and recognition	Facial Recognition	• Privacy of image and data • Privacy of behaviour and action • Privacy of association • Privacy of beliefs (political/religious/philosophical) • Privacy of home	• Is facial recognition necessary? • Formal definition of safeguards required • DPIA required (processes biometric data for the purpose of identifying an individual)
	ANPR	• Privacy of image and data • Privacy of behaviour and action • Privacy of association • Privacy of beliefs (political/religious/philosophical) • Privacy of home	• Is this processing necessary? • What is the legal basis for accessing data to identify the owner of the vehicle? • What is the retention period for the data and who can access it?
	Audio/Speech recognition	• Privacy of voice/spoken word and data • Privacy of behaviour and action • Privacy of association • Privacy of beliefs (political/religious/philosophical) • Privacy of Communications	• Is this processing necessary? • What is the legal basis for accessing data to identify the speaker? • What is the retention period for the data and who can access it?
Platform Capability	First Person View	• Risk of dehumanising data subjects arising from them being "othered" as collateral data capture not related to the primary focus of the processing.	• Need to ensure that the "human factors" of planning drone operations actively consider risks to data subjects
	Battery Endurance / Range	• "Out of sight, out of mind" risk. Drone platform could fly at altitude or in a flight range that risks more secondary capture of personal data than anticipated	• Need to ensure planning of drone operations actively considers risk of secondary data capture and appropriate mitigations

Category of Sensor /Processing	Payload / Capability	Potential Privacy Impacts	Consideration for Mitigation
	Autonomous Operation	• Drone flying a planned or machine-planned route may not consider implications of overflight of buildings, open spaces, or communal areas	• Need to ensure that appropriate safeguards are applied in the planning and execution of any autonomous flight
	Wireless data transfer (e.g. wifi/radio/Bluetooth data transfer vs on-device storage)	• Risk of data being intercepted by a 3rd party unless data exchange is encrypted/secured	• Ensure appropriate security of data transfers
	On-device storage	• Risk of data being accessed without authorisation if a 3rd party removes the on-device storage when landed/crashed	• Ensure encryption of removable media • Define protocol for securing the removable media once drone has landed / been recovered

Assessing the Use Cases for Drone Use

A recurring theme in research is a lack of a taxonomy for drone use cases and associated personal data. It is instead far more common to find individual use cases from industry used within academic study. Common use cases include:

- Emergency Use – Drones can play a pivotal role in rescue missions and other urgent humanitarian response plans. These include search and rescue, natural disaster management, humanitarian aid delivery, and ambulance services.

- Infrastructure monitoring and inspection - Drones fitted with high-resolution video recording capacity may provide simple access options for the inspection of infrastructure which would otherwise be difficult to reach safely. Such usage is common for power lines, rail tracks, wind turbines, waste management facilities.

- Mapping areas- Drones may be used for mapping for numerous projects including geographic surveys for future roads or housing development, construction planning and mining.

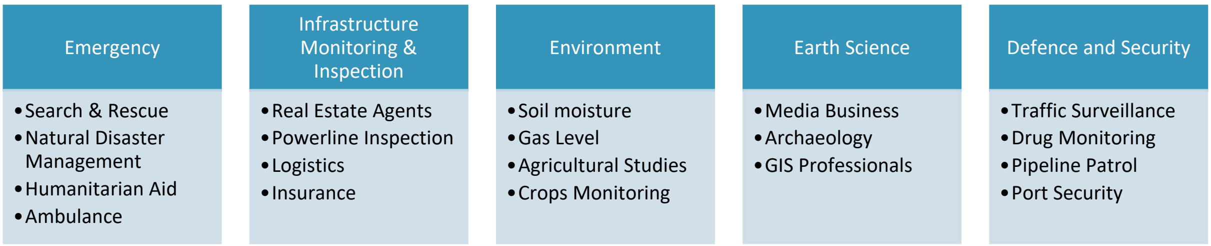
- Earth Science - the resources required for surveying and GIS mapping are greatly reduced through drone usage.

- Filming historical/cultural sights for promotion or sale

- Filming events for publicity and future promotion

- Prevention, detection, and investigation of crime

These archetypes of drone usage are reinforced through the research of Mitka and Mouroutsos[7] who represent the categories which they have identified in the figure below.



Emergency	Infrastructure Monitoring & Inspection	Environment	Earth Science	Defence and Security
• Search & Rescue • Natural Disaster Management • Humanitarian Aid • Ambulance	• Real Estate Agents • Powerline Inspection • Logistics • Insurance	• Soil moisture • Gas Level • Agricultural Studies • Crops Monitoring	• Media Business • Archaeology • GIS Professionals	• Traffic Surveillance • Drug Monitoring • Pipeline Patrol • Port Security

Figure 2: Taxonomy of Drone Use Cases. Based on Mitka & Mouroutsos (2017)

A more in-depth taxonomy of use cases for local authorities to help inform and structure data protection risk assessment of different drone use scenarios has been developed as part of the research to develop this report and is discussed later in the handbook.

[7] E Mitka and SG Mouroutsos, ‘Classification of Drones’ (2017) 6 American Journal of Engineering Research.

Recurring Privacy and Data Protection Issues

The following recurring Privacy and Data Protection issues may be noted through an analysis of the use cases examined in current industry and academic research.[8]

Issue	Description
Lawfulness, fairness, transparency	A lawful basis must be found for the proposed processing activities. This must be identified and laid out clearly. In the case of incidental data processing a lawful basis is often not even considered. Additionally, data processing is unlikely to be fair and transparent when individuals on the ground may be unaware a drone is in operation. They should be aware by whom, when and how the drone is being used and for what purpose. This allows them to adjust their privacy expectations, be prepared and keep control over their privacy by acting accordingly.
Chilling effect	Individuals may perform a form of self-preservation/ self-censorship by restricting their behaviour when they are, or believe that they are, being watched. Making individuals in the area aware of the purpose of filming and what is being captured can reduce this negative effect.
Data Minimisation	Capture only the data that is necessary for the purposes which it is employed is difficult in the case of drone use where the desire to capture as much information as possible is common.

[8] See Anne Gerdes, and Privacy Issues, Information, Technology and Innovation Research Group at University of Southern Denmark, Drones, 2017, presentation slides. http://infotechinno.sdu.dk/pdfs/Drones%20and%20privacy%20SDU_042418.pdf

Altawy Riham and Amr. M. Youssef, "Security, Privacy, and Safety Aspects of Civilian Drones: A Survey", *ACM Transactions on Cyber-Physical Systems,* Vol. 1, Issue 2, Article 7, November 2016, 25 pages. https://users.encs.concordia.ca/~youssef/Publications/Papers/Drone-Survey.pdf.

Chang, Victoria, Pramod Chundury, Marshini Chetty, ""Spiders in the Sky": User Perceptions of Drones, Privacy, and Security", *CHI '17* Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, May 06-11, 2017, Denver, CO., USA, pp. 6765 – 6776. https://hci.princeton.edu/wp-content/uploads/sites/459/2017/01/CHI2017_CameraReady.pdf

Cavoukian, Ann, "Privacy and Drones: Unmanned Aerial Vehicles", Information and Privacy Commissioner, Ontario, Canada, August 2012, p. 4. https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-drones.pdf.

Issue	Description
Storage Limitation	Data taken from drones is not often labelled as personal data when appropriate and thus is not kept in line with the storage limitation principle of GDPR.
Integrity and Storage of Data	Ensuring the safety of personal data is vital in the case of drone usage. However, it is commonly overlooked as a potential data protection or information security risk during drone operations.
Privacy of thoughts and feelings	Individuals have a right not to share their thoughts or feelings or to have them revealed. This includes their beliefs or religious views.

Data Protection by Design and Default in Drone Operations

Article 25 of GDPR sets out the requirement for Data Protection by Design and by Default. This translates to privacy and data protection as ex ante considerations which must be incorporated into the creation and implementation of technologies and policies.

The notion of privacy by design and default was first conceptualised by Ann Cavoukian, the former Information and Privacy Commissioner of Ontario. The framework sets out seven core principles.[9]

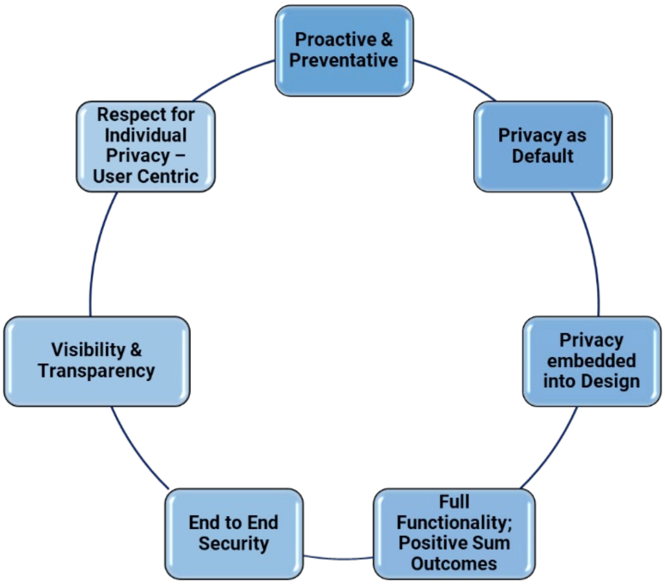

Proactive & Preventative
Privacy as Default
Privacy embedded into Design
Full Functionality; Positive Sum Outcomes
End to End Security
Visibility & Transparency
Respect for Individual Privacy – User Centric

Figure 3 Privacy by Design Principles

[9] Cavoukian, Ann, “Privacy by Design: The 7 Foundational Principles”, Information and Privacy Commissioner, Ontario, Canada, January 2011. https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf.

These are listed and applied to drone use cases below.

Principle	Application to Drone Operations
Proactive not Reactive; Preventative not Remedial	"The Privacy by Design approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred − it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after" .[10] – *Dr Ann Cavoukian* The following examples have been highlighted as ways of applying principle 1 in the case of drone use. • The use of geo-fencing and other limitation sensing technology to restrict the zone of operations. • The use of software controls facilitating a more tailored data capture approach such as keeping sensors off until needed. • Triggers for users to prevent and enable data capture during flight as personal data is encountered (e.g., turning sensors on and off in real time in response to conditions) • Application of data minimisation principles in the planning and selection of drones and sensor packages. • Ensuring encryption of data transfers, data storage, and appropriate user access controls in drone software and in the storage and processing of captured data.
Privacy as the default setting	Ensuring defaults which are privacy protecting lowers the barrier of knowledge and burden on users for protecting data protection rights. This ensures that data protection and privacy rights are more likely to be protected in practice. The following are examples of settings which drones should hold without the need for user intervention: • Geofencing compliance • Requiring access controls for drone use and data access. • Data capture settings allowing for data recording to only be triggered as a variety of user inputted conditions are met (eg. Location, timing) • Automatic data storage limitation settings.

[10] Ibid.

Principle	Application to Drone Operations
Privacy Embedded into Design	"Privacy must be embedded into technologies, operations, and information architectures in a holistic, integrative and creative way. Holistic, because additional, broader contexts must always be considered. Integrative, because all stakeholders and interests should be consulted. Creative, because embedding privacy sometimes means re-inventing existing choices because the alternatives are unacceptable".[11] – *Dr Ann Cavoukian* In the context of drone use privacy considerations must be embedded into the design and architecture of both systems and products. This includes not only the manufactured technology itself, but the policy environment in which it is applied. Therefore, responsible operation of drones requires consideration at a policy and procedure level of: • The objectives of the drone deployment and the process for formally evaluating the appropriateness of drone use and the choice of sensors that are deployed in context • The retention of recorded data and the governance and controls that are applied to any secondary uses of that data for other purposes or the combination of drone-recorded data with other data • The implementation of appropriate controls and safeguards to ensure that appropriate balances of data protection/privacy and usefulness of data processing is achieved.
Full Functionality; Positive Sum Outcomes	Privacy by design should not undermine the quality and functionality of a product. Instead, it should be incorporated in manner that allows the product to perform properly.[12] In other words, the focus in planning and assessing data protection risks in respect of drone operations should be on ensuring that there is clarity on the objective and that the appropriate tools and safeguards are implemented to deliver the best outcome in the best manner.

[11] Cavoukian, Ann, "Privacy by Design: The 7 Foundational Principles", Information and Privacy Commissioner, Ontario, Canada, January 2011. https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf.

[12] DronePro.Eu, 'Privacy by Design Guide' <https://dronerules.eu/assets/files/DRPRO_Privacy_by_Design_Guide_EN.pdf>.

Principle	Application to Drone Operations
End-to-end security	Privacy should be appropriately protected through security measures incorporated into the entire data lifecycle associated with drone usage. This applies not just to the period when the drone is recording or capturing data but for the storage and later processing of any recorded data.
Visibility and Transparency	"Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to both users and providers alike.[13]" – *Dr Ann Cavoukian* As drones often operate from heights which cannot be easily detected by individuals on the ground and can otherwise be unobtrusive or difficult to spot, it is vital to address the inherent transparency issue. Some ways of addressing this imbalance include: • Making drones more noticeable by design and including design elements which signal when its sensors are active and processing data. • Making information about the drone in use and its purposes available to the public impacted by its recording. • Placing cameras and sensors in clear to view places.[14] • Engaging in stakeholder education about the nature and type of drone operations

[13] Cavoukian, Ann, "Privacy by Design: The 7 Foundational Principles", Information and Privacy Commissioner, Ontario, Canada, January 2011. https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf.

[14] DronePro.Eu (n 10).

Principle	Application to Drone Operations
Respect for User Privacy	Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. The best Privacy by Design results are usually those that are consciously designed around the interests and needs of individual users, who have the greatest vested interest in the management of their own personal data. In the context of drone use and production this necessitates placing two categories of people at the forefront (a) potential users of the product and (b) potential data subjects. As such privacy preserving features must be incorporated to protected data subjects, but also made in such a way as to be easily implemented by the users,

Drones and Covert Surveillance

One of the more commonly identified use cases for drones is as a platform for covert as opposed to overt surveillance of an area. However, as can be seen from the emphasis on transparency in the Data Protection by Design and Default obligation and the core Transparency Principle in GDPR, this is an area which is subject to tighter restrictions given the significant impact on the right to privacy and the right to data protection.

Covert surveillance for law enforcement or national security purposes in Ireland by the Gardaí, the Revenue Commissioners, or the Defence Forces falls under the Criminal Justice (Surveillance) Act 2009 and Part 5 of the Data Protection Act 2018. For all other bodies, covert surveillance requires a specific and explicit legal basis that includes appropriate safeguards and also provides an appropriate derogation from the obligations of the GDPR in line with Section 23 of the Data Protection Act 2018.

Analysis of Use Cases and Usage Scenarios

The effective and efficient integration of Data Protection by Design/by Default into the planning and execution of drone operations by Local Authorities and other Public Sector entities requires a strategic and structured approach to be taken so that appropriate policies, procedures, templates, and checklists can be developed that are relevant, appropriate, and proportionate to the balancing of rights, risks, and requirements that arise in that specific scenario.

The categorisation of use cases for the deployment of drones by academic researchers and industry has historically focussed on specific examples. Likewise, enforcement actions and investigations by regulators have tended to focus on specific instances of use. Effective planning and execution of Data Protection by Design and by Default for the operation of drones and drone mounted sensors in a way which supports the many and varied needs of local authority stakeholders requires a framework in which new scenarios for use and new technology capabilities can be assessed.

Such a framework would need to support an objective and structured approach to assessing the necessity, proportionality, and appropriateness drones and drone-mounted sensors for particular purposes and to help inform decision making about the appropriate safeguards that should be put in place for any proposed use of drones and associated sensor and analytics technologies.

When considering the various scenarios for use, it is recommended to consider your drone use scenario using the following life-cycle of data analytics:

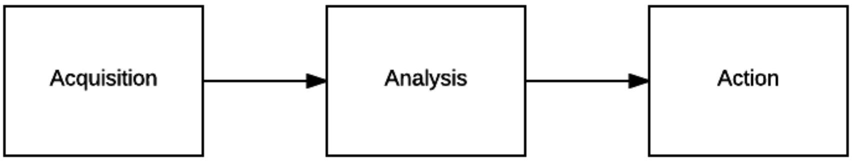


Figure 4 A Data Analytics Life Cycle Source: Ethical Data & Information Management, O'Keefe & O Brien, 2018

Life Cycle Stage	Things to Consider
Acquisition	• What types of data are you going to gather? • What types of sensors are you using? • Where will you be operating? • How will you minimise the data related to people you will capture to the minimum necessary or avoid capturing data relating to people at all?
Analysis	• How will data be analysed? Will you be using AI tools like facial recognition or event detection? • Who else might want to use this data for other use cases?
Action	• What is the thing that will be done based on the data gathered from the drone mounted sensors? Will that action affect/impact individuals? • How/when will you get rid of personal data you no longer need?

Developing a Taxonomy of Use Cases

As part of preparing this handbook, analysis was conducted of the current, planned, and anticipated uses for drones and drone mounted sensor technologies by various stakeholder groups. The objective was to identify a categorisation and classification of scenarios which could support the development of a strategic and structured approach to the appropriate assessment of data protection and privacy risks and mitigations associated with drone operations. This analysis identified approximately 50 distinct use cases which are clustered into four main categories.

The benefit of adopting a taxonomy approach to defining the use cases identified for drone use is that the categories of issue, risk, mitigation, and 'things to check' can be defined for a class of use cases (e.g., Built Environment Monitoring) but specific issues that might arise due to the particular contexts of use (e.g., choice of sensors, use of analytics technologies or machine learning, context of location or events requiring the use of the drone) can be addressed as a sub-class of that category if a different action, risk treatment, or controls and governance requirement arises.

This approach also allows for the identification of common issues, risks, and approaches to risk treatment that might arise across different areas of local authorities who might be using drones in a similar way but for different end purposes.

> A key question to ask when applying a taxonomy approach to identifying and assessing potential issues and risks is this:
>
> *"What am I planning to do, and how is it the same or different to any of the things that have already been identified here, and how are the issues and risks different?"*
>
> If your proposed use or the potential risks are different, it is another 'branch' on the taxonomy. When asking yourself the questions about what you plan to do and why it is similar or different to existing applications of drones, drone mounted sensors, and associated technologies, it's often helpful to work backwards through the life cycle of analytics:
>
> **Action:** *What are you going to do as a result of gathering this data? What is the PURPOSE for which you are deploying the drone and its sensors?*
>
> **Analysis:** *What do you need to know or measure to take the action? Is that data directly available from the drone's sensors or are you going to have to combine it with other data or process it using analytics technologies to get the information you want to act on? What is the PROCESSING ACTIVITY you will be doing to enable you to take the Action?*
>
> **Acquisition:** *How are you getting the data? Will you (or contractors working for you) be flying the drone and configuring the sensors or will you be using data / footage recorded by someone else? Where will you be acquiring the data? What types of sensors do you need to have deployed to capture the information you need to analyse? How might your sensor choice impact on the privacy rights or data protection rights of individuals in the area of operation of the drone? If you didn't capture the data directly, do you know how those issues were addressed by the original recorder of the data?*

Taxonomy Level 1 Definitions

Use Case Taxonomy Level 1	Definition
Monitoring and Measurement	Drone mounted sensors and associated technologies are used to monitor a location to gather actionable information about a thing/event or to support statistical measurement of an aspect of the environment, infrastructure, or services that are provided by the local authority.
Incident Response and Planning	Drone mounted sensors and associated technologies are used to support the planning for or response to incidents which may pose a risk to people, property, or the environment
Investigation and Enforcement	Drone mounted sensors and associated technologies are used to record and document information related to the detection, investigation, and prosecution of criminal offences or breaches of legislation
Media, Publicity, and Entertainment	Drone mounted sensors and associated technologies are used to capture audio-visual recordings of locations, incidents, or events. Drones may also be used to provide operational or logistical support to the production or execution of public events or entertainment.

It is important to note that personal data captured or recorded for one category of use case might be used for another purpose that falls under another category of use case. Also, effective and efficient use of drone assets might result in a single drone flight operation addressing requirements across one or more category of use case.

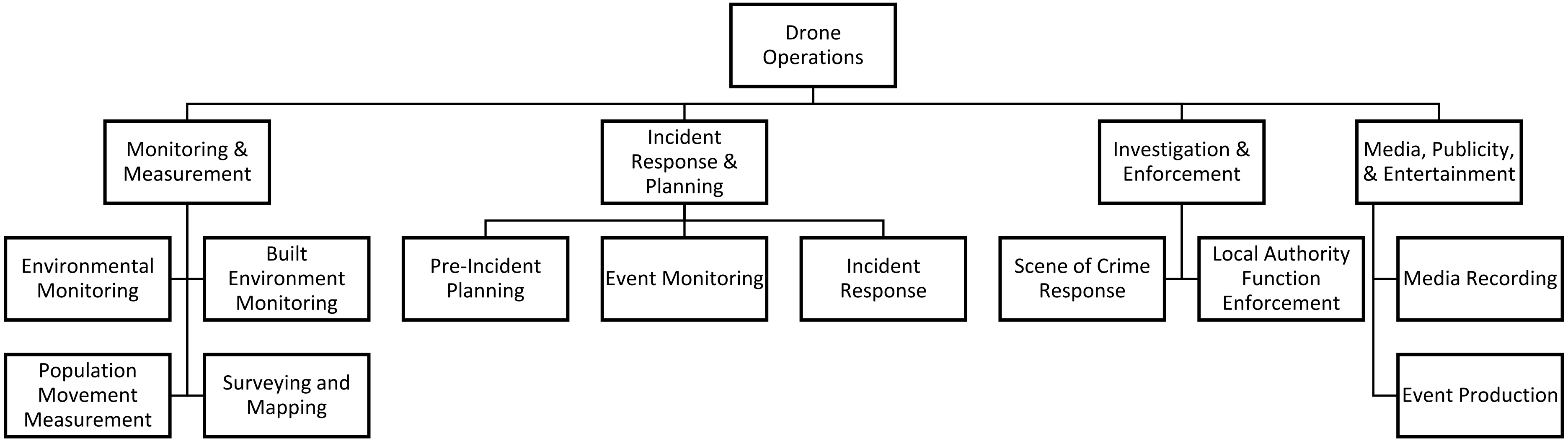
Prior planning will ensure that the appropriate sensor technologies are deployed in the correct way to ensure that appropriate safeguards are in place to protect data protection and privacy rights, particularly as any secondary use must be compatible with the purpose for which data was originally obtained (the *Purpose Specification/Limitation Principle* in Data Protection law).

Example

A drone flight is planned to capture video footage of a community litter awareness event. There is also a report of an outbreak of an invasive plant species in the area where the drone will be operating, and a survey is required to assess the extent of the problem.

The footage recorded will therefore support objectives across two categories of use case. However, the processing of footage of people would not be necessary for the environmental monitoring use case. Therefore, the drone operation will need to be planned to record the footage of the community event and then carry out a separate survey pass with people excluded from the area where the drone is operating.

A Taxonomy of Use Cases – Level 1 and Level 2



Taxonomy Level 2 Definitions

The table below describes the types of activity and processing purpose which are categorised at Level 2 on this taxonomy.

Taxonomy Level 1	**Taxonomy Level 2**	**Definition**
Monitoring and Measurement	Environmental Monitoring	Use of drone mounted sensors and associated technologies to survey, monitor, or measure features of the natural environment to detect positive and negative changes in the environment and inform policy responses and remedial action.
	Built Environment Monitoring	Use of drone mounted sensors and associated technologies to survey, monitor, or measure features of the built environment to detect positive and negative changes in the built environment, including impact on the natural environment and inform policy responses and remedial action.
	Population Movement Measurement	Use of drone mounted sensors and associated technologies to survey, and measure population movements within the area to support the development of and validation of statistical models to inform policy responses and remedial action.
	Surveying and Mapping	Use of drone mounted sensors and associated technologies to survey and map features of the natural or built environment for the purposes of producing geospatial and navigation data sets
Incident Response and Planning	Pre-Incident Planning	Use of drone mounted sensors and associated technologies to survey locations to identify issues and risks to be mitigated through the development of an incident response plan.
	Event Monitoring	Use of drone mounted sensors and associated technologies to actively monitor an event to support event management and inform response to incidents at the event.
	Incident Response	Use of drone mounted sensors and associated technologies to support the response to an emergency incident event by the relevant agencies and to inform decision-making during the incident handling. Different categories of incident may require different technology responses.

Taxonomy Level 1	Taxonomy Level 2	Definition
Investigation and Enforcement	Scene of Crime Response	Use of drone mounted sensors and associated technologies to assist the gathering of evidence and recording of information related to the scene of an accident or criminal incident to support the investigation of any offence and the prosecution of any offender.
	Local Authority Statutory Function Enforcement	Use of drone mounted sensors and associated technologies to assist the gathering of evidence and recording of information related to the scene of a breach of regulations in an area which the local authority has a statutory investigative or enforcement role to support the investigation of any offence and the prosecution of any offender.
Media, Publicity, and Entertainment	Media Recording	Use of drone mounted sensors and associated technologies to record video, audio, still imagery, or other data for publication or dissemination by the local authority or another party.
	Event Production	Use of drones without any additional sensor technologies other than those required for the safe flight operations of the drone for the purposes of supporting the production of an entertainment event (e.g. drone-enabled light displays, event lighting, or equipment transport).

In Appendix 1 to this manual we examine more granular examples of usage and the potential data protection issues, considerations, and mitigations that would need to be considered when planning or undertaking the use of drones or drone-mounted sensors. It is also important to consider not just the data protection implications of the drone operation but also the potential implications for data protection obligations that will arise from any further processing of the data such as:

- Sharing with other parties (what is your legal basis for doing so? How will that sharing be done securely?)
- Matching data with other data or combining data with other data (what is the legal basis for doing so? Is this likely to make individuals more identifiable from the data?)
- Storing data (Why are you storing the data? What is the legal basis for storing the data? What is the trigger for deleting the data?)

Conclusions and Guidance on Use Cases and Scenarios

Based on the research and analysis of the potential scenarios for the use and operation of drones by Local Authorities, several categories of scenario have been identified. The analysis has also identified a number of common modes of use which share a number of common data protection compliance risks that need to be considered in the context of the **Acquisition => Analysis => Action** life cycle.

Life Cycle Stage	Issues to Consider
Acquisition	• Will the drone be recording optical or other kinds of sensor data? • What type of data are you looking to record? Will it be directly or indirectly linked to an individual? • Where will the drone be operating? ○ Will it over-fly private homes? ○ Will it over-fly areas accessible to the public? • Will the drone be operated by the Local Authority or a contractor? ○ If the latter, is there an appropriate data processor agreement in place? • Will you be able to inform people in advance about the use of drones in the area or otherwise make people aware of the use of drones with sensors (optical/audio/etc.)?
Analysis	• How will the data obtained by the drone be analysed? • How will the data be transferred from the drone for analysis • Will you be using any machine learning technologies to process the recorded data or will you be linking it to other external data? ○ If yes, would this allow for individuals to be identified directly or indirectly (e.g. use of ANPR software or facial recognition software) • What safeguards will be implemented to restrict access to recordings or to redact/remove personal data that has been captured which is not necessary for the purposes of your processing?
Action	• What is it that you want to do the information obtained by the drone? • What is the legal basis for the thing you want to do? ○ Does that allow for the use of camera or other data? ○ Does that allow for the linking of recorded data with other information from other sources which might identify an individual? ○ Is your purpose within the scope of Part 5 of the Data Protection Act 2018 and, if so, what is the criminal offence you are planning on detecting or investigating? • Can you obtain the information/data in another way? ○ Is it necessary to obtain the data? ○ Is the use of drone mounted sensors a proportionate approach?

By developing categories of related processing activities, it is easier to identify commonly occurring risks and mitigations as well as identifying commonly applicable legal bases for processing personal data under data protection law.

PART 2: PUTTING THINGS INTO PRACTICE

A Data Protection Decision Flow for Drones and Drone Mounted Sensors

It is important to ensure that appropriate safeguards are implemented in respect of the gathering and processing of personal data or special category personal data through the use of drone-mounted sensors. Failure to ensure appropriate safeguards are in place could result in:

- Investigation and potential enforcement action by the Data Protection Commission
- Potential civil liability for the Local Authority if individuals were to sue for breaches of their data protection rights
- Potential inability to use evidence obtained through drone operations in prosecutions if the evidence is deemed to have been obtained unlawfully.

Therefore, it is essential that the planning and preparation for the use of drones for any of the categories of functions outlined above takes appropriate consideration of the potential data protection issues that arise and ensures appropriate safeguards are in place for each instance of the operation of a drone and drone-mounted sensors which might gather data that can be related to an identified or identifiable individual.

It is important to remember that data protection legislation and principles apply throughout the life cycle of data obtained using drone mounted sensors. Additional or secondary uses of data can introduce new or different data protection concerns which will need to be considered for any secondary use of data obtained, whether it is video, audio, still images, or other types of sensor data.

It is also important to be conscious of the potential downsides to the use of drone mounted sensors and recording and ensure that an appropriate balance is struck. For example, researchers have identified what is known as a “Chilling Effect” where people who feel they are under surveillance modify or restricting their behaviours. Therefore, it is essential that drones and drone mounted sensors are used responsibly and in a way which takes appropriate consideration of the data protection rights and other rights of individuals.

This is not a ‘one-size-fits-all’ requirement. The data protection considerations and balance to be struck between the use of drone-mounted sensors and the data protection and privacy rights of individuals will differ depending on the type of use case scenario involved, the location where the drone is to be operating, and the type of sensors in use. The context of any secondary use will also affect the potential data protection considerations that will need to be addressed. Therefore, it is important that the planning and execution of drone operations that involve the use of drone mounted sensors consider the potential data protection implications that arise from the acquisition, analysis, and actions that will be taken based on any data that may be gathered.

Example: A drone is to be used as part of a response to an emergency incident. It is intended to use the drone to assist in the transport of equipment into a hazardous area. The drone will be piloted remotely and will have thermal, gas detection, and optical sensors deployed. The data from the sensors will be recorded for training and after-incident review purposes.

There are two different purposes here, each with a potentially different legal basis and different data protection considerations. Consider what data protection issues and risks might arise?

The Data Protection Principles

The Data Protection Principles that must be considered always are:

Data Protection Principle	What it means in practice
Data must be obtained fairly, lawfully, and transparently (*Transparency)*	• Data Subjects who may have data relating to them recorded need to be aware that there is recording taking place, who is doing it, and why. ○ Have you advised people who might be captured in any video, audio, or still images that a drone with sensors will be operating in the area? ○ Are the operators of the drone clearly identifiable? ○ Have you considered your flight plan and considered how people might "opt-out" by avoiding the area where the drone is operating? ○ Does the information you have provided to people inform them of any analysis (e.g. statistical analysis, data matching, etc.) that might be performed on the data • You need to be clear what is the legal basis you are relying on for capturing the data. For example: ○ Is it data recording you are doing as part of a statutory function performed by the local authority? ○ Is it necessary to protect the vital interests of the data subject or another?
Data must be obtained for a specific and specified purpose and not be used for any purpose that is not compatible with that purpose. (*Purpose Specification)*	• What is the purpose or purposes for capturing data using the drone? ○ Different purposes will require different sensors and may give rise to different data protection and privacy considerations. ○ Secondary uses, such as uses of the data by other stakeholders for different purposes that are not compatible with (i.e. closely related to) the original purposes will require a separate legal basis and this will need to be communicated to any affected data subjects if personal data is to be processed. • It is useful to consider the potential additional uses of data obtained from drones, particularly If this constitutes or contains personal data of individuals and include that in the information provided to data subjects about the use of drone mounted sensors. ○ Where this is not possible, such as where the secondary use or analysis purpose isn't known in advance, consideration must be given to how any data gathered can be de-identified before it is used.

Data Protection Principle	What it means in practice
Data processed must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed. (*Data Minimisation*)	• What sensors are being used on the drone? Is the use of these sensors necessary or appropriate to the purpose? • Can the sensors (e.g. optical sensors such as cameras) be activated for a short period in a defined area to minimise the amount of data that is being captured or recorded? • A key element of this principle is the ***necessity*** test: is it **necessary** for the purpose you have to capture personal data? Could you achieve the objective in a different way that would not capture personal data or would minimise the personal data that is captured? (e.g., opting to use a different kind of sensor, planning a different flight path to reduce risk of data capture, or using a different data capturing method entirely?) • Data protection by design and default should be considered a guiding principle here. Vendors should be pressed on the privacy by design elements within their products at the procurement stage.
Data must be kept in a form that allows identification of data subjects for no longer than necessary for the purposes for which the data is processed. (*Storage Limitation*)	• In practice this means thinking about what data you will save and store and why. ○ Was the data recorded to create statistical information? If yes, is it necessary to keep the recorded data once the analysis has been completed? ○ Will the data be needed for other purposes such as after-incident reviews, or training? If so, can any personal data be redacted (e.g., by blurring faces of people)? • It is also worth considering if data needs to be stored at all – is it sufficient that it is viewed and acted upon with a record being kept of the incident or event that does not include the drone-obtained data? • As a general rule however, retaining recorded data that can be used to identify data subjects should never be done 'just in case' it might be useful in the future. • When considering if data allows the identification of data subjects, it is important to consider what other data processing technologies might be applied to the data in the future which might allow data to be identified. ○ *For example, number plates on vehicles might not directly identify people. However, because local authorities and law enforcement have the ability to link this data to the National Vehicle Driver File (subject to a statutory basis), this data could allow identification of data in the future. Therefore, consideration should be given to whether it should be retained if not required for the purposes for which the data was originally obtained.*
Data must be processed in a manner that ensures appropriate security measures	• Appropriate security measures need to be applied to processing. Bear in mind that processing includes the acquiring of data, the storage of it, the analysis of it, and the sharing or distribution of it. ○ SD cards or other removable storage used to store recorded data (e.g., video or audio recordings) should be encrypted where possible.

Data Protection Principle	What it means in practice
(Data Security)	○ Data that is recorded by a drone should be transferred as soon as possible to an appropriate secure data storage environment (e.g., a secure SharePoint repository or other Local Authority network). ○ Data should be shared with third parties using secure file share facilities. ○ Appropriate access controls should be in place in respect of the recorded data ○ Appropriate organisational controls need to be in place to prevent unauthorised access to data or the unauthorised or inappropriate processing of or combination of data. • This also means that there should be appropriate logs kept of access to data and of transfers of data. This is particularly important in the context of data that is being processed for a law enforcement purpose. ○ ***This is particularly important as Part 5 of the Data Protection Act explicitly requires logs to be kept for processing of data by automated means (i.e. not in a manual form) – See Section 82 DPA 2018.***

Data Protection Principles and Law Enforcement Processing

It is important to note that the data protection principles set out above apply, with some variation, to the processing of personal data by Local Authorities acting as Competent Authorities for the purposes of a law enforcement function. Processing of personal data for law enforcement purposes is governed under the Data Protection Directive for Law Enforcement (Directive 2018/680/EU) which is transposed into Irish law in Part 5 of the Data Protection Act 2018. You should familiarise yourself with the key differences between the normal data protection regime under GDPR and the specific provisions that apply to law enforcement processing.

Part 5 of the Data Protection Act 2018 *only* applies to the law enforcement functions of Competent Authorities (i.e. organisations with a law enforcement function). If the processing purpose is not for law enforcement function, Sections 69 to 104 of the Data Protection Act 2018 do not apply.

General Data Principles for Drones and Drone Mounted Sensors

1) Not all use scenarios are the same. Each drone deployment will need to be assessed on its merits

    a. Always consider context of use. What purpose? What sensors are being used? What location? What other rights need to be balanced?

    b. Consider use of alternative methods where available. Be able to justify any decision to use a drone mounted sensor solution over another method.

2) **Never deploy a technology that is excessive to the purpose, or which could be used to single individuals out or identify individuals unless you have a specific legal basis for the use of such technologies.**

    a. **Facial Recognition, Biometric analysis, ANPR, and similar technologies have limited scope for general use and introduce a higher risk of non-compliance with data protection obligations. They should not be deployed either within the drone solution or as part of subsequent analysis without a clear legal basis and appropriate safeguards.**

    b. **Any equipment which is procured which includes these kinds of technologies should be deployed with them deactivated by default. Ideally, equipment which includes these technologies should not be procured for general use.**

    c. **Vendors should be pressed on the privacy by design and default elements within their products at the procurement stage.**

It is an unfortunate challenge in the marketplace that vendors often emphasise the technical capabilities of their products over building in necessary safeguards and capabilities to ensure compliance with the principles of Data Protection and Privacy by Design and by Default.

However, the reality is that the Local Authority who is purchasing or procuring these technologies or services are Data Controllers with clear obligations and duties in law to ensure that appropriate organisational and technical controls are in place to ensure appropriate protection of personal data and of the fundamental rights of individuals.

It is appropriate that, as part of procurement processes the requirement to support data protection by design and by default is clearly stated and that the potential data protection implications of procured systems are considered so that the purchasing organisation can ensure they implement any additional controls and safeguards in the operation of the systems ***before*** reputational damage or regulatory enforcement risks arise from the inappropriate use of unnecessarily invasive or excessive technologies for otherwise valid and important purposes.

Biometric CCTV systems in the National Children's Hospital
The National Childrens' Hospital hit the headlines in 2019 for procuring hi-definition CCTV cameras with facial recognition capabilities. The National Paediatric Hospital Development Board issued a statement saying that it had not, even after procurement, decided what aspects of the security systems' capabilities would be used. The DPC advised the Hospital Board that a DPIA would be required to demonstrate the necessity and proportionality of such equipment *before* it was deployed.

3) Always choose the least invasive method for gathering the data you need to achieve your purpose

   a. Not all use cases require optical sensors (cameras) or audio recording.
   b. Where possible, generate statistical or measurement data "on device" and only export and store the statistical data.
   c. Only use high-definition cameras where it is necessary for the purposes for which the drone mounted sensors are being deployed.

4) Seek to reduce the chilling effect of drone operations by:

   a. Ensuring efficiencies in planning of operations and reducing the number of drone over-flights of areas through integrated planning and co-ordination of drone use between Local Authority functions and between Local Authorities.
   b. Ensuring effective safeguards are in place regarding the use of drones for monitoring gatherings or events – especially in relation to the recording of camera footage or audio. There needs to be a clear legal basis established for any processing which might result in Special Category personal data (e.g., expression of religious or philosophical beliefs or trade union membership) being processed.

5) Effective drone flight planning is a key safeguard to balance data protection rights.

   a. Avoid overflight of private houses or areas with people where possible. Where not possible, consider what sensors are used and be clear as to the legal basis for the capture and processing of personal data.
   b. Minimise flight times to reduce the risk of unintended personal data capture
   c. Make sure that people in the area are made aware of the use of drones and the purpose for which they are being used in advance of the drone flight.

A Data Protection Decision Tree for Planning Drone Operations

Rather than attempt to define a single decision tree to support data protection risk assessment and decision making across all possible scenarios, this handbook sets out set of key decision points will need to be addressed for any deployment of drones. Each decision point will result in a decision and evidence of that decision.

This “decision tree” sets out four key decisions:

1) Do you need to consider data protection and privacy issues for the specific context of your planned use of drones? There may be circumstances or aspects of your proposed drone use that don’t engage data protection or privacy issues – but you need to consciously consider this and assess the issues and risks.
2) Are you doing something that is an identified scenario, or is it something new? If it’s not new, then there should already be a defined practice and approach for implementing the drone use scenario in an appropriate way. If it is a new scenario, it may give rise to new issues or risks to consider.
3) Do you need to consider doing a DPIA? Again, depending on the nature of the drone use, the novelty of the scenario, or other factors, you may need to do a DPIA. Or you may be able to rely on an existing DPIA and implement safeguards and risk mitigations that have already been defined.
4) Does the usefulness or utility of the proposed scenario outweigh the invasiveness? What can you do to maximise one and minimise the other to ensure an appropriate balancing of objectives, rights, and duties?

It is important to note that these decision trees should be considered a starting point for the decision-making processes around and definition of safeguards for the protection of personal data and privacy in the use of drones and drone-mounted sensors. New technologies and new scenarios for use will arise and these should be assessed against the general principles outlined earlier and against the core data protection principles discussed elsewhere in this handbook.

Decision 1: Do You Need to Consider Data Protection and Privacy Issues?

Data Protection and Privacy issues arise due to the nature of the data logging and data capture capabilities of sensors that are mounted to drones and the potential secondary analysis of that data (remember: the data life cycle is three stages: Acquisition, Analysis, and Action). If a drone or drones will not have sensors mounted to it that will capture data that might identify individuals or interfere with the privacy of an individual's home, and if the analysis of that data will also not allow for individuals to be identified or interfere with the privacy of an individual's home, then the data protection and privacy risks associated with the operation of the drone will be significantly less than if such sensors were mounted. However, it is important to note that the use of optical sensors for drone operations of any kind will bring with it data protection and privacy considerations by default.

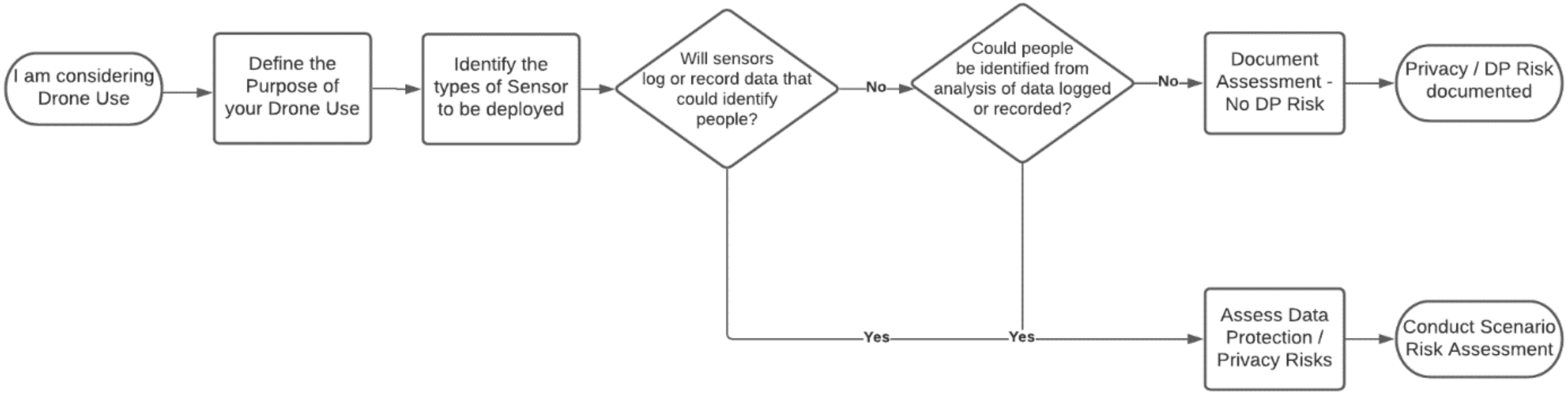

I am considering Drone Use
Define the Purpose of your Drone Use
Identify the types of Sensor to be deployed
Will sensors log or record data that could identify people?
No
Could people be identified from analysis of data logged or recorded?
No
Document Assessment - No DP Risk
Privacy / DP Risk documented
Yes
Yes
Assess Data Protection / Privacy Risks
Conduct Scenario Risk Assessment

Figure 5: Drone Use Decision 1 for Data Protection

Evidence of Decision: A record should be created of the purpose, the proposed sensors, and the basis for deciding that there is no data protection or privacy risk. This should be shared with the DPO.

Example: A light show is proposed using drones flying in a pre-planned formation display that will be similar to a fireworks display. The sensors to be used for this purpose will be the GPS and flight control and proximity sensors of the drones. There will be no optical sensors deployed on these drones.

The assessment in this decision point is that there is no Data Protection or Privacy Risk as no optical sensors are being used. This is documented as part of the planning for the display and a copy is sent to the Data Protection Officer of the Local Authority for reference.

Decision 2: Are you doing something that is an identified scenario, or is it something new?

The definition of categories of use case for drones and different kinds of drone-mounted sensor will allow Local Authorities to develop standard Data Protection Impact Assessments for each kind of use case. These standard data protection impact assessments will provide a basis for quickly assessing the appropriateness of safeguards to be implemented in any context and will also clarify the legal basis for processing for that scenario.

If a DPIA has been carried out, each operation of a drone and drone-mounted sensors can be documented using a “pre-flight” checklist rather than having to conduct a full DPIA each time.

However, if the processing purpose includes new technologies, new processing capabilities, or will result in new types of action or decision being taken by a Local Authority, it may well be that this is a new type of Use Case scenario that will require a DPIA of the novel aspects of that processing to make sure that there is appropriate clarity on the relevant legal basis, transparency, and safeguards to be applied.

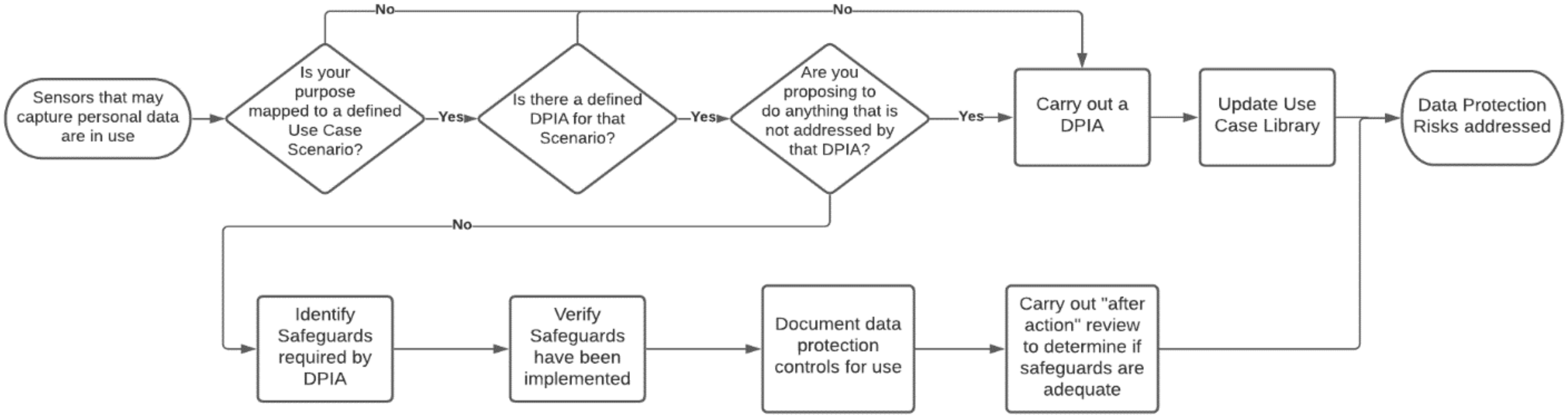

Sensors that may capture personal data are in use
Is your purpose mapped to a defined Use Case Scenario?
Yes
No
Is there a defined DPIA for that Scenario?
Yes
No
Are you proposing to do anything that is not addressed by that DPIA?
Yes
No
Carry out a DPIA
Update Use Case Library
Data Protection Risks addressed
Identify Safeguards required by DPIA
Verify Safeguards have been implemented
Document data protection controls for use
Carry out "after action" review to determine if safeguards are adequate

Figure 6 Decision Point 2: Is there a DPIA already or is this something new?

Example: A local authority decides to operate a drone with a high-resolution optical sensor to monitor amenity areas for the movement of people during a period of travel restrictions imposed due to a public health issue. The optical sensors will be used to gather data for a statistical count of vehicles parked in carparks near amenity areas. However, there is also an expectation that footage may be used to prosecute people who have breached public health restrictions.

The statistical measurement of the number of vehicles at an amenity is something which, in this scenario, has been the subject of a DPIA as it is a scenario in the Monitoring/Measuring family of Use Cases[15]. However, the use of the data to enforce public health restrictions is a new purpose and a DPIA is required to ensure that there is a clear legal basis for this use and that the appropriate safeguards are implemented in respect of that additional processing activity and purpose.

Evidence of Decision: The evidence of decision at this point is a record that the proposed drone use falls within the scope of processing for which a DPIA and defined safeguards already exists or that a new DPIA is required. If the former, records should be kept of the safeguards implemented and it is good practice to conduct an “after action review” to identify any improvements to processes or safeguards that might need to be considered.

If the latter, the commencement of a DPIA is the evidence of decision and should be recorded.

[15] Note: in reality a DPIA for this Monitoring and Measurement use case scenario has not, at the time of writing, been completed and this example is presented for illustration purposes only.

The Benefits of a Taxonomy of Use Cases

This decision point highlights the benefits of a taxonomy of use case scenarios for which DPIAs can be completed. The taxonomy we outline in this handbook has identified four main families of scenario, with sub-types of use being defined based on the specific objectives or purposes, combinations of sensor technologies, or locations for operation. For each of these families of scenarios a Data Protection Impact Assessment (DPIA) can be defined along with a standard set of safeguards and controls. More specific DPIAs can be defined for more complex or high-risk scenarios if necessary.

The WERLA has produced an extensive DPIA and Dynamic Risk Assessment for the use of drone mounted optical sensors for waste management enforcement. This falls within the **Investigation and Enforcement** family of use cases. As such, the issues identified in by that DPIA will be largely common to other Investigation and Enforcement use case scenarios. However, the context of operations may be different in other Investigation and Enforcement scenarios. This may require a DPIA for those scenarios to identify the different safeguards that will be required. For other families of Use Case Scenario, DPIAs should be developed.

The taxonomy of use cases should also be linked to and support the recording of the use of drone mounted sensors and associated technologies as part of the Local Authority's Register of Processing Activities under Article 30 GDPR and, for law enforcement functions of a Local Authority, Section 81 of the Data Protection Act 2018

The table below sets out some examples of differences that might need to be considered when assessing or evaluating new use case scenarios within a family of use cases. It is also important recognise that new sensor types, new analysis technologies, new drone capabilities, or new legislative or policy requirements can give rise to new families of use case or can change the risk assessment for existing scenarios. As such, the taxonomy of use cases and their associated DPIAs should be managed based on continuous improvement and kept up to date.

Consideration	Example Differences that may arise
Legal Basis for Acquisition, Analysis, or Action	Waste Management Enforcement DPIA specifies a legal basis under the Waste Management Act. This legal basis explicitly allows for the taking of recordings and photographs.
	What is the legal basis for the use of the type of sensor or data capture you are proposing? Is the legislation sufficiently clear that it would be reasonably foreseeable that a drone-mounted sensor could be used for this purpose? If no statutory basis can be identified, what other legal basis can you rely on under Data Protection law?
Context of Operations	The WERLA Waste Management Enforcement DPIA deals with the use of drone mounted optical sensors to record video and still images of an area that would not normally be accessible to the public and where it is possible to implement safeguards to minimise the risk of secondary capture of personal data and where individuals at the location can be informed of the use of drone mounted recording devices. The context of use also provides a basis for the data retention period that is applied in this DPIA (5 years), which is based on the length of permits and licences.
	Consider the context of your proposed drone operation. Will it be in an area where access by 3rd parties could be restricted temporarily? What safeguards could be implemented re transparency, data minimisation etc.? **What would the appropriate retention period be for data that might identify an individual in your use case scenario? If optical sensor data (video) is recorded to allow for analysis of plant types in an area, how long should those recordings be kept? If people are recorded in the data, can they be cropped from retained still images or blurred in retained video?**
Context of Technologies to be used	The WERLA DPIA deals with the recording of video only, the transfer of that video to the Local Authority, and the sharing of that video with 3rd parties if necessary. It does not include any other sensor type or other form of analysis technology or combination with other data (e.g., ANPR or object or event detection using machine learning).
	Consider if you are using other sensor types or using other technologies in your processing and whether this might give rise to additional risks to the data protection rights and other rights of individuals and what additional safeguards or legal grounds for processing might be considered as part of a DPIA.

Figure 7 Example of differences to consider between an existing DPIA and a new scenario

Decision 3: What do you need to consider in a Data Protection Impact Assessment?

Article 35(7) of GDPR sets out the minimum requirements for Data Protection Impact Assessments:

1) The approach be systematic (i.e., should follow a defined and repeatable process)
2) It should describe the proposed processing operations and their purposes.
3) It should include an assessment of the risks to the rights and freedoms of individuals
4) It should define measures that are envisaged to address these risks, including safeguards, security measures, and other mechanisms to ensure the protection of personal data and to demonstrate compliance with data protection law, taking into account the rights and legitimate interests of data subjects and others.

Regardless of what format template is used to write up the final output of a DPIA in any Local Authority, the process should seek to define and answer key questions about the proposed processing activity, the associated risks, and the proposed mitigations. It is also essential that the DPIA demonstrates that the proposed processing operation is both **necessary** to for the purposes that the Data Controller is pursuing and is **proportionate** to those objectives. This means that a DPIA must also set out a fact-based assessment of the effectiveness of the proposed measure and whether it is more, or less, intrusive than other methods or approaches. This is a key part of the philosophy of Data Protection by Design and by Default we discussed earlier in this handbook.

The steps outlined below provide a generic approach to ensuring the right questions are asked so that they can be documented appropriately, regardless of the final templates that may be adopted in any organisation.

Where a less intrusive method or approach is possible, this should be preferred over a more intrusive method. For example, if data from optical sensors are not required for your purpose, the drone you select should not have cameras mounted on it or should have them deactivated, except where necessary for flight safety reasons (which is a different purpose with a different balancing of rights to consider).

The key objectives of a DPIA are:

Describe the processing activity	• What is to be done (processing), • How is it to be done (methods), and • Why is it to be done (purpose for processing)
Identify the legal basis for processing	• What is the lawful basis for processing? • If a statutory basis, is the proposed processing foreseeable in the underlying legislation?
Assess necessity and proportionality	• Is the processing necessary and proportionate for the purpose? • Can it be done a different way?
Identify Issues, Risks, and Safeguards	• What are the risks to rights and freedoms identified? • What safeguards and mitigations can be implemented?

Standard Steps in Analysis

The Data Protection Impact Assessment Methodology is based a standard set of process steps that are to be considered when conducting a Data Protection Impact Assessment. These standard steps apply to both Triage Assessments and more detailed Data Protection Impact Assessments. **Error! Reference source not found.** below illustrates the key process steps that are described here.

Step 1: Define Goal and Approach

This step in the process requires the Process Lead to define the business goal (aka Business Need) and the high level approach that is proposed to obtain that goal or execute that objective.

This is defined in the form of a problem statement:

> We want to [*describe the processing proposed*] so that we can [*describe business objective / goal*] for the following benefits [*outline benefits to the organisation and to data subjects*]

Step 2: Analyse the Information Environment

The "Information Environment" is the scope of the processing. You should consider:

- What types of data or what categories of data are being processed? This will be a function of the type of sensors that are to be mounted to a drone and the types of analysis or data processing that will be done on data acquired from those sensors.

- What technologies are to be used to process this information? For example, will you be using object recognition machine learning to automate the counting of people in a location or LiDAR technologies to map an area?

- What types of data subject will you be processing data about (e.g., staff, contractors, or other categories)?

- What is the legal environment surrounding the processing? Is there a clearly defined legal basis for this processing? Is there a statutory basis for this processing? Are there any other legal or regulatory issues that need to be considered?

- Who are the stakeholders for this processing (internal and external)? It is important to consider the views of external stakeholders such as members of the public, particularly in relation to the use of technologies which may be surveying or monitoring publicly accessible areas or which may encroach on the privacy of the home.

By thinking about these issues in a structured way you can develop an understanding of the potential issues and risks associated with the different aspects of the processing. It also provides a basis for the Data Protection Officer or other stakeholders to engage in any review of the issues and risks associated with the processing.

Step 3: Confirming if Personal Data is being Processed

As outlined earlier in this handbook Personal data is defined in GDPR as

> *"… any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"*

An important step in the DPIA process is to establish whether personal data is being processed. If there is no personal data being processed, a DPIA may not be required but assessments of risks associated with the security or quality of data may need to be conducted.

It is important to note that where it is determined that there is no personal data in scope this is not a definitive determination and will require constant reassessment as a project or initiative is implemented, particularly where the proposed processing is innovative, or new, or as new technologies are deployed.

Step 4: Assess if the objective can be met with alternative methods

It is important as part of assessing the *necessity and proportionality* of any proposed processing that the organisation can show that the processing is necessary for the proposed objective.

This requires an assessment of whether the goal can be delivered using alternative approaches that would not require the processing of personal data or the processing of less invasive amounts of personal information.

If an alternative method would meet the needs of the organisation, there will need to be a clearly identified rationale for continuing with the processing as proposed.

Step 4a: If no Personal Data: Monitor Process and Implementation

As outlined above, if there is no personal data being processed, the Process Lead must still ensure that the process and its implementation is monitored to ensure that changes to the process do not result in personal data being included in the processing.

Step 4b: Identify Root Causes of Data Protection Issues / Risks

Where personal data is being processed and risks to the rights and freedoms of the data subject are identified it is important to understand the root causes of the data protection issues and to ensure that appropriate actions are taken to mitigate and manage these risks.

For example, if one of the risks identified is that data is being processed using spreadsheets to capture or transfer data, the root cause of the risk is the relative lack of security over the spreadsheets and the potential for data to be manipulated in spreadsheets. The mitigation might be to change the proposed approach to processing to remove spreadsheets from the process or to implement appropriate security controls over the storing and sharing of spreadsheets.

Step 5: Define Improvement Plan

Based on the understanding of root causes identified, you should define your improvement plan to address those root causes. This should be a clear set of actions to address the identified risks with a clear definition of what is to be done by whom.

Step 6: Define Necessary Controls

Associated to the Improvement plans, you should define the organisational or technical controls that are necessary to mitigate or manage the identified risks and to make sure that the improvements defined in Step 5 are working.

Step 7: Handover to Project team (if appropriate) to implement or remediate

It is not enough for an organisation to carry out a DPIA and identify controls etc. It is essential that these are translated into requirements for implementation by any project team or by the business area.

A DPIA without implementation of mitigations is an ineffective control.

This handover may include:

- Development of dynamic risk assessment templates or checklists for 'in the field' operations of drones for the defined use case scenario
- Standardised templated information leaflets that can be provided to affected data subjects
- Templated data protection notices for use in operations
- Requirements for updates to organisation-wide data protection notices
- Requirements for legislative changes to improve the safeguards and clarity of legal basis for processing.

Step 8: Communicate Actions and Results

At each stage in the DPIA process the person carrying out the DPIA will be expected to communicate the actions taken and the results delivered. At a minimum this will take the form of one or more of the following:

1) Documentation of Triage Threshold Assessment for full DPIA

2) Documentation of identified issues / risks, their priorities, and recommended actions

3) Briefing information for stakeholders on proposed processing, identified issues and risks and mitigations

4) Assessment of alternative approaches

5) Specification of process or systems changes that must be implemented to mitigate identified risks

6) Updates to Data Protection Notices, Data Protection Policies, Registers of Processing Activities, or other controls or procedures documentation.

Depending on the complexity of the proposed processing and/or the level of risk identified associated with the processing more information may need to be documented and communicated. As such, it is difficult to be prescriptive on the specifics of documentation or communication activities that might be required.

It is important that the Data Protection Officer be consulted to ensure that all relevant documentation and communication requirements are identified and implemented appropriately.

Decision 4: Utility versus Invasiveness

When assessing the information environment and the suitability the proposed processing using drone mounted sensors when carrying out a Data Protection Impact Assessment, it is useful to consider what the balance is between Utility and Invasiveness of processing. This model is set out in *Ethical Data & Information Management: Concepts, Tools, and Methods*[16].

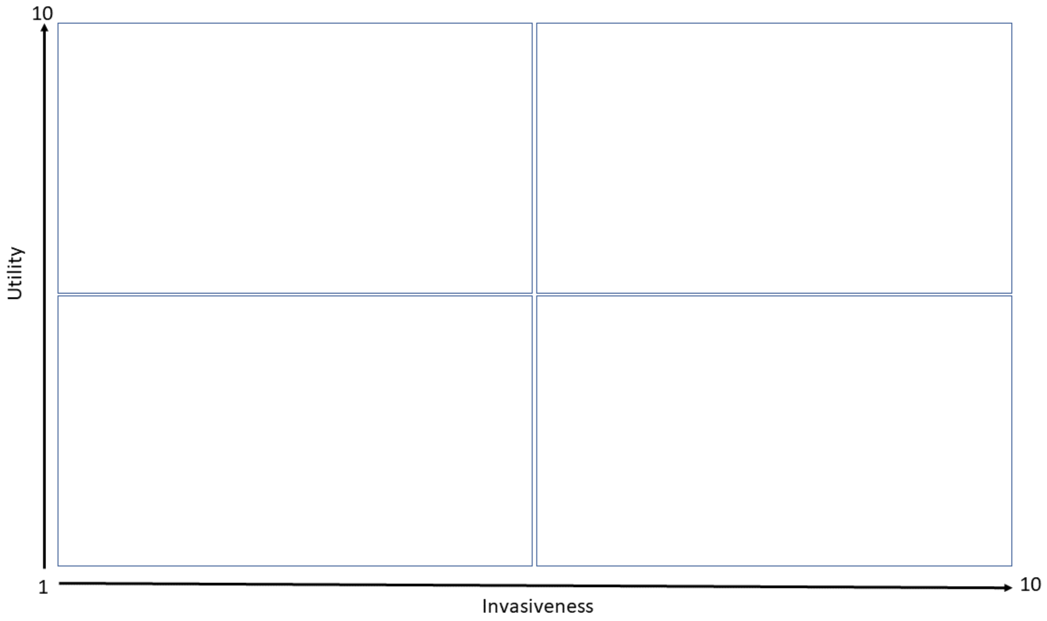


Figure 8 The Utility vs Invasiveness Matrix (adapted from O'Keefe & O Brien, 2018)

- Rate the usefulness or utility of the proposed processing on a scale of 1 to 10
- Rate the level of invasiveness of the processing on a scale of 1 to 10
- The objective is to maximise the utility and usefulness of processing while keeping the invasiveness of the data capture and processing to a minimum.
- When assessing the data protection and privacy impacts of proposed processing it is useful to consider how the invasiveness of processing might be reduced through the application of appropriate safeguards and controls.
- It is also worth considering if the processing can be made more useful or of higher utility to society as a whole.

[16] *Ethical Data & Information Management: Concepts, Tools, and Methods,* O'Keefe, K, O Brien, D, Kogan Page, 2018 at page 273-276

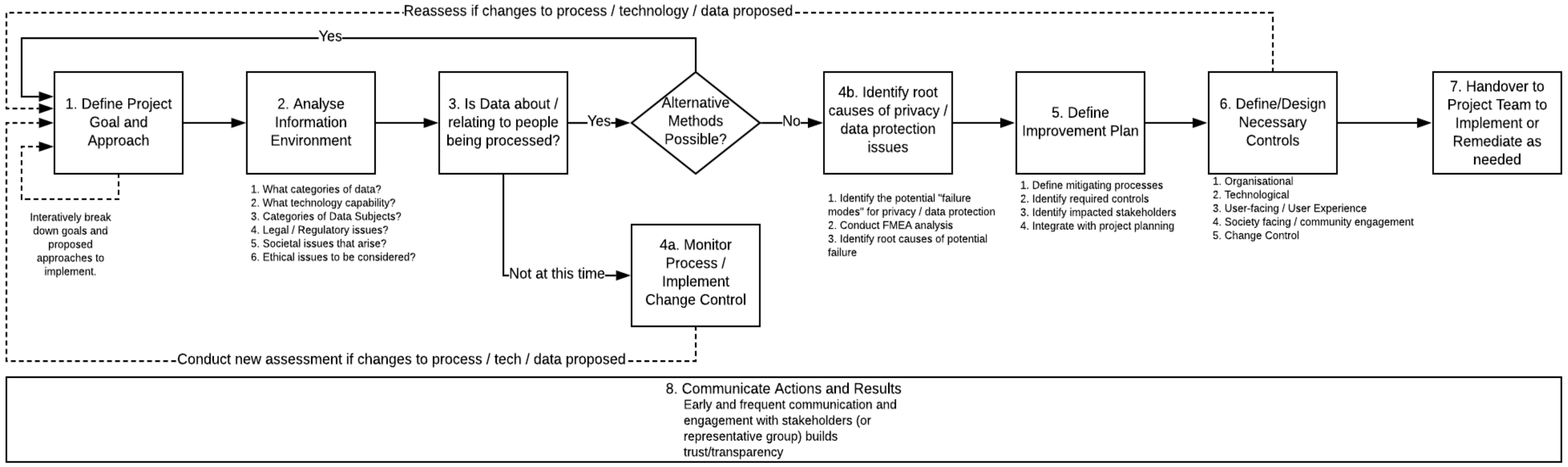

Reassess if changes to process / technology / data proposed
Yes
1. Define Project Goal and Approach
2. Analyse Information Environment
3. Is Data about / relating to people being processed?
Yes
Alternative Methods Possible?
No
4b. Identify root causes of privacy / data protection issues
5. Define Improvement Plan
6. Define/Design Necessary Controls
7. Handover to Project Team to Implement or Remediate as needed
Interatively break down goals and proposed approaches to implement.
1. What categories of data?
2. What technology capability?
3. Categories of Data Subjects?
4. Legal / Regulatory issues?
5. Societal issues that arise?
6. Ethical issues to be considered?
Not at this time
4a. Monitor Process / Implement Change Control
1. Identify the potential "failure modes" for privacy / data protection
2. Conduct FMEA analysis
3. Identify root causes of potential failure
1. Define mitigating processes
2. Identify required controls
3. Identify impacted stakeholders
4. Integrate with project planning
1. Organisational
2. Technological
3. User-facing / User Experience
4. Society facing / community engagement
5. Change Control
Conduct new assessment if changes to process / tech / data proposed
8. Communicate Actions and Results
Early and frequent communication and engagement with stakeholders (or representative group) builds trust/transparency

Figure 9 Standard DPIA Process Steps (Example)

Example:

A fire service is deploying drones as part of their standard response to fires and hazardous materials incidents. These are identified as being part of the **Incident Response & Planning** family of use cases. The scenarios identified include:

- Use of drones to move equipment at the scene where it would be hazardous for fire officers to do so, using pilot directed drone flight supported by optical sensors.
- Use of thermal and gas sensors on drones to survey scenes for risks and provide real-time information to responders about fires, hazards, and location of people.
- Recording aspects of incident response using optical sensors and audio sensors for post-incident review and training purposes.

All scenarios will require the use of optical sensors. The proposed contexts for deployment will necessitate the processing of special category data in certain circumstances. A DPIA will need to consider at least the following:

Purpose	Fire Service to use drones to support incident response operations by transporting equipment and surveying a scene for hazards and risks that will affect incident response and to record aspects of incident response so it can respond more effectively, reduce risk to responders and the public, and improve training and planning for incidents.
Legal Environment	Section 28 of the Fire Services Act 1981 empowers the person in control at a fire or other emergency to do all such things that are, in their opinion, necessary or expedient for extinguishing fire or protecting or rescuing persons or property. However, this does not explicitly address the use of drones or set out any safeguards relating to the use of drones. It therefore may not meet the requirements of Article 23 GDPR Article 6 and Article 9 of GDPR allow for the processing of personal data where it is necessary to protect the vital interests of data subjects or other natural persons.
Categories of Data	• Video recording (optical sensors) capturing people's images ○ Video images may also include special category data relating to injuries to persons associated with the incident • Audio recording • Thermal imaging (optical sensor, multi-spectral imaging) • Gas sensors (non-personal data)
Risks (example)	• Absence of clear statutory basis is a risk. However, Article 6(1)(d) arguably provides a basis in exceptional circumstances. • Audio recordings may capture personal data, particularly if combined with video. • Identifiable persons may be captured on video that is retained for training
Safeguards/ Mitigations	• Will recordings be saved to secure data repository such as SharePoint? • Will videos be redacted to remove identifiable features of people before being used for training? • Will legislative changes to be made to clarify legal basis for operation of drones and define relevant safeguards?

PART 3: BEST PRACTICE RECOMMENDATIONS

Best Practice Recommendations

There is no "one size fits all" approach or template that can be applied to the deployment of drones and drone mounted sensors by local authorities. However, adopting a structured and strategic approach to assessing and planning for the responsible use of drones it will be possible to quickly adopt and adapt appropriate technologies to the needs of Local Authorities and their stakeholders.

Recommendation 1 – Adopt a taxonomy of use cases and scenarios

By adopting a structured framework for identifying use cases and scenarios for the deployment of drones and drone mounted sensors, it will be possible to:

1) Identify commonly occurring areas of risk
2) Standardise templates for the documentation of data protection impact assessments for the deployment of drones in specific circumstances
3) Apply a 'design pattern' approach to any new use cases or emerging technologies that local authorities might wish to deploy.

Recommendation 2 – Develop a Library of DPIAs for identified use cases and scenarios

For each use case scenario that is defined, a DPIA should be developed. These should be made available as a centralised resource. New use case scenarios should be compared against this central library of data protection impact assessments.

This will have the benefit of:

1) Improving standardisation and consistency of approaches between Local Authorities
2) Reducing the time required to carry out DPIAs for drone operations

Recommendation 3 – Develop a Library of standard mitigations and controls

Related to the library of DPIAs should be library of standard mitigations and controls which can be adopted and applied to any proposed use of drone mounted sensors. These should include measures relating to transparency of processing, retention periods for data, and assessing the necessity and proportionality of processing.

This will have the benefit of:

1) Improving standardisation and consistency of approaches between Local Authorities
2) Simplifying the deployment of safeguards and controls and associated training.

Recommendation 4 – Seek to use the least invasive technologies possible for your objective

Many data protection and privacy issues associated with the use of drone-mounted sensors can be mitigated using more appropriate sensors and related technologies. This should be a fundamental principle that is applied in the specification and procurement of drones, sensors, and associated technologies and services.

This should be applied across the full life cycle of the data obtained, from acquisition to action.

Technologies such as facial recognition should not be deployed without a specific statutory basis and a clearly established necessity and proportionality. It is recommended that a specific DPIA should be undertaken for the use of any technologies that will be used to single out or identify individuals in video or other types of recorded data.

Recommendation 5 – Ensure Registers of Processing Activities are updated

The Register of Processing Activities is a key governance and control tool for data protection compliance. The use of drone mounted sensors for local authority functions should be recorded in the Register of Processing Activities.

This should be related to the classification of drone operations use cases defined in the taxonomy of use cases and should be derived from the outputs of DPIAs that have been completed for each category of use case.

Article 30 of GDPR and Section 81 of the Data Protection Act 2018 set out the requirements for information to be recorded in a Register of Processing Activities for both general data processing and for processing activities in a law enforcement context. This information includes:

- Identification of categories of affected data subjects
- Identification of categories of personal data being processed
- Description of the purposes for processing personal data
- Categories of recipients for that data
- Details of any transfers of data outside the EU/EEA, and the basis for those transfers
- The time limits for the erasure of the different categories of data
- A general description of organisational and technical security controls to protect personal data.

Recommendation 6 – Consider the life cycle of data and potential secondary uses

It is easy to focus on the Acquisition stage of the life cycle of data captured using drone mounted sensors. However, it is important to think about the potential data protection and privacy issues and risks along the entire life cycle of the data, as well as the opportunities to mitigate issues and risks.

Depending on the nature of the secondary use, it may require a separate legal basis to be identified or may constitute a new use case scenario that could need a separate DPIA to be completed.

- If video data is being recorded for statistical analysis purposes and data relating to identifiable people is captured, consider whether the source recordings need to be retained once the statistical processing has been carried out. If it does, consider how long that data needs to be retained for and what controls around access to that data need to be put in place.
- If data is obtained from drone mounted sensors for an operational purpose, consider whether that recorded data might be required for future training purposes. If it will be used for training purposes, this is something that would need to be disclosed in data protection notices. You would also need

Recommendation 7 – Improve Transparency

Transparency of planned drone operations can be improved through the development of a public register of planned flights that provides access to information about when, where, and why drone-mounted sensors are being used by Local Authorities.

This should build on the development of a taxonomy of use cases and the development of DPIAs for use case scenarios by providing access to the DPIAs for the scenarios that are being supported by the drone operation.

Unplanned emergency deployments of drones for emergency service use case scenarios could be retrospectively added to the published list of drone flights. The development of standard DPIAs will support transparency in these contexts.

Where drones are deployed for a purpose related to a law enforcement function of a Local Authority these flights should also be added retrospectively once disclosure will not prejudice the conduct of an investigation or a prosecution. Consideration should be given to the application of the CJEU ruling in *Watson/Tele2* in respect of mass surveillance of telecommunications where the CJEU ruled that where mass surveillance is deployed for the investigation of a serious criminal offence, those persons who were surveilled but were not subsequently charged with a criminal offence should be made aware of the fact of the surveillance as soon as possible after the risk to the investigation or detection of offences has passed[17].

Recommendation 8 – Where necessary implement appropriate statutory basis

Historic legislation often contains broadly framed powers for requesting information or taking actions. However, such legislation may fail to meet the requirements of necessity, proportionality, and foreseeability of processing that are required under data protection law. Historic legislation may also lack clearly defined safeguards as required under Article 23 of GDPR.

Therefore, where a Data Protection Impact Assessment identifies a potential statutory basis for processing, it is recommended that this statutory basis be critically reviewed and any amendment or additional legislative measures that may be required are introduced to ensure appropriate safeguards over the processing of personal data.

[17] Cases C-203/15 and C-698/15, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62015CJ0203

Recommendation 9 – Reduce the number of drone operations by co-ordinating flights

Related to Recommendation 7 above, it is recommended that internal governance in relation to drone operations be introduced that will support a “fly once, use many” philosophy that will encourage departments to deploy appropriate technologies to maximum benefit while reducing the potential sense of surveillance that people may feel arising from drone operations in an area.

Complementary Use Case Scenarios should be identified within the taxonomy of use cases where there is an overlap in respect of sensors to be used and data to be captured.

Example:

A drone flight is planned for a Monitoring and Measuring Use case to assess the status of a riverbank area near houses through a real-time visual inspection. The flight will use high-definition optical sensors to perform a visual inspection of the bank stability and any erosion patterns along a defined stretch of the river to inform planning of preventative maintenance and flood control works.

There has been a report of an invasive plant species outbreak in the area. The use of drone a drone survey of the area has been considered. The fact that a drone will be operating in the area with an appropriate sensor technology means that no additional drone flight is required, but:

- The drone flight path will need to be altered to include a survey of vegetation in the area and the ends of gardens adjoining the riverbank to identify any invasive species
- The drone-mounted camera will need to save a recording of the captured video and still images so that the data can be analysed for presence of invasive species using both visual inspection and a machine learning process.
- The information to be provided and published about the purposes of the drone flight will need to be updated

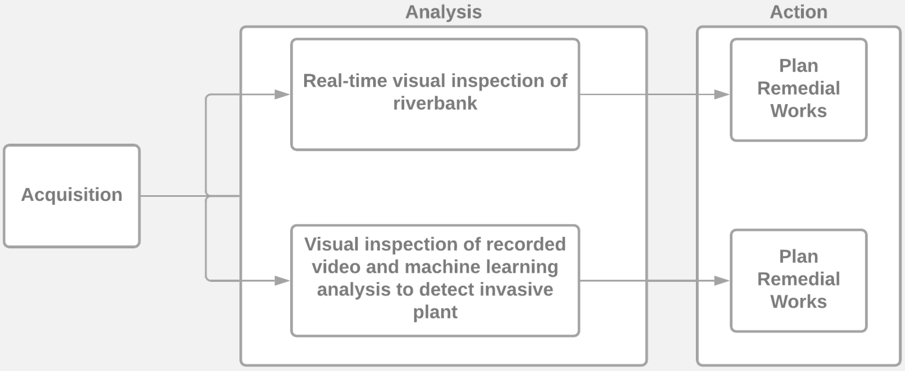

Analysis
Action
Acquisition
Real-time visual inspection of riverbank
Plan Remedial Works
Visual inspection of recorded video and machine learning analysis to detect invasive plant
Plan Remedial Works

Figure 10 Acquisition, Analysis, and Action in practice

Recommendation 10 – Develop a Code of Conduct for Drone Operations

A Data Protection Code of Conduct for Drone Operations that builds on a taxonomy of use cases, establishes a baseline set of standard controls and safeguards for each use case, and has appropriate oversight mechanisms and can be extended to reflect new use cases or technologies is strongly recommended.

Mapping Recommendations to the DPIA Framework for Drones

The development of this handbook has highlighted the importance of developing a taxonomy of Use Case Scenarios for drones in Local Authorities which support the carrying out of relevant and appropriate DPIAs and the development of standardised controls and safeguards which can be implemented easily in operational procedures and practices.

The work which has been carried out by WERLA in developing a DPIA and associated procedures for Waste Management Enforcement is a clear example of the benefit of this kind of approach for Local Authorities.

WERLA Use Case Scenario Classification

The WERLA DPIA addresses a scenario in the Inspection and Enforcement category of use cases, specifically the Waste Enforcement functions of the Local Authority. Therefore, for other local authority law enforcement functions within this category of Use Case Scenario, many of the considerations will be the same or similar and this DPIA provides a useful reference template. For Use Cases in other categories, the structure and approach is still informative and the defined template for the DPIA is sufficiently generic as to be applicable for any Use Case Scenario category.

Clarity of Legal Basis for Processing

The WERLA DPIA   clearly establishes the legal basis for processing and the necessity and proportionality of the proposed processing for the Use Case Scenario identified. It also highlights the limitations and constraints on the specific operation.

- It is constrained to waste management facilities where there is a reduced risk of capturing personal data of third parties
- It is constrained to an operating environment where it is relatively easy for the inspector to notify affected persons of the operation of a drone with drone mounted sensors.
- It sets out a retention period with a clear rationale.
- It addresses the necessity and proportionality with reference to alternative methods for conducting similar evidence gathering or surveys of facilities.

Other Use Case Scenarios will have different constraints. For example, the operation of a drone mounted optical sensor in a public place for a waste management enforcement activity would require a different DPIA as it gives rise to different constraints and considerations and would likely result in the capturing or processing of personal data of third parties. The weighing of necessity and proportionality will be different in different scenarios.

Specification of Safeguards

The WERLA DPIA for Waste Management enforcement contains a variety of safeguards to ensure appropriate protection of personal data and other fundamental rights and freedoms.

Some of these safeguards will be common to all Use Case Scenarios. Others will be specific to an Investigation and Enforcement Use Case. Others will be relevant only to the operation of optical sensors for recording of surveys of waste management facilities. However, the identification and classification of safeguards and mitigations can help inform the output of other DPIAs, as recommended above.

Conclusion

Local Authorities should adopt a strategic approach to the classification of drone sensor use cases and the categorisation of data protection and privacy risks associated with the operation of data capture using drones.

By developing a taxonomy of use cases for drone-mounted sensors that takes into consideration a life cycle of data from Acquisition to Analysis to Action and which applies a Data Protection by Design philosophy it will be possible to develop appropriate processes, procedures, and safeguards for the operation of drones and drone-mounted sensor technologies that is both simple to use but also supports the continued development of data protection governance in this area that can keep pace with the rapid evolution of technologies and potential scenarios for use.

Associated with this taxonomy of Use Cases should be a library of DPIAs and associated safeguards, controls, and standard procedures to mitigate risks and ensure an appropriate balancing of individual rights with the needs of local government operations.

Within this framework of Use Cases, DPIAs, and standardised safeguards will need to be an adoption of core policies and principles around the careful and responsible deployment of technologies and the linking of data gathered from drone-mounted sensors with other data from other sources in a way which could identify or otherwise impact on individuals and their rights and freedoms.

Technologies such as facial recognition, ANPR, and Artificial Intelligence applications will need to be considered carefully and deliberately to ensure that their impact on data protection rights and other rights and freedoms is necessary and proportionate. This will require careful attention to the technologies being procured and deployed as often these additional analytics capabilities are acquired as a bundled by-product of procuring otherwise straightforward systems[18].

Local Authorities should aim to develop these libraries of Use Case Scenarios, DPIAs, and associated safeguards as the basis of a Code of Conduct for data protection compliance in the use of drone-mounted sensors and associated technologies. Within this there should be recognition that there are use cases for drones which do not require the capture or processing of personal data at all, but even then, there is a need to 'trust but verify' through appropriate governance, controls, and transparency.

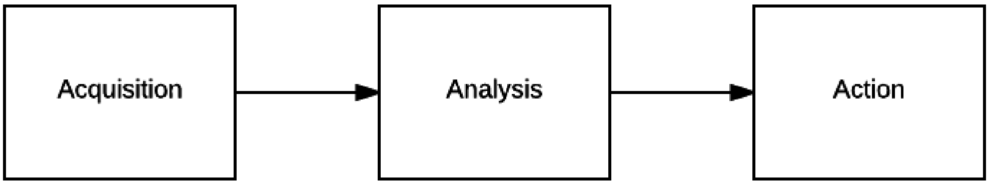


Figure 11 The High-Level Data Life Cycle

[18] *Facial Recognition technology latest woe at National Children's Hospital*, Irish Times, 12th December 2019 https://www.irishtimes.com/business/technology/facial-recognition-technology-latest-woe-at-national-children-s-hospital-1.4112451

Appendix 1 – Level 2 and Level 3 Use Case Taxonomies

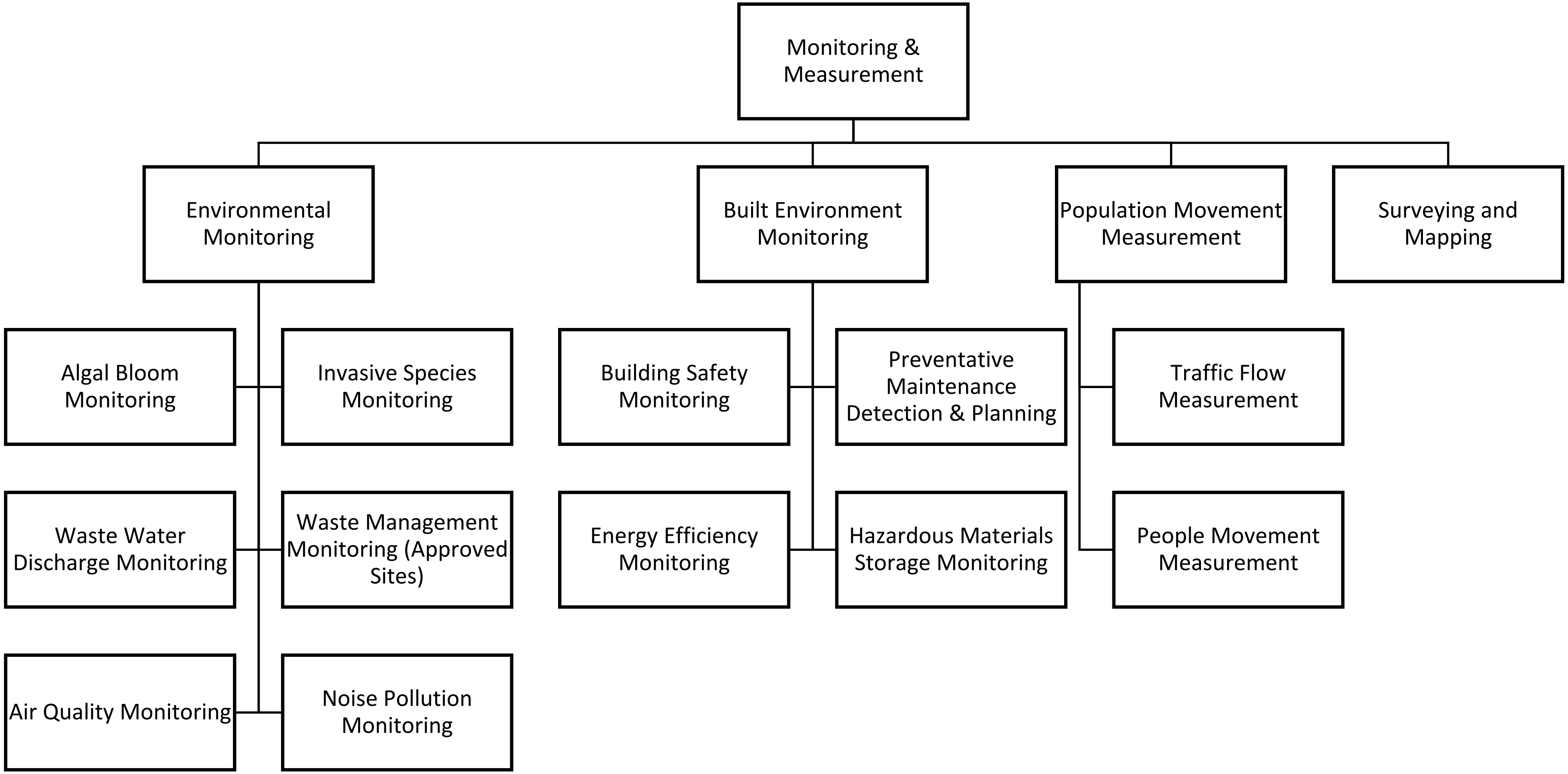
The scenarios and use cases identified at Level 3 of this taxonomy are generally examples of specific use cases or categories of specific use case. Within each of these categories it should be possible to identify a clear **Action**, a defined approach and method for **Analysis**, and to determine what types of drone mounted sensor would be used for the **Acquisition** of the data being processed. If necessary, an additional level of classification could be introduced for more granular definition of use cases and scenarios. This has been done for this handbook in the context of scenarios relating to the investigation and enforcement of statutory functions of a local authority.

At this level of Use Case definition it should be possible to identify the commonly occurring data protection and privacy issues that may arise in the context of the use case and define a set of recommended mitigations to be applied in each case. These can then be aggregated into Standard Operating Procedures for the type of drone use envisaged.

These Standard Operating Procedures should then be used to support the Data Protection and Privacy Impacts decisions that must be documented as part of the evidence of the operation of controls for Data Protection by Design and by Default that is required under Data Protection legislation.

It should be noted that the examples provided in the tables below are for illustrative purposes only in this handbook. In the interests of brevity they do not examine the legal basis for any processing in the scenarios discussed.

It should also be noted that the taxonomy of use cases and scenarios presented here is not exhaustive. Scenarios may arise which can be added over time. What this handbook has aimed to do is provide a structured way of classifying scenarios so that common data protection risks and issues can be identified and so that the governance controls and decision making processes around the use of drone-mounted technologies can be simplified.


Monitoring & Measurement
Environmental Monitoring
Built Environment Monitoring
Population Movement Measurement
Surveying and Mapping
Algal Bloom Monitoring
Invasive Species Monitoring
Waste Water Discharge Monitoring
Waste Management Monitoring (Approved Sites)
Air Quality Monitoring
Noise Pollution Monitoring
Building Safety Monitoring
Preventative Maintenance Detection & Planning
Energy Efficiency Monitoring
Hazardous Materials Storage Monitoring
Traffic Flow Measurement
People Movement Measurement

Environmental Monitoring

Taxonomy Level 3	Definition	Example Acquisition and Analysis Approach
Algal Bloom Monitoring	Use of drone mounted sensors and associated analytics technologies to identify, map, and measure the extent of algal bloom outbreaks and inform planning around remedial actions	• **Acquisition:** Drone survey of an area using optical and hyperspectral imagery • **Example Risk:** overflight of homes or individuals in public or private areas while optical sensors are active and/or recording. • **Example Mitigation:** ○ Activate optical sensors only when over target area (measured by GPS mapping). ○ Apply narrow framing of optical imagery to reduce risk of secondary capture. ○ Select optical sensor with appropriate resolution to reduce risk of unnecessary capture of high definition video imagery in which people could be identifiable
Invasive Species Monitoring	Use of drone mounted sensors and associated analytics technologies to identify, map, and measure the extent of invasive species outbreaks and inform planning around remedial actions	• **Acquisition:** survey of an area using optical and hyperspectral imagery • **Example Risk:** overflight of homes or individuals in public or private areas while optical sensors are active and/or recording. • **Example Mitigations:** ○ Activate optical sensors only when over target area (measured by GPS mapping). ○ Apply narrow framing of optical imagery to reduce risk of secondary capture. ○ Select optical sensor with appropriate resolution to reduce risk of unnecessary capture of high definition video imagery in which people could be identifiable
Waste Water Discharge Monitoring	Use of drone mounted sensors and associated analytics technologies to identify, map, and measure, the discharge of waste water into the environment.	• **Acquisition:** Drone survey of an area using optical, multi-spectrum or thermal imagery • **Example Risk:** overflight of homes or individuals in public or private areas while optical sensors are active and/or recording. • **Example Mitigations:** ○ Activate optical sensors only when over target area (defined by GPS and/or geofencing). ○ Apply narrow framing of optical imagery to reduce risk of secondary capture. ○ Select optical sensor with appropriate resolution to reduce risk of unnecessary capture of high definition video imagery in which people could be identifiable

Taxonomy Level 3	Definition	Example Acquisition and Analysis Approach
Waste Management Monitoring	Use of drone mounted sensors and associated analytics technologies to identify, map, and measure, the operation of approved waste disposal locations. This could include the use of gas sensors to measure emission of methane or other gases.	• **Acquisition:** Drone survey of an area using optical, multi-spectrum imagery or gas sensors • **Example Risk:** Risk of secondary capture of individuals visiting or working at the waste management facility. • **Example Mitigations:** ○ Activate optical sensors only when over target area (defined by GPS and/or geofencing). ○ Apply narrow framing of optical imagery to reduce risk of secondary capture. ○ Restrict access to areas that are subject to drone flight. ○ Select optical sensor with appropriate resolution to reduce risk of unnecessary capture of high definition video imagery in which people could be identifiable.
Air Quality Monitoring	Use of drone mounted sensors and associated analytics technologies to gather statistical data on air quality in an area.	• **Acquisition:** Survey of air quality in an area using drone-mounted pollution sensors • **Example Risk:** Use of optical sensors on drone for flight/navigation may capture imagery of homes/private areas or individuals in public or private areas • **Example Mitigations:** ○ Activate optical sensors only when over target area (defined by GPS and/or geofencing). ○ Apply narrow framing of optical imagery to reduce risk of secondary capture. ○ Select optical sensor with appropriate resolution to reduce risk of unnecessary capture of high definition video imagery in which people could be identifiable
Noise Pollution Monitoring	Use of drone mounted sensors and associated analytics technologies to gather statistical data on noise pollution and ambient noise levels in an area.	• **Acquisition** Survey of air quality in an area using drone-mounted microphones and audiometry sensors • **Example Risk:** Use of optical sensors on drone for flight/navigation may capture imagery of homes/private areas or individuals in public or private areas; Retention of recordings may include personal data (secondary obtaining) • **Example Mitigations:** ○ Activate optical sensors only when over target area (defined by GPS and/or geofencing). ○ Apply narrow framing of optical imagery to reduce risk of secondary capture. ○ Select optical sensor with appropriate resolution to reduce risk of unnecessary capture of high definition video imagery in which people could be identifiable ○ Retain only metric data calculated on-device not raw recordings.

Built Environment Monitoring

Taxonomy Level 3	Definition	Example Acquisition and Analysis Approach
Building Safety Monitoring	Use of drones to survey buildings, particularly areas that are inaccessible or difficult to access without other safety equipment, to assess risks to public from defects or damage	• **Acquisition:** Survey of building using optical sensors (cameras) to capture high definition images of features or defects. Might also include use of gas sensors to detect emissions or toxic gases. Imagery/sensor data would usually be recorded for inspection or to be shared with other stakeholders involved in remediation. • **Example Risk:** High definition optical sensors increases risk that individuals will be identifiable in recordings. Recordings may capture imagery of homes/private areas or of individuals in public or private areas. Retained recordings may contain personal data. • **Example Mitigation**: ○ Activate high definition cameras only in the area where inspection is taking place and for the duration of the recording ○ Advise public / residents in advance of the use of drones for recording ○ Only retain recordings if required to support planning and execution of remedial works or if more detailed inspection of footage is required.
Preventative Maintenance Planning & Monitoring	Use of drones to survey buildings or other built environment, particularly areas that are inaccessible or difficult to access without other safety equipment, to assess, identify, and prioritise requirements for preventative maintenance	• **Acquisition:** Survey of building using optical sensors (cameras) to capture high definition images of features or defects. Might also include use of gas sensors to detect emissions or toxic gases. Imagery/sensor data would usually be recorded for inspection or to be shared with other stakeholders involved in remediation. • **Example Risk:** High definition optical sensors increases risk that individuals will be identifiable in recordings. Recordings may capture imagery of homes/private areas or of individuals in public or private areas. Retained recordings may contain personal data. • **Example Mitigation**: ○ Activate high definition cameras only in the area where inspection is taking place and for the duration of the recording ○ Advise public / residents in advance of the use of drones for recording ○ Only retain recordings if required to support planning and execution of remedial works or if more detailed inspection of footage is required.

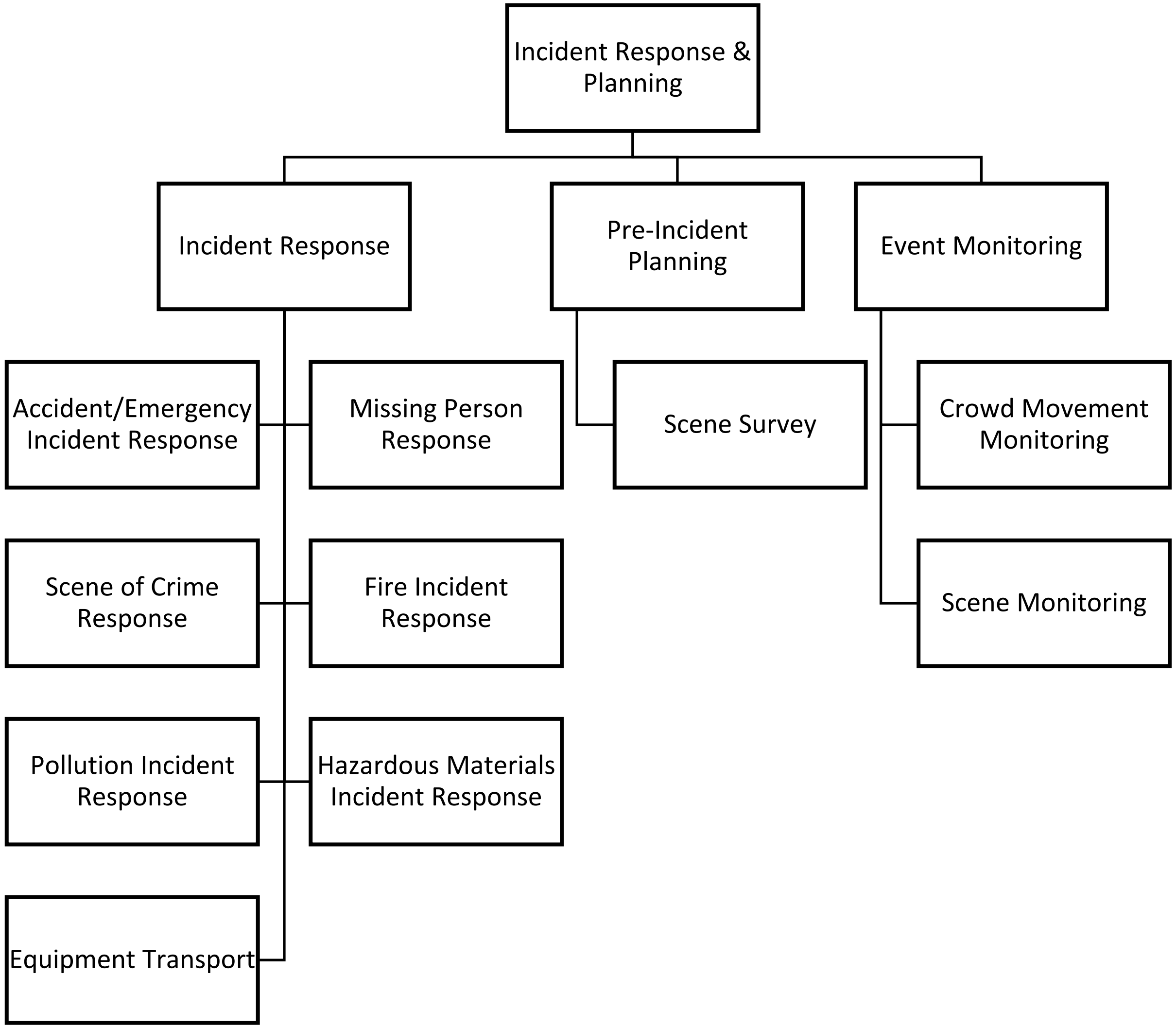
Taxonomy Level 3	Definition	Example Acquisition and Analysis Approach
Energy Efficiency Measurement & Monitoring	Use of drones to survey buildings or other built environment, particularly areas that are inaccessible or difficult to access without other safety equipment, to assess, identify, and prioritise requirements for preventative maintenance	• **Acquisition:** Survey of building using optical sensors (cameras) to capture high definition images of features or defects. Might also include use of gas sensors to detect emissions or toxic gases. Imagery/sensor data would usually be recorded for inspection or to be shared with other stakeholders involved in remediation. • **Example Risk:** High definition optical sensors increases risk that individuals will be identifiable in recordings. Recordings may capture imagery of homes/private areas or of individuals in public or private areas. Retained recordings may contain personal data. • **Example Mitigation**: ○ Activate high definition cameras only in the area where inspection is taking place and for the duration of the recording ○ Advise public / residents in advance of the use of drones for recording ○ Only retain recordings if required to support planning and execution of remedial works or if more detailed inspection of footage is required.
Hazardous Material Storage Monitoring	Use of drones to survey buildings or other built environment, particularly areas that are inaccessible or difficult to access without other safety equipment, to identify any risks associated with the storage of hazardous or potentially hazardous materials.	• **Acquisition:** Survey of locations using optical sensors (cameras) to capture high definition images of areas where hazardous or potentially hazardous materials are stored. Might also include use of gas sensors to detect emissions or toxic gases or LIDAR mapping of areas obscured by foliage. Imagery/sensor data would usually be recorded for inspection or to be shared with other stakeholders involved in remedial action. • **Example Risk:** High definition optical sensors increases risk that individuals will be identifiable in recordings. Recordings may capture imagery of homes/private areas or of individuals in public or private areas. Retained recordings may contain personal data. • **Example Mitigation**: ○ Activate high definition cameras only in the area where inspection is taking place and for the duration of the recording ○ Advise public / residents in advance of the use of drones for recording ○ Only retain recordings if required to support planning and execution of remedial works, investigation of suspected criminal offences, or if more detailed inspection of footage is required.

Population Movement Measurement

Taxonomy Level 3	Definition	Example Acquisition and Analysis Approach
Traffic Flow Measurement	Use of drones to survey traffic flow for defined short periods (statistical sampling)	• **Acquisition:** Capture of optical image data of vehicles to be analysed off-line using machine learning technologies or human inspection to generate statistical analysis of traffic flow. • **Example Risk:** Optical sensor may capture images of that individuals who will be identifiable in recordings. Recordings may capture imagery of homes/private areas or of individuals in public or private areas. Retained recordings may contain personal data. • **Example Mitigation**: ○ Activate cameras only in the area where inspection is taking place and for the duration of the recording ○ Frame the recording to reduce risk of recording footage of private homes or private areas ○ Advise public / residents in advance of the use of drones for recording ○ Only retain recordings if required to support planning and execution of remedial works or if more detailed inspection of footage is required. ○ Limit access to recorded data. Retain for no longer than necessary to create
People Movement Measurement	Use of drones to survey pedestrian movements for defined short periods (statistical sampling)	• **Acquisition:** Capture of optical image data of vehicles to be analysed off-line using machine learning technologies or human inspection to generate statistical analysis of traffic flow. • **Example Risk:** High definition optical sensors (if used) increases risk that individuals will be identifiable in recordings. Recordings may capture imagery of homes/private areas or of individuals in public or private areas. Retained recordings will contain personal data. Definition of personal data is broad. • **Example Mitigation**: ○ Activate high definition cameras only in the area where inspection is taking place and for the duration of the recording ○ Avoid use of technologies such as APNR unless a clear statutory justification is identified ○ Advise public / residents in advance of the use of drones for recording ○ Only retain recordings if required to support planning and execution of remedial works or if more detailed inspection of footage is required.

Taxonomy Level 3	Definition	Example Acquisition and Analysis Approach
Surveying and Mapping	Use of drone mounted sensors and associated technologies to survey and map features of the natural or built environment for the purposes of producing geospatial and navigation data sets	• **Acquisition:** Capture of optical image data of landscape and landscape features • **Example Risk:** High definition optical sensors (if used) increases risk that individuals will be identifiable in recordings. Recordings may capture imagery of homes/private areas or of individuals in public or private areas. Retained recordings will contain personal data. Definition of personal data is broad. • **Example Mitigation**: ○ Activate high definition cameras only in the area where inspection is taking place and for the duration of the recording ○ Operate drone at an altitude which reduces the risk of individuals being identifiable from any recorded image or video. ○ Consider use of alternate technology such as LiDar to carry out mapping and surveying to reduce risk of secondary capture of identifiable data.

Incident Response and Planning



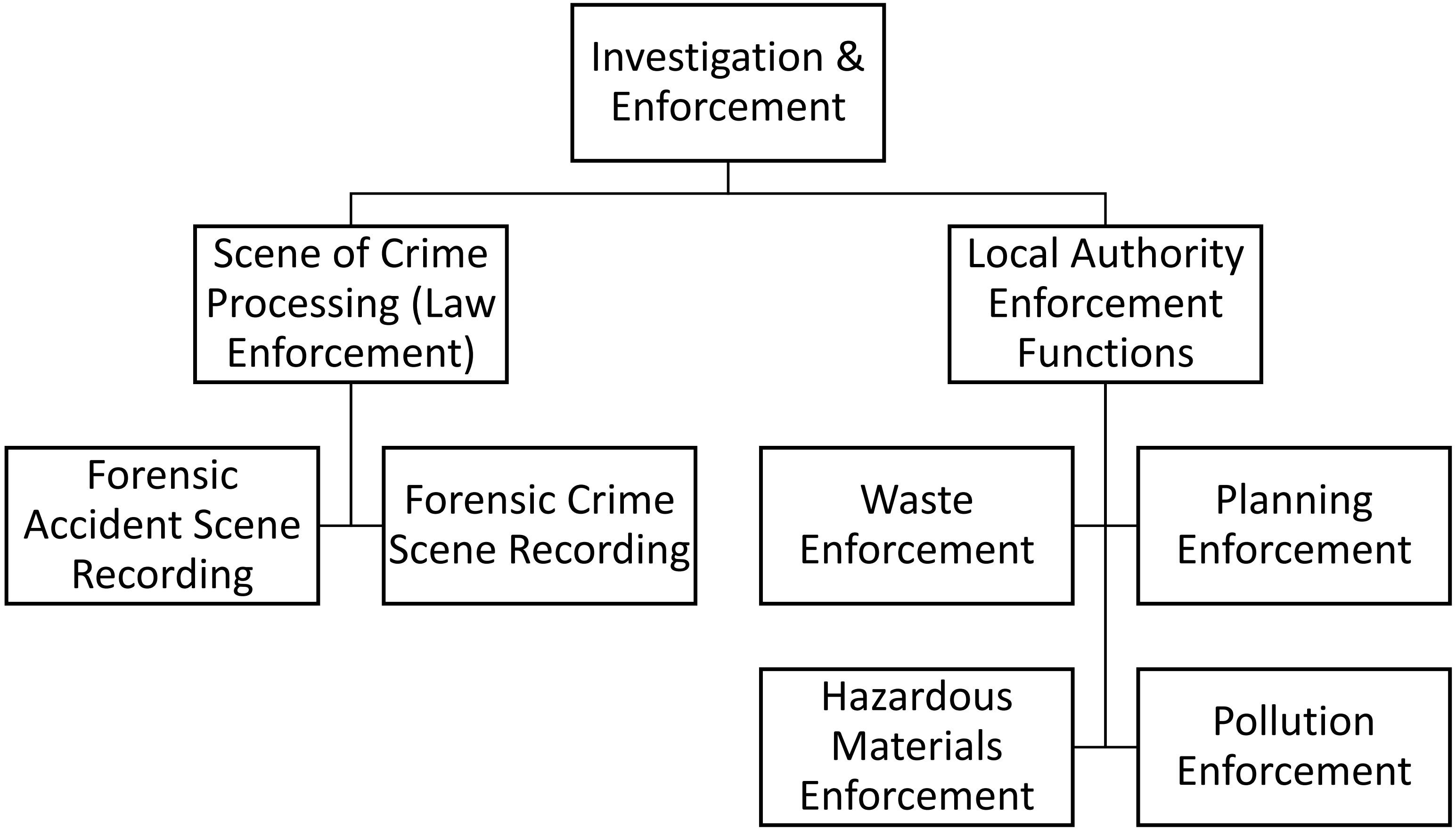
Taxonomy Level 3	Definition	Example Acquisition and Analysis Approach
Accident/Emergency Response	Use of drones to assess scene of an accident or emergency incidents to provide information on the incident and associated risks.	• **Acquisition:** ○ Survey of an incident location using high definition optical / thermal/ gas sensors to provide real-time overview of scale of incident and provide advance warning of risk factors or identify blocked roads etc. ○ Record incident response for post-incident review and training purposes ○ Use of LiDar or similar technologies for rapid mapping of incident area. • **Example Risk:** High definition video recording will capture identifiable people. Imagery may include data relating to health if injured persons are captured. • **Example Mitigation**: ○ Activate HD cameras only where necessary to provide operational information for incident response ○ Ensure drone device is visible and identifiable as an emergency service asset. ○ Ensure appropriate controls over storage and use of recordings for secondary purposes such as training and response planning. ○ Ensure appropriate controls to restrict disclosure/publication of recorded video to 3rd parties.
Missing Person Response	Use of drones to assist in the search for missing persons	• **Acquisition:** ○ Survey of an incident location using high definition optical / thermal/ audio sensors/ LiDAR mapping ○ Record incident response for post-incident review and training purposes. • **Example Risk:** High definition video recording will capture identifiable people. Imagery may include data relating to health if injured persons are captured. • **Example Mitigation**: ○ Activate HD cameras only where necessary to provide operational information for incident response ○ Ensure drone device is visible and identifiable as an emergency service asset. ○ Ensure appropriate controls over storage and use of recordings for secondary purposes such as training and response planning. ○ Ensure appropriate controls to restrict disclosure/publication of recorded video to 3rd parties.

Taxonomy Level 3	Definition	Example Acquisition and Analysis Approach
Pollution Incident Response	Use of drones to assist in the execution of response to a pollution incident	• **Acquisition:** ○ Survey of an incident location using high definition optical / thermal/multi-spectrum imagery ○ Record incident response for post-incident review and training purposes ○ Use of LiDar or similar technologies for rapid mapping of incident area. • **Example Risk:** High definition video recording will capture identifiable people. Imagery may include data relating to health if injured persons are captured. • **Example Mitigation**: ○ Activate HD cameras only where necessary to provide operational information for incident response ○ Ensure drone device is visible and identifiable as an emergency service asset. ○ Ensure appropriate controls over storage and use of recordings for secondary purposes such as training and response planning. ○ Ensure appropriate controls to restrict disclosure/publication of recorded video to 3rd parties.
Fire Incident Response	Use of drones to assess scene of an fire safety incidents to provide information on the incident and associated risks.	• **Acquisition:** ○ Survey of an incident location using high definition optical / thermal/multi-spectrum imagery to provide real-time information to responders. ○ Record incident response for post-incident review and training purposes ○ Use of LiDar or similar technologies for rapid mapping of incident area. • **Example Risk:** High definition video recording will capture identifiable people. Imagery may include data relating to health if injured persons are captured. • **Example Mitigation**: ○ Activate HD cameras only where necessary to provide operational information for incident response ○ Ensure drone device is visible and identifiable as an emergency service asset. ○ Ensure appropriate controls over storage and use of recordings for secondary purposes such as training and response planning. ○ Ensure appropriate controls to restrict disclosure/publication of recorded video to 3rd parties.

Taxonomy Level 3	Definition	Example Acquisition and Analysis Approach
Hazardous Materials Incident Response	Use of drones to assess scene of emergency incident where there is a known or potential Hazardous materials risk to provide information on the incident and associated risks.	• **Acquisition:** ○ Survey of an incident location using high definition optical / thermal/multi-spectrum imagery to provide real-time information to responders. ○ Record incident response for post-incident review and training purposes ○ Use of LiDar or similar technologies for rapid mapping of incident area. • **Example Risk:** High definition video recording will capture identifiable people. Imagery may include data relating to health if injured persons are captured. • **Example Mitigation**: ○ Activate HD cameras only where necessary to provide operational information for incident response ○ Ensure drone device is visible and identifiable as an emergency service asset. ○ Ensure appropriate controls over storage and use of recordings for secondary purposes such as training and response planning. ○ Ensure appropriate controls to restrict disclosure/publication of recorded video to 3rd parties.
Pre-Incident Planning (Scene Survey)	Use of drones to survey a location in advance of an event or as part of a risk assessment and mitigation planning for a location.	• **Acquisition:** ○ Survey of an incident location using optical / thermal/multi-spectrum imagery/LiDAR to support risk assessment and planning ○ Record imagery for off-site analysis • **Example Risk:** Drone may overfly private homes or other private spaces. Cameras may capture individuals in public or private locations • **Example Mitigation**: ○ Activate Cameras only where necessary to carry out the survey activity ○ Consider necessity of resolution of imagery for the planning purpose ○ Ensure drone device is visible and identifiable as an emergency service asset. ○ Ensure appropriate controls over storage and use of recordings for secondary purposes such as training and response planning. ○ Ensure appropriate controls to restrict disclosure/publication of recorded video to 3rd parties.
Event Monitoring	Use of drones to monitor crowd movements at events to provide	• **Acquisition:**

Taxonomy Level 3	Definition	Example Acquisition and Analysis Approach
	feedback to event security and support personnel	○ Survey of an event location using optical sensors and audio sensors to provide real-time information to event staff. ○ Record imagery for off-site analysis • **Example Risk:** High definition video recording will capture identifiable people. Imagery may include data relating to health if injured persons are captured. Audio sensors • **Example Mitigation**: ○ Cameras only where necessary to carry out the survey activity ○ Consider necessity of resolution of imagery for the planning purpose ○ Ensure drone device is visible and identifiable as an emergency service asset. ○ Ensure appropriate controls over storage and use of recordings for secondary purposes such as training and response planning. ○ Ensure appropriate controls to restrict disclosure/publication of recorded video to 3rd parties.
Equipment Transport	Use of drones at incidents or events to transport equipment to inaccessible or hazardous areas	• **Acquisition:** ○ Use of GPS and drone mounted sensors to support piloting of drone to required location. ○ Record imagery for off-site analysis, incident response review, training. • **Example Risk:** High definition video recording will capture identifiable people. Imagery may include data relating to health if injured persons are captured. Audio sensors • **Example Mitigation**: ○ Cameras only where necessary to carry out the transport activity ○ Consider necessity of resolution of imagery for the transport purpose ○ Ensure drone device is visible and identifiable as an emergency service asset. ○ Ensure appropriate controls over storage and use of recordings for secondary purposes such as training and response planning. ○ Ensure appropriate controls to restrict disclosure/publication of recorded video to 3rd parties.

Investigation and Enforcement

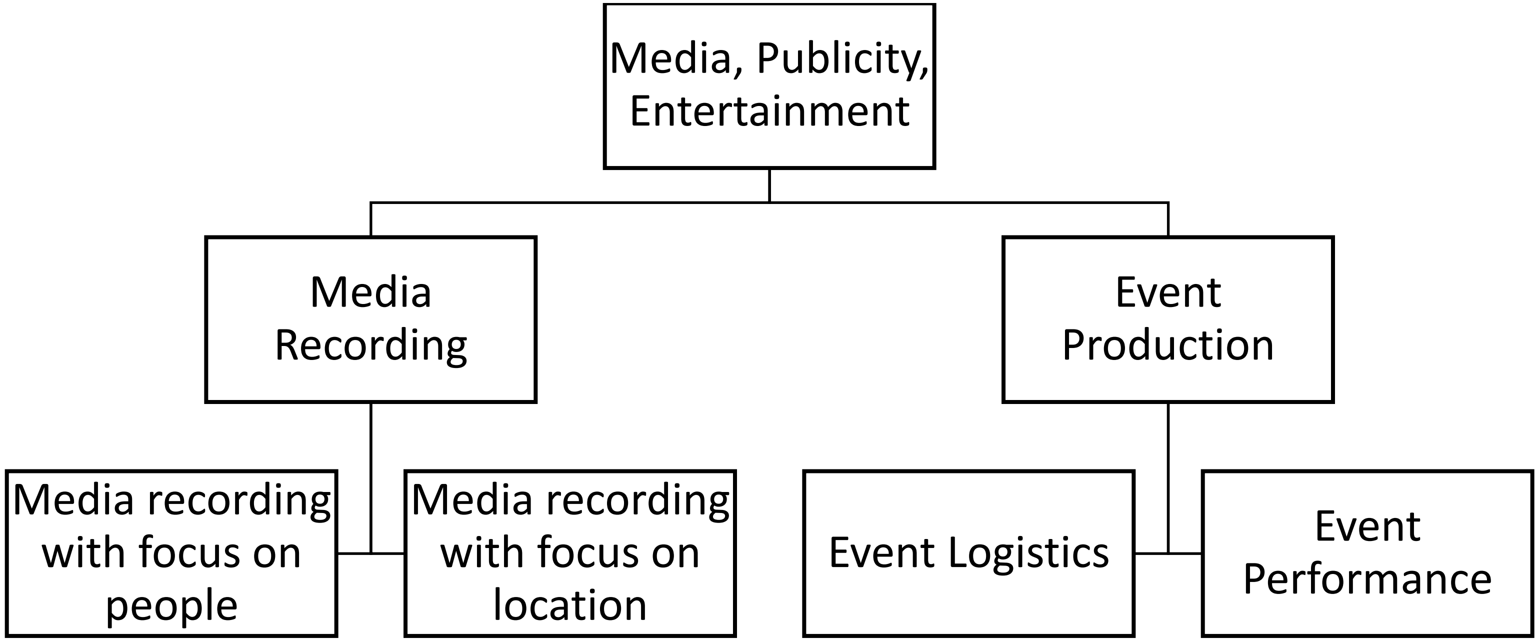

Investigation & Enforcement
Scene of Crime Processing (Law Enforcement)
Local Authority Enforcement Functions
Forensic Accident Scene Recording
Forensic Crime Scene Recording
Waste Enforcement
Planning Enforcement
Hazardous Materials Enforcement
Pollution Enforcement

Taxonomy Level 3	Definition	Example Acquisition and Analysis Approach
Forensic Accident Scene Recording [Note: processing may be covered by Part 5 of Data Protection Act 2018]	Use of drones to conduct survey of an accident scene to support investigation process	• **Acquisition:** ○ Survey of accident area using high definition video / thermal imagery or other sensors ○ Use of LiDAR or similar technologies for rapid mapping of incident area. ○ Analyse data off-site to support accident investigation and potential criminal prosecution. • **Example Risk:** High definition video recording may capture identifiable people. Drone may overfly private homes or other private areas. There is a risk of secondary capture of personal data of bystanders if they are recorded. • **Example Mitigation**: ○ Activate HD cameras only where necessary to record the accident location and scene. ○ Ensure drone device is visible and identifiable as an emergency service asset when active ○ Ensure appropriate controls over storage and use of recordings for secondary purposes such as training and response planning. ○ Ensure appropriate controls to restrict disclosure/publication of recorded video to 3rd parties.
Forensic Crime Scene Reporting [Processing is covered by Part 5 of Data Protection Act 2018]	Use of drones to conduct survey of an a known crime scene to support investigation process	• **Acquisition:** ○ Survey of accident area using high definition video / thermal imagery or other sensors ○ Use of LiDAR or similar technologies for rapid mapping of incident area. ○ Analyse data off-site to support accident investigation and potential criminal prosecution. • **Example Risk:** High definition video recording may capture identifiable people. Drone may overfly private homes or other private areas. There is a risk of secondary capture of personal data of bystanders if they are recorded. • **Example Mitigation**: ○ Activate HD cameras only where necessary to record the accident location and scene. ○ Ensure drone device is visible and identifiable as an emergency service asset when active ○ Ensure appropriate controls over storage and use of recordings for secondary purposes such as training and response planning. ○ Ensure appropriate controls to restrict disclosure/publication of recorded video to 3rd parties.
Waste Management Enforcement	The use of drone mounted sensors to carry out inspections of authorised and unauthorised waste management facilities	• **Acquisition:** ○ Survey of accident area using high definition video / thermal imagery or other sensors ○ Use of LiDAR or similar technologies for rapid mapping of incident area. ○ Analyse data off-site to support investigation and any further search or response, and potential criminal prosecution.

Taxonomy Level 3	Definition	Example Acquisition and Analysis Approach
	and to gather evidence of any legislative or regulatory breaches.	• **Example Risk:** High definition video recording may capture identifiable people. Drone may overfly private homes or other private areas. There is a risk of secondary capture of personal data of bystanders if they are recorded. • **Example Mitigation**: ○ Activate HD cameras only where necessary to record the inspection location. ○ Ensure drone device is visible and identifiable as being operated by the local authority asset when active ○ Ensure appropriate controls over storage and use of recordings for secondary purposes such as training. ○ Ensure appropriate controls to restrict disclosure/publication of recorded video to 3rd parties.
Planning Enforcement	The use of drone mounted sensors to carry out inspections of any building or development to assess compliance with planning permissions and gather evidence of any legislative or regulatory breaches.	• **Acquisition:** ○ Survey of accident area using high definition video / thermal imagery or other sensors ○ Use of LiDAR or similar technologies for rapid mapping of incident area. ○ Analyse data off-site to support investigation and any further search or response, and potential criminal prosecution. • **Example Risk:** High definition video recording may capture identifiable people. Drone may overfly private homes or other private areas. There is a risk of secondary capture of personal data of bystanders if they are recorded. • **Example Mitigation**: ○ Activate HD cameras only where necessary to record the inspection location. ○ Ensure drone device is visible and identifiable as being operated by the local authority when active ○ Ensure appropriate controls over storage and use of recordings for secondary purposes such as training. ○ Ensure appropriate controls to restrict disclosure/publication of recorded video to 3rd parties.
Pollution Enforcement	The use of drone mounted sensors to gather evidence to support prosecutions for pollution offences.	• **Acquisition:** ○ Survey of accident area using high definition video / thermal imagery or other sensors ○ Use of LiDAR or similar technologies for rapid mapping of incident area. ○ Analyse data off-site to support accident investigation and potential criminal prosecution.

Taxonomy Level 3	Definition	Example Acquisition and Analysis Approach
		• **Example Risk:** High definition video recording may capture identifiable people. Drone may overfly private homes or other private areas. There is a risk of secondary capture of personal data of bystanders if they are recorded. • **Example Mitigation**: ○ Activate HD cameras only where necessary to record the inspection location. ○ Ensure drone device is visible and identifiable as being operated by the local authority when active ○ Ensure appropriate controls over storage and use of recordings for secondary purposes such as training ○ Ensure appropriate controls to restrict disclosure/publication of recorded video to 3rd parties.
Hazardous Materials Storage Enforcement	The use of drone mounted sensors to gather evidence to support the detection of and removal of materials and the execution of any criminal or administrative sanctions.	• **Acquisition:** ○ Survey of accident area using high definition video / thermal imagery or other sensors ○ Use of LiDAR or similar technologies for rapid mapping of incident area. ○ Analyse data off-site to support accident investigation and potential criminal prosecution. • **Example Risk:** High definition video recording may capture identifiable people. Drone may overfly private homes or other private areas. There is a risk of secondary capture of personal data of bystanders if they are recorded. • **Example Mitigation**: ○ Activate HD cameras only where necessary to record the inspection location. ○ Ensure drone device is visible and identifiable as being operated by the local authority when active ○ Ensure appropriate controls over storage and use of recordings for secondary purposes such as training ○ Ensure appropriate controls to restrict disclosure/publication of recorded video to 3rd parties.

Media, Publicity, and Entertainment


Media, Publicity, Entertainment
Media Recording
Event Production
Media recording with focus on people
Media recording with focus on location
Event Logistics
Event Performance

Taxonomy Level 3	Definition	Example Acquisition and Analysis Approach
Media Recording with focus on people	Use of drones to capture video, still images or footage of events or activities where the focus of the recording is an individual or a group of individuals with the intention of publication.	• **Acquisition:** ○ Use of optical or audio sensors to record video, still images, or other audio visual information. • **Example Risk:** High definition video recording may capture identifiable people. Drone may overfly private homes or other private areas. There is a risk of secondary capture of personal data of bystanders if they are recorded. • **Example Mitigation**: ○ Activate HD cameras only where necessary to record the people at the location and scene. ○ Ensure that people are aware that there will be recording taking place and ensure that individuals have the ability to "opt-out" by being able to avoid the flight path of the drone. ○ Ensure appropriate controls over storage and use of recordings for secondary purposes. ○ Ensure appropriate controls to restrict disclosure/publication of recorded video to 3rd parties.
Media Recording with focus on location	Use of drones to capture video, still images or footage of events or activities where the focus of the recording is an individual or a group of individuals with the intention of publication.	• **Acquisition:** ○ Use of optical or audio sensors to record video, still images, or other audio visual information. • **Example Risk:** Flight path of drone may overlook private homes or other private areas. There may be secondary capture of identifiable data subjects • **Example Mitigation**: ○ Plan flight plan for recording to avoid private homes where possible ○ Activate HD cameras only where necessary to record the accident location and scene. ○ Ensure that people are aware that there will be recording taking place and ensure that individuals have the ability to "opt-out" by being able to avoid the flight path of the drone. ○ Edit footage to remove secondary capture of people ○ Ensure appropriate controls over storage and use of recordings for secondary purposes. ○ Ensure appropriate controls to restrict disclosure/publication of recorded video to 3rd parties.
Event Logistics	Use of drones to provide logistics/transport support for the	• **Acquisition:** ○ Use of GPS and drone mounted sensors to support piloting of drone to required location. ○ Record imagery for off-site analysis, incident response review, training.

Taxonomy Level 3	Definition	Example Acquisition and Analysis Approach
	execution of an event or publicity activity.	• **Example Risk:** Video sensors will capture identifiable people or may capture footage of private homes or private locations. • **Example Mitigation**: ○ Cameras only where necessary to carry out the transport activity ○ Cameras should not be flown over private homes while recording ○ Consider necessity of resolution of imagery for the transport purpose ○ Consider the necessity of recording/retaining imagery from the specific drone (may be required for insurance or other purposes) ○ Ensure appropriate controls over storage and use of recordings for secondary purposes such as training and response planning. ○ Ensure appropriate controls to restrict disclosure/publication of recorded video to 3rd parties.
Event Performance	Use of drones to carry out a planned flight path as part of the execution of a performance activity.	• **Acquisition:** ○ Use of GPS and drone mounted sensors to support piloting of drones in a defined flight path to execute a performance event. ○ Record imagery for off-site analysis, incident response review, training. • **Example Risk:** High definition video recording will capture identifiable people. Imagery may include data relating to health if injured persons are captured. Audio sensors • **Example Mitigation**: ○ Cameras only where necessary to carry out the transport activity ○ Cameras should not be flown over private homes while recording ○ Consider necessity of resolution of imagery for the performance purpose ○ Consider the necessity of recording/retaining footage from the specific drone (may be required for insurance or other purposes) ○ Ensure appropriate controls over storage and use of recordings for secondary purposes such as training and response planning. ○ Ensure appropriate controls to restrict disclosure/publication of recorded video to 3rd parties.

This handbook was developed as part of the Dublin City Council 'Accelerating the Potential of Drones for Local Government' Project, supported by the Department of Public Expenditure and Reform's Public Sector Innovation Fund 2021.

Project Partners are:

Comhairle Cathrach
Bhaile Átha Cliath
Dublin City Council

Our Public Service

SMART DUBLIN

LGMA
An Ghníomhaireacht Bainistíochta Rialtais Áitiúil
Local Government Management Agency

Maynooth University
National University of Ireland Maynooth

This material is based upon works supported by U-Flyte (Unmanned Aircraft Systems Flight Research) 17/SPP/3460 which is funded under the Science Foundation Ireland Strategic Partnership Programme and based in Maynooth University