DENTONS

Drone laws around the world

A comparative global guide to drone regulatory laws

Second Edition, 2023

Grow | Protect | Operate | Finance

Contents

Overview

Drones are a disruptive technology that accelerate new approaches and opportunities in a variety of industries. Great strides have been made toward regulating autonomous and beyond the visual line of sight operations of drones. This new frontier of disruptive technology has generated many ingenious new solutions to old problems and promises more for those willing to embrace the technology.

Now expanded to include 17 different regions, this second edition of **Dentons' Drone laws around the world: a comparative global guide to drone regulatory laws** provides detailed accounts and analysis of regulations that impact operations around the globe. This second edition of the Guide includes analysis and comparison of the regulations, sanctions and liability, privacy and future regulatory and innovative developments for the following regions:

- Australia
- Canada
- EU
- EU Member states:
  - Denmark
  - France
  - Germany
  - Italy
  - Luxembourg
  - Netherlands
  - Romania
  - Spain
- Japan
- Korea
- New Zealand
- Singapore
- United Kingdom
- United States of America

Commercial applications of drones demonstrate the ingenuity of those engaged in this burgeoning sector. This Guide explores applications in the real estate, oil and gas and counter-drone / security industries, discussing some key risks and identifying opportunities for those considering using drones in their non-aviation operations.

The Aviation and Aerospace team at Dentons provides practical, proactive business-focused advice to all participants in the drone industry, including those in non-aviation fields. Harnessing the largest global platform to provide seamless legal advice to our clients, our multi-disciplinary team possesses the local knowledge and specialized expertise to navigate this complex regulatory environment.

Why have we changed the terminology for this Guide from "remotely piloted aircraft systems", or "RPAs" to "drones"?

Despite a lack of uniformity of terms in regulations around the world, most people commonly use the term "drone" to refer to autonomous, uncrewed, aerial vehicles. For consistency in this Guide, we have used the term "drone" to promote accessibility. We expect that as regulations and international conventions continue to evolve, a common term will eventually cement itself in this industry.

List of Abbreviations

Abbreviation	Definition
AGL	Above Ground Level
BVLOS	Beyond Visual Line of Sight
DAA	Detect-and-avoid
EASA	European Aviation Safety Agency
EVLOS	Extended Visual Line of Sight
FAA	Federal Aviation Authority
IATA	International Air Transport Association
ICAO	International Civil Aviation Organization
JARUS	Joint Authorities for Rulemaking on Unmanned Systems
LAANC	Low Altitude Authorization and Notice Capability
RPA	Remotely Piloted Aircraft
RPAS	Remotely Piloted Aircraft Systems
RTM	Remote Traffic Management
SORA	Specific Operations Risk Assessment
VLOS	Visual Line of Sight

Australia

Overview

Drones are regulated in Australia at the federal level of government by the Civil Aviation Safety Authority (CASA) in accordance with the *Civil Aviation Act 1988 (Cth)*. CASA is Australia's national aviation regulatory body and was established as an independent statutory authority in July 1995.

The *Civil Aviation Act 1988 (Cth)* was passed along with an ancillary set of regulations, the *Civil Aviation Safety Regulations 1998 (Cth)*. Together, they form the legislative framework that regulates the operation of drones in Australia.

The legislative framework distinguishes drones into two distinct major flight purposes:

- Drones that are flown for commercial or business reasons; and
- Drones that are flown for sport or recreation.

Registration is mandatory for drones that are flown for commercial or business reasons, and their operator must be accredited with CASA.

CASA considers that anything other than sport or recreation constitutes a commercial or business reason for flying a drone. Therefore, if a drone is to be flown for professional activities such as research, training, community and government services, or any work undertaken on behalf of one's employer, the drone must be registered and its operator must be accredited with CASA.

Since the establishment of a registration system in September 2020, more than 22,000 drones have been registered with CASA and over 13,000 operator accreditations have been issued. By way of comparison, CASA records indicate that Australia has 15,771 registered aircraft.[1]

The laws and regulations that regulate drones in Australia are largely distinguished between the two major flight purposes (commercial or business reasons and sport or recreation). They do not distinguish based on the risks associated with the flight of the drone.

CASA's regulations extend to both the pilot (the person manipulating the flight controls of the drone) and the operator (the person, organization or enterprise engaged in, or offering to engage in, an aircraft operation).

VLOS and BVLOS regulations

Government agencies with jurisdiction over drones	Region this agency covers. (e.g., entire jurisdiction or province/ state)	Role of the agency
Civil Aviation Safety Authority (CASA)[2]	Entire jurisdiction of Australia	CASA is a government body that regulates Australian aviation safety and the operation of Australian aircraft overseas. CASA employs about 800 people working across Australia. CASA licenses pilots, registers aircraft, oversees aviation safety and promotes safety awareness. CASA is also responsible for making sure that Australian airspace is administered and used safely.[3]

CASA's regulations classify drones according to size and extend to both the pilot and the operator of the drone.[4]

The categories of size are:

Size	Weight
Micro	Less than 250 g
Very Small	250 g to 2 kg
Small	2 to 25 kg
Medium	25 to 150 kg
Large	Greater than 150 kg

1 https://updates.communication.casa.gov.au/link/id/zzzz603ed9f383dc0116/page.html.

2 *Sections 8 and 9 of the* Civil Aviation Act 1988 (Cth).

3 https://www.casa.gov.au/about-us/who-we-are.

4 Regulation 101.022 of the *Civil Aviation Safety Regulations 1998 (Cth)*.

CASA's regulations impose Standard Operating Conditions on pilots and operators.[5] Some important aspects of the Standard Operating Conditions include:

- The drone must be operated during daytime and by the visual line of sight only;
- The maximum operating height for a drone is 120 m (400 ft) above ground level in controlled airspace or outside a CASA-approved area. These restrictions are subject to any permission that has been given by CASA to fly above this height;
- The drone must not be flown over any populous area, which is any area where the failure of the drone could cause injury to people or property not connected with the operation of the drone; and
- The drone must not be flown within 30 m of people. In certain circumstances, CASA's regulations will permit the drone to be flown within 15 m of people.[6]

Drones classified as micro or very small generally are entitled to certain exemptions from the Standard Operating Conditions.

There are certain circumstances where a drone operator can apply for flight authorization to fly outside of the Standard Operating Conditions. Such flight authorizations are available to pilots who:[7]

- Intend to fly the drone for commercial or business reasons; and
- Hold a remotely piloted aircraft operator's certificate.

Some of the flight authorization available include:

- Operating the drone BVLOS;[8]
- Operating the drone more than 120 m (400 ft) above ground level; and[9]
- Operating the drone within 3 nautical miles of controlled airspace.[10]

VLOS is defined in CASA's regulations as being where the person operating the drone can continually see, orientate and navigate the drone to meet the person's separation and collision avoidance responsibilities, with or without corrective lenses, but without the use of binoculars, a telescope or other similar device.[11]

In October 2021, new legislation commenced whose purpose is to incorporate drones into the incident reporting requirements that already exist for other forms of aircraft[12]:

- For drones classified as medium or large[13]:
  - If they are involved in an incident that involves death, serious injury or serious property damage, its pilot and operator must immediately report the incident to the Australian Transport Safety Bureau; and[14]
  - If they are involved in an incident that involves any procedure for overcoming an emergency or other occurrences that result in difficulty, its pilot and operator must report the incident to the Australian Transport Safety Bureau within 72 hours;[15]

5 Regulation 101.238 of the *Civil Aviation Safety Regulations 1998 (Cth)*.

6 Regulation 101.245 of the *Civil Aviation Safety Regulations 1998 (Cth)*.

7 Regulations 101.029, 101.030 and 101.080 of the *Civil Aviation Safety Regulations 1998 (Cth)*.

8 Regulation 101.029 of the *Civil Aviation Safety Regulations 1998 (Cth)*.

9 Regulation 101.030 of the *Civil Aviation Safety Regulations 1998 (Cth)*.

10 Regulation 101.030 of the *Civil Aviation Safety Regulations 1998 (Cth)*.

11 Regulation 101.073 of the *Civil Aviation Safety Regulations 1998 (Cth)*.

12 Transport Safety Investigation Act 2003 (Cth).

13 Regulation 6 of the Transport Safety Investigation Regulations 2021 (Cth).

14 Section 18 of the Transport Safety Investigation Act 2003 (Cth) and Regulation 11(1) of the Transport Safety Investigation Regulations 2021 (Cth).

15 Section 19 of the Transport Safety Investigation Act 2003 (Cth) and Regulation 12(1) of the Transport Safety Investigation Regulations 2021 (Cth).

- For drones classified as very small or small:[16]
  - If they are involved in an incident that involves death or serious injury, its pilot and operator must immediately report the incident to the Australian Transport Safety Bureau; and[17]
  - If they are involved in an incident that involves serious property damage, its pilot and operator must report the incident to the Australian Transport Safety Bureau within 72 hours.[18]

Liability

Criminal Liability

Non-compliance with specific regulations/laws

Failure to comply with CASA's regulations for drones generally constitutes strict liability criminal offences that attract penalties, which are measured by a certain number of penalty units. At the date of this report, one penalty unit is AU$222.[19]

Some of the strict liability offences include:

- Operating an unregistered drone or without an operator accreditation (or remote pilot licence) for commercial or business reasons – carrying a penalty of up to 50 penalty units (approximately AU$11,100);[20]
- Failure to operate a drone over a populous area at a height less than the height from which, if any of its components fails, it would be able to clear the area – carrying a penalty of up to 50 penalty units (approximately AU$11,100);[21]
- Failure to operate a drone within the operator's visual line of sight – carrying a penalty of up to 50 penalty units (approximately AU$11,100); and[22]
- Operating a drone in or over a prohibited area, or in or over a restricted area, without the permission of, or not in accordance with any conditions imposed by, the authority controlling the area – carrying a penalty of up to 25 penalty units (approximately AU$5,550).[23]

Civil Liability

Drone operators should be aware of the risk of breaching confidence if images are surreptitiously obtained. This tort is considered the closest form of protection that Australia has to a common law right protecting our privacy. The traditional formulation of the cause of action for breach of confidence has three elements:

1. The information must have the necessary quality of confidence;
2. The information must be communicated in circumstances importing an obligation of confidence; and
3. There must be an unauthorized use of that information to the detriment of the communicator.

The first limb has been broadened in recent times to include the protection of personal identities and domestic activities.[24]

Drone operators should also be aware that they may risk trespassing on private property if the altitude of the drone intrudes the airspace necessary for the occupier's ordinary use and enjoyment of the land.[25]

16 Regulation 6 of the Transport Safety Investigation Regulations 2021 (Cth).

17 Section 18 of the Transport Safety Investigation Act 2003 (Cth) and Regulation 11(3) of the Transport Safety Investigation Regulations 2021 (Cth).

18 Section 19 of the Transport Safety Investigation Act 2003 (Cth) and Regulation 12(3) of the Transport Safety Investigation Regulations 2021 (Cth).

19 Section 4AA of the *Crimes Act 1914* (Cth).

20 Regulation 101.252 of the *Civil Aviation Safety Regulations 1998 (Cth).*

21 Regulation 101.280 of the *Civil Aviation Safety Regulations 1998 (Cth).*

22 Regulation 101.073 of the *Civil Aviation Safety Regulations 1998 (Cth).*

23 Regulation 101.065 of the *Civil Aviation Safety Regulations 1998 (Cth).*

24 See, for example, *Australian Football League v The Age Co Ltd* (2006) 15 VR 419.

25 See, for example, *JP Investments Pty Ltd v Howard Chia Investments Pty Ltd* (1989) 24 NSWLR 490, 495-6.

Furthermore, where the drone substantially and unreasonably interferes with rights in relation to or in connection with the use of the land of a particular individual, a complainant may be able to make out a breach of the tort of nuisance.[26] Generally, a complainant must make out multiple infractions for a breach to occur[27].

Data privacy and security

Private organizations with a turnover of more than AU$3 million annually and certain government agencies must comply with the *Privacy Act 1988* (Cth) and the Australian Privacy Principles which impose certain rules in relation to the collection, use and dissemination of personal information by an organization. It is relevant to surveillance equipment on drones insofar that a person's identity is clear or can be reasonably ascertained from the recorded information.

In the *Surveillance Devices Act 2007* (Cth), the use of a "listening device" or "optical surveillance devices" to record a private conversation without the consent of the subject of the recording is a Commonwealth criminal offence. Most Australian states, including New South Wales and Victoria, have equivalent state legislation prohibiting the use of listening and optical surveillance devices.

Aside from the above statutory remedies, drone operators should be aware of the risk of breaching confidence if images are surreptitiously obtained. A cause of action for 'breach of confidence' is considered the closest form of protection that Australia has to a common law right protecting a person's privacy.

Unmanned traffic management

In 2020, Airservices Australia, the government-owned organization responsible for the safe and efficient management of Australian airspace, released a Request for Information seeking information from the industry on the key elements that may constitute a future Flight Information Management System with a view to connecting Unmanned Traffic Management participants with Australia's air traffic management system.

While the Request for Information period closed on June 27, 2021, Airservices Australia has not advised on the outcomes of the consultation or otherwise released their findings.

Counter-drone technology

Currently, Australia's drone-specific legislation and regulations generally address drone usage from a safety perspective only.

Jamming devices

Under the *Radiocommunications Act 1992 (Cth)*, the Australian Communications and Media Authority (ACMA) may declare that the operation, supply and possession of certain devices is prohibited.[28]

To date, ACMA has issued declarations prohibiting two forms of jamming devices:

- In 2011, public mobile telecommunications service jammers, i.e., mobile phone jammers;[29] and
- In 2014, devices that were capable of jamming frequencies used by satellite navigation services such as GPS (radio navigation-satellite service).[30]

26 *AG v PYA Quarries Ltd* [1957] 2 QB 169 at 190-1.

27 See *JP Investments Pty Ltd v Howard Chia Investments Pty Ltd* (1989) 24 NSWLR 490 at 496.

28 Section 190 of the *Radiocommunications Act 1992 (Cth).*

29 *Radiocommunications (Prohibition of PMTS Jamming Devices) Declaration 2011.*

30 *Radiocommunications (Prohibited Device) (RNSS Jamming Devices) Declaration 2014.*

In 2018, the ACMA issued temporary authorization for the Australian Federal Police to employ drone-jamming devices as part of providing security for the Invictus Games in Sydney.[31]On October 8, 2020, ACMA issued an authorization for police to use counter-drone devices to respond to threats.[32]

Drone operator qualifications

The legislative framework distinguishes between two principal classes of person in relation to drones:

- Pilot (the person manipulating the flight controls of the drone); and
- Operator (the person, organization or enterprise engaged in, or offering to engage in, an aircraft operation).

There are circumstances where the pilot and/or the operator are required under CASA regulations to be accredited/registered.[33]

The pilot of a drone must hold a Remote Pilot Licence in order to fly a drone larger than the Very Small category (i.e., above 2 kg) for commercial or business reasons.[34]

There is no minimum age requirement to obtain a Remote Pilot Licence.

For drones that are of the Medium category size or under, there are a limited number of Excluded Category scenarios where a Remote Pilot Licence may not be required.[35]

As of January 28, 2021, the operator of a drone must be accredited for any drone that is flown for commercial or business reasons.

An applicant to be an accredited operator of a drone must be at least 16 years of age.[36]

Operating an unregistered drone or without an operator accreditation (or remote pilot licence) for commercial or business reasons is a strict liability offence under CASA regulations and carries a penalty of up to 50 penalty units (approximately AU$11,100).[37]

Developments

We expect that the opportunities presented by the commercialization of drones will continue driving innovations in Australia, as well as continue to exert pressure on CASA to develop practical and useful regulations.

31 *Radiocommunications (Invictus Games Anti-Drone Technology/RNSS Jamming Devices) Exemption Determination 2018.*

32 *Radiocommunications (Police Forces – Disruption of Unmanned Aircraft) Exemption Determination 2020.*

33 Regulation 101.374B of the *Civil Aviation Safety Regulations 1998 (Cth).*

34 Regulation 101.252 of the *Civil Aviation Safety Regulations 1998 (Cth).*

35 Regulation 101.237 of the *Civil Aviation Safety Regulations 1998 (Cth).*

Industry Focus: Oil and gas

The oil and gas industry is a hotbed of drone activity—applications for this disruptive technology range from remote monitoring and inspection, to the deployment of advanced technologies for imaging, surveying, sensing and data transmission. Assessing asset weaknesses, monitoring corrosion and weathering, and tracking emissions, drones are proactively managing assets and infrastructure for oil and gas companies.

Large and small operations alike see massive benefits to adding drones to their existing fleets. Drones can do similar work to traditional aircraft at a fraction of the operational, human and compliance costs. The accessibility and viewpoints that drones create on all work sites is unmatched, along with the multitude of sensors that can be carried as payload to provide specific, real-time data. Additionally, with increasing pressure on oil and gas companies to reduce the environmental impacts of their operations, drones offer another tool in furtherance of that goal.

Drones help manage liability risks by preventing incidents from occurring or demonstrating prudence, due diligence and reasonableness of operations at an oil and gas facility. Among other things, using drones as a regular part of operations or inspections leads to the following risk-mitigating results:

- Provide real-time data that can help avoid issues caused by leaks or emissions;
- Promote and support safe work environments for employees, including by using a drone to access dangerous areas in hazardous environments instead of people;
- Support the defence in a lawsuit where the duty of care owed to neighbours was met and the operation was conducting operations in a safe, compliant and reasonable manner; and
- Ensure faster, more efficient responses in the event of emergency.

ICAO

The International Civil Aviation Organization (ICAO) was formed by the Chicago Convention in 1944 by national governments to support cooperation and standardization of policy in air transport. ICAO is a United Nations organization located in Montreal, Canada. ICAO now comprises 193 nations.

It serves as the global forum for international civil aviation, maintaining an administrative and expert bureaucracy to research and develop new aviation policies and standards, undertaking compliance audits, performing studies and analyses and providing assistance to member states.[36] It convenes panels, task forces, conferences and seminars to support these policy developments.

ICAO publishes Standards and Recommended Practices (SARPs). A standard is binding, like a regulation. Member States are required to adopt a standard in domestic law and a recommended practice is advisory only.

ICAO's burgeoning involvement in RPAS policy - ICAO model regulations

With respect to unmanned aircraft systems, ICAO has developed a set of model regulations, model training and competency materials for operators, a toolkit for recreational and professional operators and guidance on the use of UAS for the purposes of humanitarian aid. It reviewed the existing UAS regulations prepared by many states to identify commonalities and best practices consistent with the ICAO aviation framework, which could be implemented across states. The ICAO Model UAS Regulations are intended to be a starting point for states without existing drone regulations, or to be used as a guide for states to bolster and improve upon their existing regulations.

The ICAO Model UAS Regulations, which can be found in their entirety in PDF form here, currently include three parts, which provide template language for states to use in creating regulations for different categories of operation, and for the creation of approved aviation organizations certification:

Open Category – Part 101:

All unmanned aircraft should be registered;

UA weighing 25 kg or less and operating in Standard UA Operating Conditions (101.7) require no additional operational review; however, if the UA weighs more than 15 kg, the UA must be inspected and approved under 101.21 or 102.301.

Specific Category – Part 102:

Addresses all UA operations using UA that weigh more than 25 kg or those weighing 25 kg or less but do not adhere to Part 101 requirements;

Enables on-going operations or one-time events through certification; and

Enables a more expeditious review when manufacturers declare a type or model of UA as being sufficiently tested for a specific operational category or that has received an approval through an Approved Aviation Organization.

Approved Aviation Organizations Certification – Part 149:

Promotes the use of an Approved Aviation Organization to serve as a designee authorized by the civil aviation authority to perform specific tasks. Once the organization has been certified, the authorized tasks (remote pilot licensing, UA inspection, UA approval, etc.) may provide more expeditious processing and may reduce the workload for CAA Inspectors.

The ICAO has also prepared advisory circulars which clarify and expand on particular sections of the model UAS regulations, including the carriage of dangerous goods using UAS and drone safety assurance.

36 www.icao.int/about-icao/Pages/default.aspx.

Manufacturing standards

ICAO advisory circular 922-001 provides a model of performance-based criteria for UAS manufacturing standards based on the standards set by Transport Canada. This document lays out criteria for system design and description, aircraft serviceability, payloads, and command and control data link, among other things. It also sets out methods for demonstrating compliance on the part of the manufacturer, as well as specific guidelines for modifications.

Training and educational recommendations

The foundation of ICAO's training and education recommendations is the Remotely Piloted Aircraft Systems (RPAS) Manual. The manual provides guidance on the technical and operational issues applicable to the integration of drones into non-segregated airspace and at aerodromes. The primary focus of the RPAS manual addresses international IFR operations of RPA versus the operation of smaller and likely non-certified drones. The manual also provides recommendations on training and certifying authority personnel, minimum age for remote pilots, competencies and training objectives for pilot training programs, practical skills and tests for remote pilots, and medical and licensing standards.

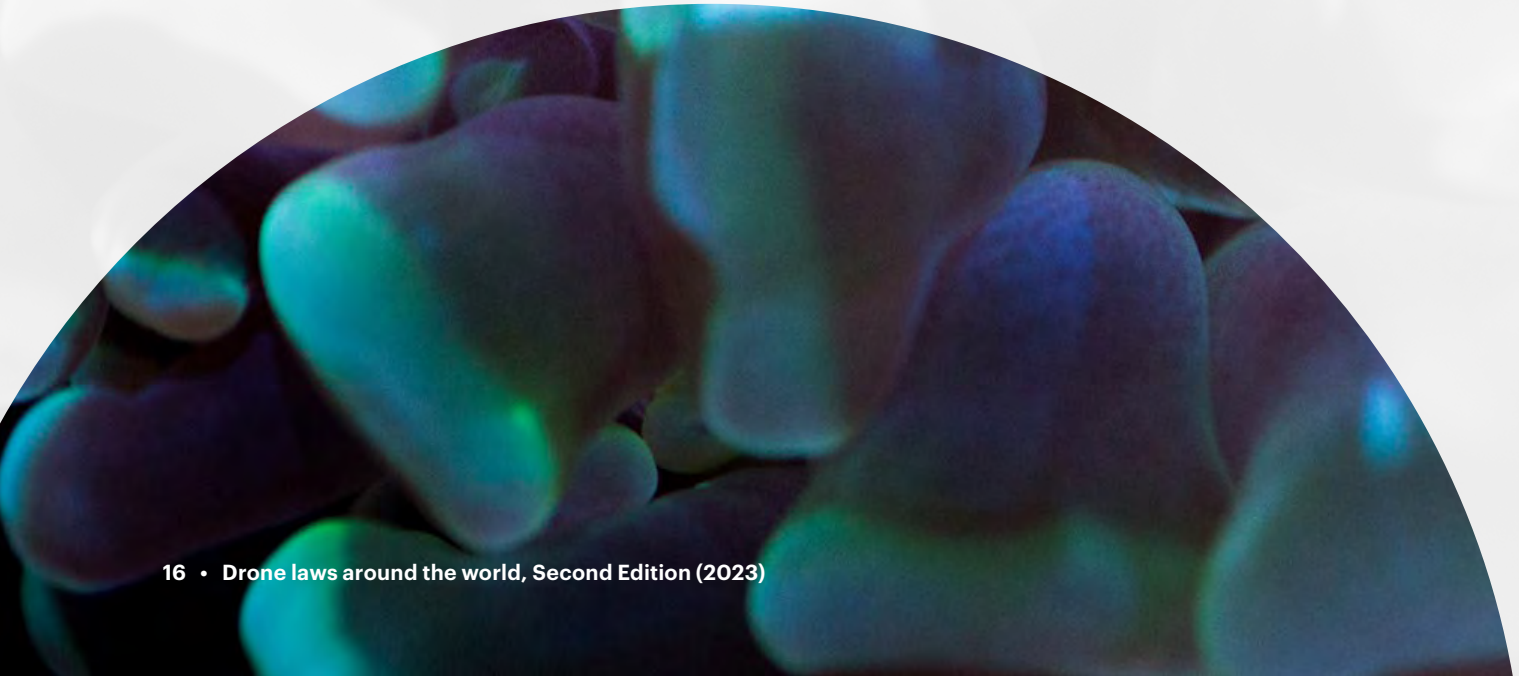
ICAO's role in the future of the drone industry

Given the continued integration of drones into airspace, and the potential for drone operations across international borders, we expect that the need for harmonization will prompt international organizations like ICAO to continue promoting best practices and pioneering thought leadership.

To assist governments, civil aviation authorities and other organizations, ICAO has developed an Implementation Package (termed an iPack) for establishing a regulatory framework for RPAS. Access ICAO's iPack here.

Developments

In 2021, the ICAO Remotely Piloted Aircraft System (RPAS) Panel published revisions to Annex 8 – Airworthiness of Aircraft, for certification of drones conducting international cargo operations or aerial work. The RPAS Panel is also in the process of revising Annex 10 – Aeronautical Telecommunications, with an initial package on the communications and control link. Additional revisions are being made to Annex 1 (personnel licensing for RPAS pilots) and Annex 2 (rules of the air).



Canada

Overview

The *Canadian Aviation Regulations* (CARs)[37] currently authorize the VLOS operation of drones based on weight (250 g to 25 kg) and the risk level of the operation. Operations outside those parameters, such as drones[38] weighing in excess of 25 kg or BVLOS, currently require a special flight operations certificate (SFOC). Subject to a few exceptions, pilot certification and registration are required for drone flights in Canada.

On April 23, 2020, the regulator, Transport Canada, took the first step towards making BVLOS operations a reality in Canada by releasing a notice of proposed amendment for lower-risk beyond visual line of sight (the Notice). The Notice is a foundational step in the Canadian Aviation Regulation Advisory Council process to solicit feedback about potential laws and regulations. The Notice proposes permitting lower-risk BVLOS flights without the need for a SFOC, expanding permissible VLOS operations, requiring declarations of airworthiness for drones and altering requirements for operational and pilot certifications. The first set of proposed BVLOS regulations were published for Canada in June 2023.

While Transport Canada requires drone operators to register their drones, they have not enacted regulations regarding remote ID, nor have they taken an official position on remote ID.

While VLOS operations are permitted by regulations, draft regulations to permit low-risk BVLOS were released in June 2023.

VLOS and BVLOS regulations

As aircraft, drones are regulated under the existing aeronautical and aviation statutes (being the *Aeronautics Act* and the CARs, primarily). The CARs govern civil aviation safety and security in Canada and are administered by Transport Canada. *Part IX –Remotely Piloted Aircraft Systems* of the CARs covers most of the rules that apply to drones weighing 250 g to 25 kg. The regulations do not govern the operations of drones that weigh less than 250 g. Drones weighing in excess of 25 kg require an SFOC to be operated.

Pilot certifications

There are currently two types of pilot certificates in Canada: 1) Small Remotely Piloted Aircraft (VLOS) - Basic Operations; and 2) Small Remotely Piloted Aircraft (VLOS) - Advanced Operations. In order to obtain a basic operations pilot certificate, the pilot must be at least 14 years old and have completed the basic operations exam, a flight review and certain recurring training obligations. Subject to a few exceptions, to obtain an advanced operation pilot certificate, the pilot must be at least 16 years of age, have completed the advance operations exam, successfully completed a flight review and must complete recurring training operations.

Registration

All drones weighing between 250 g to 25 kg are required to be registered and the registration number must be clearly visible on the drone. Drones under 250 g do not need to be registered and drones over 25 kg do not need to be registered but require an SFOC to operate. In order to be a registered owner of a drone, you must be a citizen or permanent resident of Canada that is over the age of 14, a Canadian or provincially incorporated company, or a municipal, provincial or federal entity. Pilots must keep the certificate of registration in an accessible location for the entire duration of the operation.

37 Canadian Aviation Regulations (SOR/96-433).

38 Canada's regulations refer to drones as "remotely piloted aircraft" or "RPAs."

Non-Canadian drone operators who wish to operate in Canada must have a SFOC to fly a drone for any purpose and must also complete the necessary pilot certification in Canada (regardless of whether they are licenced in their home jurisdiction). The foreign drone operator must already be allowed to use the drone for the same purpose in the foreign operators' home jurisdiction, and the approval/authorization must be included in the application for a Canadian SFOC.

Operation types

At this time, drone operations fall into one of four categories for VLOS operations: micro drones, basic operations, advanced operations and SFOC operations.

Micro drones (under 250 g)

Pilots of micro drones do not need to register their drone or get a drone pilot certificate to fly them. While they are not bound by the same requirements as other drones, they must not operate in a reckless or negligent manner as to endanger or be likely to endanger aviation safety or the safety of anyone. There is an expectation for the pilot of a micro drone to use good judgement, identify potential hazards and take all necessary steps to avoid any risks associated with flying their drone.

'Basic' and 'advanced' operations

If an operator meets all five of the following conditions when flying, they qualify to conduct "basic" operations:

1. Fly in uncontrolled airspace;
2. Fly more than 30 m (100 ft) horizontally from bystanders;
3. Never fly over bystanders;
4. Fly more than 3 nautical miles from a certified airport or a military aerodrome; and
5. Fly more than 1 nautical mile from a certified heliport.

When conducting basic operations, the operator must: a) register the drone with Transport Canada, b) mark it with its unique registration number, c) hold a Drone Certificate – Basic Operations' issued by Transport Canada and d) when flying, carry that the pilot certificate and proof of the drone's registration.

"Advanced" operations include:

1. Flying in controlled airspace;
2. Flying over bystanders;
3. Flying within 30 m of bystanders (measured horizontally);
4. Flying less than 3 nautical miles from a certified airport or a military aerodrome; or
5. Flying less than 1 nautical mile from a certified heliport.

If you are conducting advanced operations, you must: a) register your drone with Transport Canada; b) mark your drone with the registration number; c) hold a "Drone Certificate – Advanced Operations" issued by Transport Canada; d) use a drone with an appropriate safety declaration; e) pass the Small Advanced Exam; f) pass a flight review with a flight reviewer; and g) when flying, carry the pilot certificate and proof of the drone's registration. If flying in controlled airspace, advanced approval is required from Canada's air navigation service provider, NAV CANADA. NAV CANADA launched an application to assist drone pilots with flight planning, NAV DRONE.

SFOC operations

For drone operations outside the basic/advanced operation rules, or BVLOS, pilots must apply to Transport Canada to obtain a SFOC in advance of flying.

Government agencies with jurisdiction over drones	Region this agency covers (e.g., entire jurisdiction or province/state)	Role of the agency
Transport Canada	All of Canada	Transport Canada is the civil regulatory authority for Canada. Transport Canada is responsible for establishing, managing and developing the safety and security standards for civil aviation, which includes all drones with the exception of military drones.
Department of National Defence	All of Canada when operating in civil or military restricted airspace	Department of National Defence (DND) is the military authority for Canada. Domestic or foreign military UAVs come under the authority of DND when operating in civil airspace or military restricted airspace.[39]
NAV CANADA	All of Canada	NAV CANADA is a not-for-profit, self-regulating, private corporation. It owns and operates Canada's civil air navigation service, providing air traffic control services, airport advisory and flight information, and aeronautical information to users of Canada's airspace.

Liability

Drone operations are subject to several areas of liability: regulatory penalties for non-compliance, civil, criminal and other laws.

Non-compliance with Canadian Aviation Regulations (CARs)

First and foremost, a drone operator must comply with drone regulations. In general, the CARs prescribe offences for conducting drone operations that violates principles of aviation safety. Transport Canada has broad jurisdiction to investigate and enforce non-compliance. Canadian law enforcement has also been authorized to issue administrative monetary penalties for violations of the CARs. The failure to comply can result in fines and can impact the operator or a business' ability to use drones in the future. Depending on the severity of the offence, individual fines range from CA$1,000 to CA$5,000, and fines for businesses range from CA$5,000 to CA$25,000. Some noteworthy offences and fines include:

Fines for individuals:

- Up to CA$1,000 for flying without a drone pilot certificate;
- Up to CA$1,000 for flying unregistered or unmarked drones;
- Up to CA$1,000 for flying where you are not allowed; and
- Up to CA$3,000 for putting aircraft and people at risk.

Fines for corporations:

- Up to CA$5,000 for flying without a a drone pilot certificate;
- Up to CA$5,000 for flying unregistered or unmarked drones;
- Up to CA$5,000 for flying where you are not allowed; and
- Up to CA$15,000 for putting aircraft and people at risk.

39 Drones in Canada, Report by the Research Group of the Office of the Privacy Commissioner of Canada, March 2013.

Civil liability

As well as the regulations and criminal law risks above, individuals and businesses may be liable under a variety of statutes and the common law for negligence, trespass, nuisance and breach of privacy. As an example, under the Ontario *Trespass to Property Act*, a trespasser can be found guilty of an offence, and on conviction is liable to a fine of up to CA$10,000 plus any damages and costs. A drone that wanders or deliberately ventures onto private property could result in the operator, and the business who hired them, being liable for trespass.

Criminal liability

Operating a drone outside of the law can also have criminal consequences (though most likely for the drone operator personally rather than the business or person who has hired them). The *Criminal Code* of Canada[40] also contains a number of offences including: Section 77(c) and (d) damaging an aircraft while in service in a manner that could endanger the safe operation of the aircraft or airport and Section 77(e) interfering with the operation of any air navigation facility in a manner likely to endanger the safety of an aircraft in flight. In addition to these offences, criminal negligence could also apply under section 219 of the Criminal Code along with relevant sections of the Criminal Code relating to breaking and entering and mischief.

Other liability – municipal bylaw infractions

In order to mitigate legal risks when conducting flights, drone operators need to analyze and abide by all applicable municipal bylaws before flight. Unless a court determines that a municipal bylaw impacting drone operations is invalid, drone operators must comply with the bylaw at all times. For example, in Calgary, Alberta, municipal bylaws prohibit the launch or operation in a park of "any remote control device including ... planes" and prohibit the operation of "model airplanes of any nature" from using a street for the "purposes of flying."[41]

Parks Canada also prohibits the recreational flight of drones in Canada's national parks, although certain non-recreational flights are permitted in some circumstances with advance permission.

Other liability – privacy torts

In Canada, statutory torts and common law torts are available for breaches of privacy by individuals and organizations. In tort law, an individual can launch an action in court to obtain a civil remedy, such as damages, against the person who committed the act or omission (e.g., an invasion of privacy).

Certain provinces have established a statutory tort for the invasion of privacy, which allows an individual to bring a civil action for improper access to or use of personal information. For example, under the *Privacy Act*[42] in British Columbia, an individual has a right to sue for invasion of privacy. It is a tort for a person to use the portrait (or image) of another for commercial purposes without consent.

Individuals can also use common law torts to seek redress for breaches of privacy. This includes the tort of "intrusion upon seclusion" and the novel tort for "disclosure of private facts." These torts and others (such as the tort of trespass) are potentially available to individuals who have their privacy invaded by drones.

The tort of intrusion upon seclusion may occur where:

- The drone operator's conduct was intentional (including recklessness);
- The drone operator invaded, without lawful justification, the plaintiff's private affairs or concerns; and
- A reasonable person would regard the invasion as highly offensive, causing distress, humiliation or anguish.

The tort of disclosure of private facts may occur where:

- The drone operator publicized an aspect of the plaintiff's private life;
- The plaintiff did not consent to the publication;
- The matter publicized or its publication would be highly offensive to a reasonable person; and

40 RSC 1985, c. C-46.

41 For more information, please see our article "Municipal bylaws impacting drone operations – are they legal?".

42 RSBC 1996, CHAPTER 373.

- The publication was not of legitimate concern to the public.

There are no reported court cases in Canada alleging a drone operator had committed any of these privacy torts. When it does occur, the accused drone operator will be well advised to follow certain best practices of operations to avoid committing privacy breaches.

Data privacy and security

Canada's privacy laws apply to commercial and recreational drone operators alike and should be considered before all operations. Transport Canada has also released privacy guidelines for drone users. Transport Canada suggests that recreational drone operators bear the following privacy principles in mind when operating a drone: 1) be accountable; 2) limit collection; 3) obtain consent; 4) store information securely; and 5) be open and responsive about your activities.

Relevant privacy law

Commercial drone operators must follow the *Personal Information Protection and Electronic Documents Act* (PIPEDA).[43] In Canada, federal legislation, PIPEDA, as well as substantially similar provincial legislation in the provinces of British Columbia, Alberta and Québec, establish rules on how private-sector organizations may collect, use or disclose "personal information" in the course of commercial activities.

One important threshold issue is whether information and data collected by drones is "personal information." "Personal information" is information about an identified or identifiable individual, either alone or in combination with other information.

Every organization subject to PIPEDA must comply with 10 principles. The most notable principles for commercial drone operators are:

Accountability: An organization is accountable for personal information under its control, and must implement a governance structure and privacy policies to demonstrate compliance with privacy law.

Consent: Consent (express or implied) of an individual is required to collect personal information. Whether consent be express or implied depends on the sensitivity of the information, the reasonable expectations of the individual in the circumstances and the risk of harm. Consent must be informed, free and meaningful.

Limiting collection: An organization cannot collect information beyond what it needs to provide the goods or services offered.

Safeguards: Personal information must be protected by security safeguards at a level appropriate to its sensitivity.

Openness: An organization must proactively make available their policies and procedures on information management in clear and accessible language.

Individual access: Individuals have the right to obtain access to their personal information upon request.

Remedies: Individuals must have recourse to complain about compliance concerns.

Unmanned traffic management

There is currently no formal structure for unmanned traffic management in Canada.

In 2018, the Remote Traffic Management Action Team (RTMAT) was established to consider Canada's approach to unmanned traffic management. Members of the RTMAT include Transport Canada, NAV CANADA and other key industry stakeholders. Now termed the "RTM Advisory Committee," work is underway to develop processes in controlled airspace for how to assess, communicate and manage and mitigate risk. Air traffic control in Canada, operated by NAV CANADA, currently segregates drone operations from traditional aircraft operations.

While Transport Canada requires drone operators to register their drones, there are no regulations (either proposed or enacted) regarding remote ID. In March 2022, Transport Canada established a

43 SC 2000, c. 5.

working group (along with other Canadian industry stakeholders) to provide policy and technical recommendations for the implementation of remote ID in Canada.

Counter-drone technology

While technology that assists in the detection of drones is likely legal in Canada, the use of counter-drone technology to disrupt or interfere with drones in flight is generally illegal. The three most common counter-drone measures are jamming devices, software exploitation devices and physical disruption. All of these counter-drone measures are illegal in Canada.

Jamming devices

Jamming devices operate by interfering with, or 'jamming', the radiofrequency between the controller and the drone and/or the GPS function of the drone that relays its location. If successful, jamming devices often render the drone inoperative.

Sections 4(4) and 9(1)(b) of the *Radiocommunication Act*[44] prohibit the use, possession, manufacturing, importing, distribution, leasing, offering for sale and sale of jamming devices in Canada. Individuals charged under these provisions can face a fine of up to CA$5,000 and/or imprisonment for up to one year. Corporations may face fines of CA$25,000, and in some cases, several millions of dollars per offence.

Though generally illegal for civilians, the RCMP may possess and operate jammers in specific circumstances. On July 2, 2019, an exemption order for RCMP officers entitled the Radiocommunication Act Exemption Order (Jammers – Royal Canadian Mounted Police) came into force. Similar to the exemption that was previously in force since 2015, this exemption allows RCMP officers who are required, as part of their duties or training, to install, use, possess, manufacture or import a jammer for purposes like ensuring national security, public safety and the investigation of offences. Before use, RCMP officers must notify the Minister of Industry. Further, officers must maintain records of all usage and make every reasonable effort to limit the jammer's interference with other radio communications.

Software exploitation devices

Software exploitation devices target the drone's software directly and often allow the attacker to take control of the drone and to obtain access to data from the drone.

Section 342.1 and Section 342.2 of the Criminal Code prohibit counter-drone technology that exploits the drone's software. Under these sections, it is unlawful to intercept (or cause an interception of any function of a computer system) and to make, possess, sell, offer for sale, import, obtain for use, distribute or make available a device that is designed or adapted primarily to intercept any function of a computer system. Drones and the associated equipment likely constitute a "computer system" for the purposes of these provisions, rendering these devices unlawful. Penalties under these sections range from summary conviction to an indictable offence with imprisonment of up to 10 years.

Physical disruption

Physical disruption devices include objects like lasers, nets and projectiles that are used to physically interfere with or intercept a drone.

While these devices are not expressly prohibited by regulation or statute, their use likely constitutes a trespass to the property of the drone's owner. There have yet to be a judicial decisions in Canada to confirm this interpretation. Further, it is unclear how a court would handle a case where a drone conducted an unauthorized flight over private property and the property owner used a physical disruption method to interrupt the drone's flight.

44 RSC 1985, c. R-2.

Drone operator qualification requirements

Drone weight	License requirement
Under 250 g	No license required
250 g – 25 kg	Pilot Certificate-Basic Operations or Pilot Certificate-Advanced Operations is required
Over 25 kg	Special Permission from Transport Canada is required

In Canada, a drone pilot certificate is required to operate a drone, with two notable exemptions. The first exemption is for drones that weigh less than 250 g. Drones that weigh less than 250 g are commonly referred to as "micro drones," an example of such a drone is a "DJI Mini."

At present, there are two different drone pilot certificates, one for basic operations and one for advanced operations. The certificate a pilot needs will depend on if they are conducting basic or advanced operations. Standard 921.04 – Recency Requirements outlines acceptable activities, including: (a) attending a safety seminar endorsed by Transport Canada Civil Aviation; (b) completing a recurrent drone training program; and (c) completing a self-paced study program endorsed by Transport Canada Civil Aviation.

Developments

On June 23, 2023, Transport Canada published the long-awaited proposed regulatory amendments to the CARs to provide for low-risk BVLOS operations in Canada. Not only is this a first for Canada, these regulations are among the first in the world. Transport Canada noted the importance of BVLOS regulations to the continued development of the industry:

> **"To unlock the potential of medium-sized RPAS and beyond visual line-of-sight operations, regulatory amendments are needed to allow more routine operations, provide regulatory predictability, and support economic growth. This would help the Canadian [drone] industry to remain competitive in the global market while also supporting economic recovery in Canada post-pandemic."**

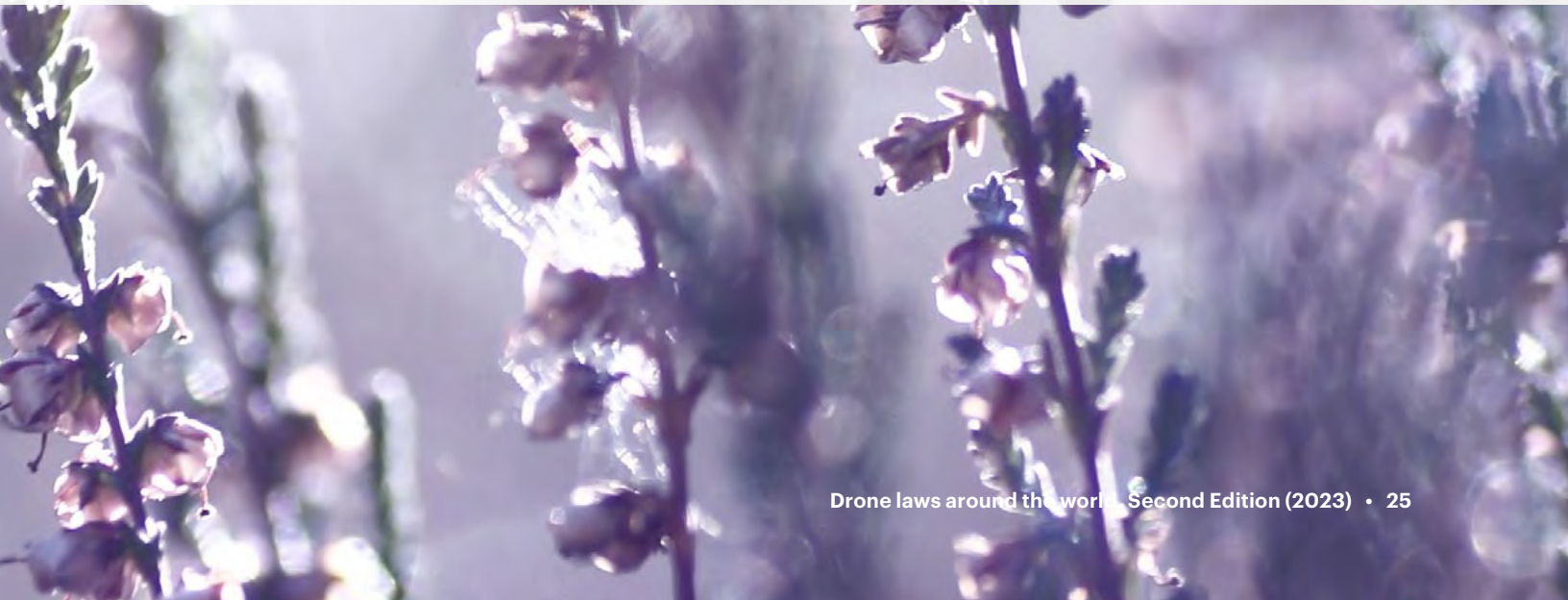
This proposal provides for routine BVLOS operations by drones weighing up to 150 kg carrying on low-risk operations: where the operations are in sparsely populated areas, in uncontrolled airspace and at low altitudes. In these areas, package delivery, first responder operations and natural resource and wild life studies can routinely take place. Also, as anticipated, the proposed amendments provide for further VLOS operations for medium sized drones (those weighing up to 150 kg).

Grouped into three areas of focus, the proposed amendments relate to: 1) pilot training and certification, 2) aircraft and supporting systems, and 3) operational rules. Notable aspects of the amendments include:

- Elimination of the need to obtain an SFOC for certain lower-risk BVLOS operations;
- Broadened privileges for pilots conducting advanced operations and a new class of pilot certificate is proposed for BVLOS;
- New requirements for organizations operating BVLOS;
- Pilot medical requirements (which builds on Transport Canada's 2021 proposal for medical requirements);
- Additional guidance for manufacturers; and
- New services and fees to support the expanded framework to support drone operations.

Some of the regulations are anticipated to come into force in the Fall of 2024 when they are published in Canada Gazette, Part II. The remainder of the regulations will likely come into force on April 1, 2025. In 2025 and beyond, Transport Canada is expected to publish subsequent regulatory packages for more complex operations (including larger drones, highly automated drones, medium-risk BVLOS, delivery and Advanced Air Mobility).

Additionally, updates have been made to applicable standards and Transport Canada publications to support the proposed amendments, being: *Standard 921 Remotely Piloted Aircraft, Standard 922 RPAS Safety Assurance and TP 15263 Knowledge Requirements for Pilots of Remotely Piloted Aircraft Systems, 250 g up to and including 150 kg, Basic and Advanced Operations*. Two new standards and one new Transport Canada Publication will be available for comment as well: *Standard 923 Vision-Based detection and avoidance (DAA), Standard 924 RPAS Medical Requirements and TP 15530 Knowledge Requirements for Pilots of Remotely Piloted Aircraft Systems Operated Beyond Visual-Line-of-Sight (BVLOS)*.



European Union

Overview

As of January 1, 2021, national regulations in European countries relating to drones were largely replaced by European regulations[45] (the EU Regulations). EU Regulations are intended to simplify and standardize the rules for all EU countries in order to encourage the development of the drone industry in Europe. The European Commission has also published a regulation for U-space airspace, which is the airspace in which most drone operations are expected to be conducted. That rule took effect in January 2023.

The EU regulations recognize the competence of Member States by giving them significant responsibility to grant operational authorizations in the Specific category, grant Light UAS Operator Certificates (LUC), establish U-space airspace, and determine geographic zones where drone operations are prohibited or restricted.

While several European national drone regulations distinguished between recreational activities and professional activities, EU Regulations no longer make this distinction and base their requirements solely on the risk levels of the operations, regardless of any commercial consideration of the operation.

EU Regulations create three categories:

Category	Risk
Open	The Open category for low-risk operations (line-of-sight flying in geographical areas that represent a low risk to air traffic and people).
Specific	The Specific category for moderate risk operations (line-of-sight or out-of-sight flight in conditions that are not compliant with the "open" category).
Certified	The Certified category for high-risk operations requiring a high level of reliability of the aircraft and operations (e.g., transport of people).

Recreational activity is mainly included in the Open category; professional activity usually corresponds to the Specific and Certified categories.

VLOS operations

Open category drones covered by the EU Regulations are those with a particular focus on VLOS.

EU Regulations for the Open category require drones to have a CE marking accompanied by an indication of their class, noted from C0 to C4. The class depends on technical characteristics such as mass or speed. In simple terms, the requirements are higher for heavier drones or ones operating closer to people. Effective January 1, 2023, all drones marketed must include an indication of their class; without such an indication, a drone will no longer be permitted to be sold in Europe.

The Open category includes subcategories A1, A2 and A3, which may allow, in some cases, overflight of people (but never over gatherings of people):

Subcategory	Class	Overflight of people
A1	C0, C1	• Tolerated for C0 (<250 g) • Yes, if unintentional for C1 (max 400 g)
A2	C2	• Overflight is forbidden • Flight at 5m from people with low-speed mode • Flight at 30 m from people otherwise
A3	C2, C3, C4	• Forbidden

EU Regulations for the Open category provide that:

- The pilot is held responsible for the safety of the flight;
- One must register to obtain a "UAS operator number" to fly a drone weighing more than 250 g or equipped with a camera;
- A mandatory online training course is required to operate an aircraft weighing more than 250 g (validated by passing an exam);

45 Commission Implementing Regulation (EU) 2019/947 of 24 May 2019; Commission Delegated Regulation (EU) 2019/945 of 12 March 2019

- The maximum flight height is 120 m (except for certain model aircraft clubs);
- It is forbidden to fly over a gathering of people;
- It is necessary to fly in direct view of the pilot;
- In the case of immersion flights, the pilot must be assisted by an observer (who must keep the aircraft in direct view);
- It is forbidden to transport dangerous materials; and
- Flying in the vicinity of emergency services is prohibited.

If the above conditions are not met, the drone cannot be operated in the Open category and will fall in the Specific category.

In 2022, the European Commission determined that Open category operations not in compliance with Parts 1 to 5 of the Commission Delegated Regulation (EU) 2019/945 may be permitted until December 12, 2023.

Specific category operations

In general, any operation that does not meet the requirements of the Open category falls into the Specific or Certified category. Specific category operations require an operational authorization from the Member State unless the operation complies with the requirements for a standard scenario.

A drone operator may declare itself in compliance with one of the European standard scenarios STS-01 or STS-02. Member States may continue to authorize Specific category operations under a national standard scenario until December 12, 2023, provided that such operations meet the requirements of UAS.SPEC.020 of the Annex to the Commission Implementing Regulation (EU) 2019/947. Beginning January 1, 2024, no declaration can be made according to any national standard scenario.

The two European Commission standard scenarios STS-01 or STS-02 (entered into force: December 2, 2021, but delayed as explained above).

Scenario	Operations
STS-01	Operations in direct view (VLOS) at a maximum height of 120 m above a controlled area on the ground in a populated environment.
STS-02	Beyond visual line of sight (BVLOS) operations at a maximum height of 120 m above a controlled area on the ground in a low population density environment. It can be operated at a maximum of 1 km from the pilot; this distance may be increased to 2 km if an observer is present.

A Light UAS Operator Certificate (LUC) is an organizational approval certificate that can be used by a drone operator to have its organization assessment by the National Aviation Authority.[46]

Operational authorizations:

Any operation outside the standard scenarios described above requires an operational authorization issued by the Member State civil aviation authority (CAA), after assessing the risk analysis submitted by the applicant in accordance with the Specific Operations Risk Assessment (SORA) method defined in the "Acceptable Means of Compliance" proposed by the European Aviation Safety Agency (EASA). SORA version 2.0 will be replaced in 2024, after JARUS publishes its final version of SORA 2.5, expected by the end of 2023.

The operator must also provide a statement confirming that the proposed operation complies with applicable EU and national rules, including privacy, data protection, liability, insurance, safety and environmental protection.

EASA has developed Predefined Risk Assessments (PDRAs) to simplify and expedite the operational authorization process. A PDRA is an operational scenario for which EASA has conducted a risk assessment and published an acceptable means of compliance (AMC) to Article 11 of the

46 The requirements are defined in Part C of Regulation. (EU) 2019/947 (p.35).

Implementing Regulation (EU) 2019/947. Instead of performing a SORA, an applicant can complete the PDRA table, prepare the operator manual and submit the application to the CAA of the state of registration. EASA has developed five PDRAs and will adopt several more PDRAs expected to be published by JARUS later in 2023.

PDRA S-01 (AMC3) – Agricultural works, short range cargo operations

- VLOS;
- Below 120 m or 150 m* (also in urban environment); and
- No involved person is present in controlled ground area.

PDRA S-02 (AMC4) –Surveillance, agricultural works, short-range cargo operations

- BVLOS up to 1 km distance of 2 km is airspace observer is used;
- Below 120 m or 150 m (not in urban environment); and
- No involved person is present in controlled ground area.

PDRA G-01 (AMC2)– Surveillance, long-range cargo operations

- BVLOS;
- Uncontrolled airspace below 120 m or 150 m (over sparsely populated area);
- With a UAS maximum dimension less than 3 m;
- PDRA G-02 (AMC3) – All range of BVLOS operations, in the range of the direct C2 link (radio line of sight);
- Below 120 m or 150 m in reserved/segregated airspace over sparsely populated area; and
- With a UAS maximum dimension less than 3 m.

PDRA G-03 (AMC6) – Linear inspections, agricultural works

- BVLOS, in the range of the direct C2 link (radio line of sight);
- Controlled or uncontrolled airspace;
- Below 30 m or close to obstacles over sparsely populated area; and
- With a UAS maximum dimension less than 3 m.

For each of these PDRAs, the drone must meet the technical requirements in the PDRA, and the altitude limitation of 120 m may be increased to 150 m with additional mitigations.

For medium risk operations in the (Specific Assurance and Integrity (SAIL) III and IV), operators may need to undertake a design verification process with EASA. The Commission recognizes the burdens design verification may impose on drone operators, and intends to develop additional Standard Scenarios and PDRAs. For SAIL V and VI, EASA has responsibility to issue an operator certification or an LUC may be used.

Liability

Even though the EU Regulations are in force, civil and criminal liability can still accrue to drone operators under the European country's national laws.

Data privacy and security

The right to privacy and personal data protection is considered a fundamental right in Europe.

Data privacy

The right to privacy and personal data protection is a fundamental right in the European Union, and the common legal framework is provided by the Reg. (UE) 2016/679 (**GDPR**).

Although the GDPR does not provide for specific rules applicable for drones only, it is a wide and comprehensive piece of legislation. The GDPR applies to any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, retrieval, consultation, use, disclosure, erasure and destruction.

In light of the above, data privacy must be considered carefully when drone operations are carried out. As a matter of fact, several privacy risks may arise in relation to the processing of data, as drones are usually equipped with devices capable of collecting and processing personal data (e.g., images, sounds and video recording). Such risks range from the lack of transparency to the unlawful collection of a wide bulk of data and the difficulty to inform the data subject about the ongoing processing. Therefore, all the core principles of the GDPR also apply to drone operations and to the personal data processed. By way of example, drone operators shall ensure that:

- Drones only collect personal data strictly necessary for the purpose of processing (if any);
- The hardware and software used to operate the drones are developed in compliance with *privacy by design and by default* principles;
- An information notice, pursuant to Article 13 of the GDPR, is delivered to the data subject prior to the data processing activity;
- Data processing activities are mapped in relevant records pursuant to Article 30 of the GDPR; and
- A data protection impact assessment is carried out to identify privacy risks and related security measures.

In 2015, the Working Party Article 29 (now, European Data Protection Board- **WP29**) released the "Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones." Among other things, the WP29 recommends a "multi-level strategy" to comply with the information notice obligations through warnings near overflowed areas and information published on each drone's operator website. It also recommends that drone operators use technology that limits data collection and processing to the extent that is essential for their purposes and implement *privacy by default* measures, ensuring the drone is as visible and traceable as possible.

Unmanned traffic management (UTM)/U-space

UTM/U-space is recognized as a key enabler to ensure the safe and efficient integration of unmanned vehicles in the airspace. The European Commission published three U-space Airspace Implementing Regulations, which took effect on January 26, 2023.[47] Those regulations permit each member state to designate certain uncontrolled airspace as U-space airspace. Member States may also determine whether the ANSP or a federated system of U-space Service Providers will operate the U-space system. Manned aircraft operating in U-space airspace must be equipped with electronic conspicuity technology.

Developments

In November 2022, the Commission published "Drone 2.0 strategy," which aims to ensure that drones contribute, through digitization and automation, to a new offer of sustainable services and transport, while taking into account possible civil/military technological synergies. The Commission envisions a complete U-space regulatory framework by 2030, with the integration of legacy and unmanned traffic in the same airspace, inside and outside of U-space airspace.

EASA has published Acceptable Means of Compliance (AMC) and Guidance Material (GM) for Implementing Regulation (EU) 2019/947.

EASA has proposed guidelines for noise measurement of drones lighter than 600 kg operating in the Specific category. Comment period which ended in January 2023. EASA has stated that national authorities may use these guidelines in evaluating applications for operational authorization.

47 European Commission Implementing Regulation (EU) 2021/664; European Commission Implementing Regulation (EU) 2021/665, amending Implementing Regulation (EU) 2017/373 (ATM and air navigation services in controlled airspace); European Commission Implementing Regulation (EU) 2021/666, amending Regulation (EU) No. 923-2012 (manned aircraft operations in uncontrolled airspace).

European Union Member State Authority

Denmark

France

Germany

Italy

Luxembourg

Netherlands

Romania

Spain

As previously stated, the EU regulations recognize the competence of Member States by giving them significant responsibility to grant operational authorizations in the Specific category, grant Light UAS Operator Certificates (LUC), establish U-space airspace and determine geographic zones where drone operations are prohibited or restricted. Member States are beginning to implement the EU regulations, although their progress is limited and varied to date. For example, national standard scenarios or equivalents are still in force until the end of 2023. Also, the U-space regulation did not come into force until January 26, 2023. The number of operational authorizations varies significantly among Member States. There are only a handful of Light UAS certificates, given how much of a burden it is to obtain such certificate, and, at this time, there are only four design verification applications throughout the EU. Below are results of a survey of how several Member States are implementing the EU Regulations.

Denmark

Operational authorizations: predefined Risk Assessment's (PDRAs)

Operators predominantly use PDRA 01. Several schools in Denmark have been set up to train operators on using PDRAs.

Light UAS Operator Certificates

To date, the CAA has received only one LUC application, which is still being processed. The CAA has not issued any guidance,

U-space airspace

No U-space airspace has been determined at this time. The CAA will be prepared to do this beginning with the January 26, 2023 implementation date. While Denmark will have a federated system, no company has applied yet to be a U-space Service Provider. The ANSP has shown interest in providing these services, but it will be required to establish a private entity to avoid the conflict.

Geographic zones

Denmark has established three geographic zones, one around Hans Christian Andersen Airport, and another at a test facility at Unser Airport. The geographic zones are available on the CAA website.

France

Operational authorizations

The Directorate of Civil Aviation Safety (*Direction de la sécurité de l'aviation civile* or DSAC) indicates that 133 authorizations were issued in 2021 and 168 were issued in 2022.[48]

Standard scenarios. Until January 1, 2024, an operator may only declare itself according to one of the three national scenarios; S1, S2 or S3.[49] These scenarios are defined in a ministerial order dated December 3, 2020 (link). They can be summarized as follows:[50]

National standard scenario	Operation
S1	Use outside populated areas, without overflight of third parties, operation in sight and at a maximum horizontal distance of 200 m from the pilot.
S2	Use outside populated areas, without third parties on the ground in the area of evolution, not meeting the criteria of scenario S1, at a maximum horizontal distance of 1 km from the pilot.
S3	Use in populated areas, without overflight of third parties, operating in direct view and at a maximum horizontal distance of 100 m from the pilot.

As of January 1, 2024, these three national scenarios will no longer be available. However, if an operator has already declared itself according to one of the national scenarios before January 1, 2024, it will be able to keep operating under the applicable national scenario until January 1, 2026.

48 Email from dsac-autorisations-drones-bf@aviation-civile.gouv.fr dated November 5, 2022.

49 The original deadline of December 2, 2021 has been extended by 2 years.

50 Dentons, *Remotely Piloted Aircraft Systems: a comparative guide of the drone regulatory laws around the world*, 2021, p. 33.

Light UAS Operator Certificates

The DSAC indicates that one Light UAS Operator Certificate (LUC) has been issued so far.[51] The French Civil Aviation Authority (*Direction Générale de l'Aviation Civile,* or DGAC) published a guide on the specific category updated in March 2023. The guide, in principle, indicated an applicant shall be a legal person, and an operator of UAS of significant size and complexity, operating outside the standard scenarios and carrying out various types of operations that would require multiple authorizations. An FAQ has been published on the Ministry of Ecology website (link, p.7), which mentions that, in the long term, it is likely that a fee would be charged to hold a LUC. As a LUC is a "very specific case," the guide does not go into further detail, but invites interested drone operators to contact the DSAC for further information at the following e-mail address: dsac-autorisations-drones-bf@aviation-civile.gouv.fr.

Contacted by an association of drone operators, the DSAC indicated that it is not able to provide operators with personal assistance in compiling their application files.[52]

U-space airspace

The U-space system in France will be federated. To date, no U-space airspace has been designated by the *Direction Générale de l'Aviation Civile* (DGAC), a department of the Ministry of Ecology. A U-space service provider (USSP) must obtain a certificate issued by the DSAC for a USSP whose principal place of business is in France.[53]

Certification by the DSAC will involve seven steps:

1. Declaration of application by the candidate service provider;
2. Designation by the DSAC of an agent responsible for the certification and implementation of a certification plan, in coordination with the candidate;
3. Production of a certification file by the candidate;
4. Study of the certification file by the DSAC;
5. Certification audit by the DSAC of the candidate, if applicable;
6. Treatment of possible non-conformities; and
7. Issuance of the certificate, if applicable.

After certification, the USSP will enter a phase of continuous monitoring by the DSAC. Exchanges between service providers and the DSAC regarding their certification or their continuous surveillance will be carried out thanks to the METEOR application (link).

Based on the available information online, we understand that the government will be the entity responsible for establishing U-space airspace.

Geographic zones

Geographic zones in which special rules apply to drones are available on the SIA (*Service de l'Information Aéronautique*) website (link). The geographic zones identified in the user guide correspond to the airspace use restrictions available in French aeronautical information publications (AIP) (link) and are listed in the user guide.

As geographic zones are a part of the airspace in which special conditions apply to the operation of drones for various reasons (including safety, privacy and personal data protection, security and environment), geographic zones result from various regulations and take several forms (e.g., controlled airspace, restricted or prohibited areas, or national park areas).

51 Email from dsac-autorisations-drones-bf@aviation-civile.gouv.fr dated March 20, 2023."

52 SORA, LUC les différences pour obtenir une autorisation d'exploitation - APADAT.

53 EASA is however competent to certify USSP whose principal place of business is in a third country of EASA, or who are established or resident in such a country.

Furthermore, a map developed by the DSAC and the IGN (*Institut national de l'information géographique et forestière*) displays areas subject to prohibitions or restrictions on the use of drones in the Open category or by model aircraft associations (outside published model aircraft sites) in metropolitan France. The map is available on the géoportail website.

French geographic zones are not defined by a dedicated sector of the government that is solely responsible in that regard. They are the result of disparate regulations creating specific conditions in a given area that are adopted by several entities of the government (e.g., the order dated December 3, 2020, on the use of airspace by unmanned aircraft that was adopted by the Ministry of Ecology, the Minister of the Armed Forces and the Minister of Overseas France decrees creating natural parks such as the Decree No 2019-1132 dated November 6, 2019, creating the National Park Forests adopted by the Prime Minister, the Minister of Ecology and the Minister of Public Accounts, etc.). However, the part of the government responsible for providing information regarding geographic zones appears to be the DGAC, more precisely the DSAC and the SIA.

Germany

Numbers on authorizations, to our knowledge, are not publicly available on the webpage of the Federal Aviation Office (LBA).

Standard scenarios

Germany is currently using a national standard scenario for the ground-level use of unmanned aerial vehicles on agricultural land (DE.STS.FARM).

Light UAS Operator Certificates

A guidance document providing general information for people interested in a Light UAS Operator Certificate is available here.

A guidance document for the preparation of a manual for flight operations with a Light UAS Certificate is available here.

U-space airspace

On December 15, 2022, the Federal Ministry of Digital and Transport (BMDV) issued a U-space concept.

The concept provides guidelines for a law to be enacted in 2023 which will establish U-spaces in Germany. A U-space coordinator based at the BMDV will decide on the establishment of U-Space airspaces.

Germany envisions several U-space Service Providers in a U-space. These will be the points of contact for drone operators and, among other things, will issue flight permissions for the drone operations. The USSPs will receive their information from the Single Common Information Service Provider (Single CISP). It will provide the USSP with all relevant airspace and traffic data for the performance of U-space services.

Each U-space airspace must have at least one USSP authorized by the Federal Supervisory Authority for Air Navigation Services (BAF), by a Member State of the European Union, or approved by the EASA.

The approval of USSPs is regulated by the provisions of the Implementing Regulation (EU) 2021/664 of the Commission (IR 2021/664) and, in the future, by the Acceptable Means of Compliance (AMC) and the Guiding Material (GM) of the EASA (link).

The entity responsible for this is the BMDV. The BMDV, or a federal authority designated by the BMDV, shall appoint a U-space coordinator whose task it is to conduct a risk assessment in coordination with the competent authorities (in particular, the state aviation and environmental authorities and the German Military Aviation Authority (LufABw), or the competent unit of the Federal Ministry of Defence (BMVg)), including the local authorities and agencies pursuant to Article 18 (f) IR 2021/664. On the basis of the risk assessment, the BMDV shall define the performance requirements for the U-space airspace pursuant to Article 3 (3) and (4) IR 2021/664 (UAS Capabilities, U-space services, operating conditions and airspace restrictions). Should environmental, noise, nature conservation or consumer protection aspects be affected significantly, the decision shall be made

in consultation with the Federal Ministry for the Environment, Nature Conservation, Nuclear Safety and Consumer Protection (BMUV), or a federal authority designated by the BMUV (link).

No U-space airspace has been designated yet. Once legislation has been passed in 2023, the first U-space airspaces can be designated.

Geographic zones

The BMDV is responsible for designating geographic zones (section 21h (4) of the Rules of the Air Regulations (LuftVO)). Section 21h LuftVO lists geographical zones in which operations are only possible under certain conditions. The following list provides an overview of these geographical zones:

- Aerodromes (section 21h (3) no. 1 LuftVO);
- Airports (section 21h (3) no. 2 LuftVO);
- Industry and energy supply, as well as special facilities and authorities (section 21h (3) no. 3 LuftVO);
- Other facilities and authorities (section 21h (3) no. 4 LuftVO);
- Rail, ship and road transport (section 21h (3) no. 5 LuftVO);
- Nature conservation areas (section 21h (3) no. 6 LuftVO);
- Residential property (section 21h (3) no. 7 LuftVO);
- Outdoor swimming pools (section 21h (3) no. 8 LuftVO);
- Control zones (section 21h (3) no. 9 LuftVO);
- Hospitals (section 21h (3) no. 10 LuftVO);
- Accidents and deployment sites (section 21h (3) no. 11 LuftVO) and
- Temporary geographical zones (section 21h (4) LuftVO).

The geographical zones described can be viewed using the provided map tool. Unless otherwise determined by the BMDV or a federal agency designated by the BMDV, geographic zones pursuant to section 21h LuftVO remain valid within the U-space airspaces.

Italy

Operational authorizations

The Italian Civil Aviation Authority (ENAC) has issued 61 authorizations to carry out operations falling under the notion of the Specific category. The up-to-date list of authorizations is publicly available at this link. In Italy, there are no additional standard scenarios to those adopted by the EASA. Therefore, any drone operation that does not fit in the EASA's scenarios shall be authorized by the ENAC, pursuant to Article 12 of the Regulation (EU) 2019/947. The application for authorizations can be filed electronically by sending, via certified e-mail, (i) the form available at this link (in Italian only) and (ii) the receipt of payment of the administrative fee, which can be paid online at this link.

Light UAS Operator Certificates

To date, there is no official data regarding the number of applications for Light UAS Operator Certificates (LUC). The list of UAS Operator is available at this link. This includes UAS Operator who consented to the publication only, not a complete list of UAS Operators.

U-space airspace

According to the agreement in force between ENAC and ENAV, ENAV (through its controlled company D-Flight S.p.A.) is the authority responsible for establishment of U-space airspace. ENAV S.p.A., the Italian public company responsible for the management and control of civil air traffic (together with its controlled company D-Flight S.p.A.), will be the exclusive U-space service provider in charge of developing the U-Space airspace in Italy.

According to an ENAV timeline (available at this link), U-space full services will be implemented in 2025 (i.e., integration of interfaces with manned aviation and implementation of new additional services, based on a very high level of automation, connectivity and digitalization). As of now, only the U-Space initial services have been implemented (i.e., support to the management of drone operations: flight planning, flight approval, localization, dynamic airspace information and procedural interfaces with air traffic control).

Pending the full applicability of the U-Space regulations, with regard to the use of drones in the Italian airspace, ENAC supports the experimental initiative of promoting a remote identification service provided through D-Flight in the near-surface airspace, normally used by drones of small size, in order to foster the safe development of the sector.

Geographic zones

As of now, no geographic zone has been published in Italy. Vertical and horizontal boundaries of U-space airspace, relevant drone geographic zones and static and dynamic restrictions of competent authorities will be available when the services are fully implemented. As of now, user may consult the following link to collect further information (sign-up required).

As of now, Italy has not published any process for design verification.

However, it is reasonable to assume that reference will be made to the EASA's general guidance for Drone operators, manufacturers and national authorities.

Luxembourg

Operational authorizations

Luxembourg has issued 35 operational authorizations to date.

Very few operators have used Predefined Risk Assessments (PDRA), as it has proven difficult to determine what constitutes a "controlled area."

Light UAS Operator Certificates

Luxembourg has yet to receive an application for a LUC.

U-space airspace

No U-space airspace has been designated yet. Luxembourg has not yet decided whether the ANSP will serve as the exclusive USSP, or whether Luxembourg will have a federated system.

Geographic zones

Luxembourg has only three categories of geographic zones due to its relatively small size.

Netherlands

Operational authorizations

At this time, 190 operators have been issued a single license that is good for multiple operations.

Most operators are using Predefined Risk Assessments.

Standard scenarios

The Netherlands used three national standard scenarios based on SORA, but is no longer using these, as the CAA is converting to the EASA standard scenarios.

Light UAS Operator Certificates (LUC)

The CAA has issued one LUC and two applications are pending. The CAA has published no guidance other than what EASA has developed.

U-space airspace

The CAA is still considering how to structure U-space and how to set up the architecture and financing. The ANSP may want to be a USSP, but it will need to establish a separate legal entity to do so. No U-space airspace has been designated yet and not is likely this year. However, the Port of Nottingham serves as a trial area for U-space.

Romania

Operational authorizations

Romanian CAA has issued only 20-25 operational authorizations to date in the specific category. Authorizations are issued in a digital format.

Standard scenarios

Many operators in Romania are using the Standard Scenario.

Light UAS Certificate

Romania has not yet issued any Light UAS Operator Certificate.

U-space airspace

Romania has not yet decided whether the ANSP will serve as the only USSP for U-space airspace or whether there will be a federated system of USSPs. No U-space airspace has been designated to date.

Geographic zones

Geographic zones are published by the CAA, and maps of geographic zones are available on the CAA website. Requests to operate over a geographic zone must be approved by the Ministry of Defense and Ministry of Transport. The City of Bucharest is a geographic zone.

Spain

Operational authorizations

Spain has issued about 30 operational authorizations, which includes authorization of swarm operations. Only three operators to date have used an EASA Predefined Risk Assessment (PDRA).

Standard scenarios

About 5,000 Standard Scenario declarations have been submitted to date. AESA developed two standard scenarios similar to the two developed by EASA, such that the transition of operators to the EASA standard scenarios should not be difficult. The two AESA standard scenarios replaced the C-marking requirement with other requirements, such as an added distance and MTOM limit of 10 kg for STS-01 and added distance, a height limit and NOTAM requirements for STS-02.

Light UAS Operator Certificates

Spain has received about 17 LUC applications but has not yet issued an LUC. AESA has published guidance, which EASA is reviewing.

Design verification

To date, no operator is conducting flights pursuant to a design verification.

Industry Focus: Real estate

As commercial uses for drones increase, so too do the opportunities on the horizon for real estate developers and property owners. Developers and owners have been using drones for many years to inspect construction sites, produce topographical photographs and detect issues within buildings after completion. The new opportunities lie in using the land - and the air – to facilitate and profit from drone delivery.

Drone delivery is yet to become a reality in many countries around the world, despite pioneering efforts by companies like Zipline, Wing and Amazon. The reasons for this are many, but are largely due to nascent regulatory frameworks to enable large scale autonomous, BVLOS operations and public acceptance issues.

The coming of drone delivery is inevitable, and property developers and owners are well-advised to plan for it now. Property developers and owners should consider installing infrastructure to support drones on their lands and buildings, in terms of the roof (or other) space required, charging and storage facilities and sufficient network connectivity in the area. Not only would encouraging drone delivery hubs in commercial real estate developments generate new revenue streams for property owners, increased use of the land and air ensures that the area is relevant to the community and provides traffic to all neighbouring businesses.

Delivery by drone presents one of the most significant business opportunities for buildings located near airports, shopping malls, downtown and community centres.

Japan

Overview

In 2015, the Civil Aeronautics Act[54] (CAA) was amended to regulate the operation of drones in Japan, introducing a new definition of "Unmanned Aerial Vehicles" (UAVs) in the CAA. This was the first regulation of drones in Japan in response to a high-profile incident that occurred in the same year when a drone infiltrated the premises of the Japanese Prime Minister's Official Residence, eventually landing on the helipad on its roof.

Drone laws in Japan have rapidly evolved since 2015, reflecting both business needs to expand drone operations and security threats that drones potentially pose. In 2018, the Ministry of Land, Infrastructure, Transport and Tourism (MLIT) amended the standards for issuing permission for certain drone operations (subordinate legislation to the CAA), enabling the BVLOS operation of drones without the assistance of observers over areas where a third party does not enter. In both 2020 and 2021, with the aim of realizing the BVLOS operation of drones over cities without the assistance of observers, a few key regulations were added under the CAA, which became effective in 2022. More specifically, mandatory drone registration requirements took effect on June 20, 2022, followed by the introduction of a drone pilot certification system and airworthiness requirements for individual drones, which came into effect on December 5, 2022.

Separate from the CAA, the Drone Regulation Act was enacted in 2016. This law prohibits (unless prior permission is obtained) the operation of drones over and in vicinity of certain facilities, including, but not limited to, the Imperial Palace, the Prime Minister's Official Residence, the National Diet Building and nuclear power plants. In 2019 and 2022, a list of prohibited facilities under this law was expanded to include military bases (including U.S. military bases in Japan) and certain major airports. As a result, drone operation is now prohibited over a substantial part of central Tokyo.

54 This official translation has not reflected recent amendments regarding drone regulation.

VLOS and BVLOS regulations

Government agencies with jurisdiction over drones	Region this agency covers. (e.g., entire jurisdiction or province/ state.)	Role of the agency
Ministry of Land, Infrastructure, Transport and Tourism	Japan	Regulation of drones under the CAA (e.g., issuing permits for certain types of drone operation, managing drone registration and drone pilot licensing and certification).
National Police Agency	Japan	Implementation of Drone Regulation Act, including issuing permits to operate a drone over prohibited facilities under this Act.
Japan Transport Safety Board	Japan	Investigation of accidents and incidents involving drones.

Under the amended CAA, which became effective on December 5, 2022, drone operations (except those that involve drones that weigh less than 100 g) fall under one of three categories (namely, Category I, Category II and Category III)[55] depending on the potential risks it poses to persons, property or manned aircraft. The two factors that determine the operation category are Specified Flight and Entry Control Measures.

Specified Flights

Drone operations in certain airspaces or under certain conditions are categorized as "Specified Flight" under the CAA[56] as detailed below (as can be observed, BVLOS operation always falls under Specified Flight).

Airspaces[57]

- In the vicinity of airports;
- At or above 150 m AGL; and
- Over densely populated areas.

Conditions[58]

- Night operation;
- BVLOS operation;
- Operation less than 30 m from persons or property;
- Operation over certain major events;
- Operation for carrying hazardous materials; and
- Operation for dropping objects.

Entry Control Measures

Entry Control Measures are defined as appropriate measures to prevent a third party (i.e., a person other than the drone pilot or his/her assistant(s)) from entering the area below the flight path of the drone.[59] These measures include (but are not necessarily limited to) deploying assistant observers to the area below the flight path and establishing a no-entry zone.[60]

55 This categorization is well recognized although these three categories are not explicitly stated in the CAA.

56 Article 132-87 of CAA.

57 Article 132-85, Paragraph 1 of CAA.

58 Article 132-86, Paragraph 2 of CAA.

59 Article 132-85, Paragraph 1 of CAA

60 Article 236-70 of Regulation for Enforcement of the Civil Aeronautics Act (a subordinate legislation of CAA) (the CAA Regulation).

Category III operations

Category III pertains to drone operations falling under Specified Flight without taking Entry Control Measures (e.g., BVLOS operations over cities without deploying assistant observers). Accordingly, this category is the most strictly regulated of the three categories, requiring the operator to meet all of the three conditions explained below.

First, the drones used in Category III operations must have a first-class airframe approval issued for that individual drone[61] (i.e., a first-class type approval issued for that type of drone does not suffice).[62] The standards to be eligible for first-class airframe approval are generally higher than that for second-class airframe approval.

Second, the drone operator must have a first-class drone pilot certificate.[63] The certification requirement is further explained in a later section.

Lastly, drone operation falling under Category III requires the MLIT's approval.[64] The MLIT examines the operator's ability to manage the drone operation properly before issuing an approval.[65]

Category II operations

Category II is for drone operations falling under Specified Flight while taking Entry Control Measures. Typical examples of Category II operation are (i) BVLOS operations over a mountain or a lake, (ii) VLOS operations over a major event where the organizer of the event sets up areas where the audience is prohibited from entering and (iii) the VLOS operations at night over private land.

Unlike Category III operations, some of Category II operations do not require MLIT's approval for each flight if the operation meets all of the three conditions, which are:

a. The drone has first-class or second-class airframe approval;

b. The operator has a first-class or second-class drone pilot certificate; and

c. The weight of the drone is less than 25 g.[66]

However, whether or not this exemption of the requirement of MLIT's approval is applicable depends on the type of drone operations. Among the examples of typical Category II operations, this exemption is applicable to BVLOS operations over a mountain or a lake and the VLOS operations at night, but is not applicable to VLOS operations over a major event.[67]

If this exemption is not applicable, Category II operations still require MLIT's approval.[68] MLIT, similarly to Category III operations, examines the operator's ability to manage drone operations properly prior to issuing an approval. However, MLIT can omit some items of the examination if the requirements (a) and (b) above are met (i.e., the drone has airframe approval and the operator has a drone pilot certificate).

61 Article 132-13 of CAA.

62 However, some of the inspections required for issuing first-class airframe approval can be omitted if the drone has first-class type approval (Article 132-13, Paragraph 5 of CAA).

63 Article 132-42 of CAA.

64 Article 132-85, Paragraph 2 and Article 132-86, Paragraph 3 of CAA.

65 Ibid.

66 Article 132-85, Paragraph 3 and Article 132-86, Paragraph 4 of CAA; Article 236-73 of the CAA Regulation.

67 Ibid.

68 Article 132-85, Paragraph 2 and Article 132-86, Paragraph 3 of CAA.

Category I operations

Category I pertains to drone operations that do not fall under either Categories III or II (i.e., drone operations that do not fall under Specified Flight). A typical example of Category I operations is a VLOS operation during the daytime over a mountain and below 150 m AGL.

Category I operations do not require approval from MLIT even if the drone utilized in the operation does not have airframe approval and/or the operator does not have a drone pilot certificate.

Liability

Criminal liability

Causing a drone accident can have criminal consequences (though most likely for the drone operator personally rather than the business or person who hires them). By way of example, when a drone operator negligently crashes a drone, injuring a person on the ground, the operator can be punishable by a fine of up to JPY300,000.[69] The punishment can be more severe if the drone operation is business-related, in which case, a drone operator theoretically can face imprisonment.[70] A drone operator also can be punishable by imprisonment if the operator obstructs the business of another person (e.g., interrupting a game by flying a drone over a major sport event).[71]

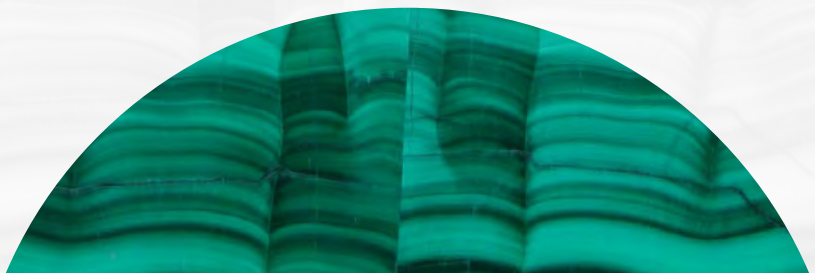
Separately, non-compliance with drone regulations provided in the CAA or in the Drone Regulation Act can also result in criminal liability. Below are several examples of such regulations.

- Under the Drone Regulation Act, a drone operator is punishable by imprisonment for up to one year or a fine up to JPY500,000 if the operator (i) flies a drone over a prohibited zone (e.g., Imperial Palace) or (ii) does not follow a police officer's order against the operator to retract a drone from the vicinity of a prohibited zone.[72]
- Under the CAA, a drone operator is punishable by imprisonment for up to one year or a fine of up to JPY300,000 if the operator flies a drone over a public place under the influence of alcohol or drugs that can impair the operator's ability to fly a drone normally.[73]
- Under the CAA, a drone operator is punishable by a fine of up to JPY500,000 if the operator conducts Category III or Category II operation without obtaining the appropriate permission from MLIT.[74] In this case, the business entity or the person who hires the operator is also punishable.[75]
- Under the CAA, a drone operator is punishable for a fine of up to JPY300,000 if the operator fails to report a certain type of drone accident or if the operator files a false report of such drone accident.[76]

Civil liability

Causing a drone accident can also result in civil liability. In the event where a drone operator negligently crashes the drone, injuring a person or damaging property on the ground, the operator is required to compensate the damage incurred by the injured person or the owner of the property.[77] In most cases, the business or the person who hires the operator is also jointly and severally liable to the injured person or the owner.[78]

69 Article 209 of Penal Code.
70 Article 211 of Penal Code.
71 Article 234 of Penal Code
72 Article 13 of Drone Regulation Act.
73 Article 157-8 and Article 132-86, Paragraph 1, Item 1 of CAA.
74 Article 157-9 of CAA
75 Article 159 of CAA.
76 Article 157-10, Paragraph 2 of CAA
77 Article 709 of Civil Code.
78 Article 715 of Civil Code.



Separately, a drone manufacturer or a drone importer may be liable under the Product Liability Act for any harm suffered by persons or property caused by a defective drone.[79] This gives rise to a claim in strict liability, and thus does not require any negligence on the part of the manufacturer or the importer. A drone is considered to be "defective" when it contains a design defect, a manufacturing defect or inadequate instructions or warnings.

Data privacy and security

Data privacy

In Japan, data privacy and security law largely is governed by the Act on the Protection of Personal Information (APPI).[80] While APPI does not specifically address drone operation, the APPI is applicable to certain types of drone activity.

More specifically, under the APPI, an image of the face of a person is protected as "personal information."[81] Accordingly, if a drone captures a video or an image that contains faces of persons which can be individually identified, the drone operator is deemed to be collecting personal information.

In this connection, however, not all drone operators are subject to the APPI's regulations even if they collect personal information; the drone operator is subject to the APPI's regulations only if they create a database that contains searchable personal information.[82] If the drone operator is subject to APPI's regulations, they must take measures prescribed under the APPI including, among other things:

i. Specifying the purpose of utilizing the personal information;[83]
ii. Notifying such purpose to any individual identified by the personal information (or alternatively, disclosing such purpose to the public);[84]
iii. Not utilizing the personal information beyond the purpose it has specified or disclosed;[85] and
iv. Not transferring the personal information to a third party.[86]

Portrait rights / Privacy rights

Certain drone activities, such as the capturing of a video or an image from the above, can infringe the portrait rights or privacy rights of individuals. Rights over one's own portrait and privacy rights are protected under the Constitution of Japan, and elaborated by relevant case law. Generally speaking, privacy rights are protected in relation to personal matters that people generally do not wish to be known, disclose or publicize. However, as of yet, there exist no clear criteria or rules defining privacy zones. To determine whether or not an invasion of privacy exists, the relevant court cases analyze factors such as the importance of the claimant's privacy interest and the legitimate needs by the defendant to disclose the claimant's private facts.[87]

Turning to drone-specific regulations, while not legally binding, the Ministry of Internal Affairs and Communications issued the "Guidelines for Handling Videos Taken by Drones on the Internet"[88] in 2015. These guidelines recommend, in the context of drone photography, the taking of certain measures to protect privacy and portrait rights. More specifically, it recommends (i) taking into consideration the shooting angle in order to avoid

79 Article 3 of Product Liability Act; note a seller or a distributor of such defective drone is generally not liable under Product Liability Act of Japan although they may be liable for contractual claims brought by the buyer.

80 Note this official translation is tentative and has not reflected recent amendments.

81 Article 2, Paragraph 1, Item 1 of APPI.

82 Article 16, Paragraph 1 of APPI; note that "searchable personal information" here is not necessarily limited to personal information collected through drone operation. If a drone operator creates a searchable database of business cards, they are subject to APPI's regulation even if they do not create a database of persons' faces captured through its drone operation.

83 Article 17, Paragraph 1 of APPI.

84 Article 21, Paragraph 1 of APPI; certain exceptions apply.

85 Article 18, Paragraph 1 of APPI; certain exceptions apply.

86 Article 27, Paragraph 1 of APPI; certain exceptions apply.

87 Sup.Ct. Feb. 8, 1994, no.48, 2 Minsyu 149.

88 No official English translation is available.

capturing images in a residential area and (ii) the blurring of images of persons' faces and personal items when these can be used to infer the living conditions of said individuals (e.g., from shots showing indoors, license plates or laundry).

Unmanned traffic management

Japan has been developing a UTM system with the aim of realizing BVLOS drone operations over cities. Currently, the government plans to start the operation of an advanced UTM system around 2025, which will enable multiple operators to conduct high-risk drone operations within the same airspace at the same time. In parallel with this, it is also looking into standard technical specifications to be used to connect multiple UTM systems developed by different providers.

Separately, the amendments to the CAA, which became effective on June 20, 2022, introduced mandatory drone registration requirements. Under these requirements, all drones of 100 g or more, unless an exemption applies,[89] must be registered with the MLIT.[90] The information to be registered includes, among other things, the type of the drone, the manufacturer of the drone and the name and the address of the owner.[91] Upon the completion of the registration, the MLIT can issue a registration number to each registered drone, which must be displayed on its airframe.[92]The registration is valid for three years.[93] The amendment to the CAA also requires, unless an exemption applies, drones of 100 g or more to be equipped with a remote identification system.[94]

Counter-drone technology

The Drone Regulation Act authorizes the police (or alternatively the Japan Self-Defense Force or the Japanese Coast Guard, as the case may be) to take necessary measures to protect a designated facility (e.g., the Imperial Palace) from drone flyovers or from drones flying in their vicinity.[95] This law explicitly allows the police to obstruct the flight of the drone and to destroy the drone if necessary.[96] In line with this directive, in 2019 the police acquired jamming devices and obtained the necessary permission allowing them to operate the jamming devices under the Radio Waves Act from the Ministry of Internal Affairs and Communications (the MIAC).[97] The police also reportedly operate interceptor drones that can capture a drone by trapping it with the help of a net hung from an interceptor drone.

On the other hand, the civil use of counter-drone technology is generally considered illegal or, at least, not practical. As for jamming devices, their operation requires permission under the Radio Waves Act granted by the MIAC. We understand, however, the MIAC would not readily give permission for the civil use of jamming devices for counter drone purposes. Separately, physical disruption of a drone can have criminal consequences. It generally falls under damage to property under the Penal Code[98], and can be justified mainly in terms of self-defence or defense of others, which requires a case-by-case analysis.

89 A drone is not required to be registered for R&D or test flight purposes.

90 Article 132-2 of CAA.

91 Article 132-4, Paragraph 1 of CAA.

92 Article 132-4, Paragraph 3, and Article 132-5, Paragraph 1 of CAA.

93 Article 132-6, Paragraph 1 of CAA, Article 236-8, Paragraph 1 of CAA Regulation.

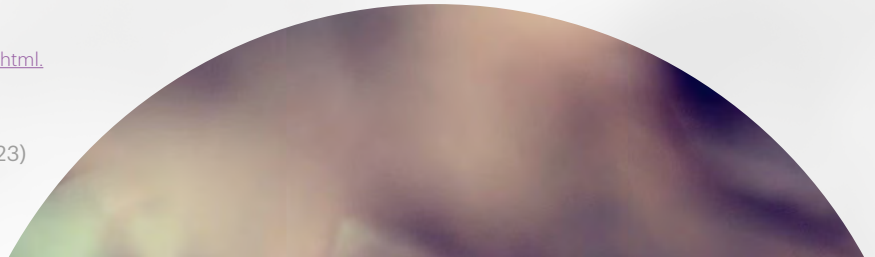
94 Article 132-5, Paragraph 1 of CAA, and Article 236-6, Paragraph 1, Item 2 of CAA Regulation; This requirement does not apply to drones registered on or before June 20, 2022.

95 Article 11 of the Drone Regulation Act.

96 Ibid.

97 https://www.asahi.com/articles/ASM4D3D0CM4DUTIL00B.html.

98 Article 261 of Penal Code.



Drone operator qualification requirements

The amendments to the CAA of 2021, which became effective on December 5, 2022, introduced a drone pilot certification system. This consists of a two-tier drone pilot certification regime, namely, that of first-class drone pilot and that of second-class drone pilot.[99] To become a drone pilot, a person must pass (i) a medical check, (ii) a knowledge test and (iii) a practical test.[100] A certificate is valid for three years.[101]

This two-tier certification system dovetails with the parallel categories that govern the operation of drones. More specifically, Category III operations (e.g., BVLOS operations over cities without deploying assistant observers) require an operator to have a first-class drone pilot certificate. When first-class drone pilots use drones with a first-class airframe approval in their operations, the MLIT may also issue permission to operate Category III flights.[102]

Turning to Category II flights, having a second-class drone pilot certificate may reduce the regulatory burden for the operator. More specifically, some types of Category II flights (e.g., BVLOS operations over a mountains or lakes using a drone that weighs less than 25 kg) do not require the MLIT's permission for flights if the operator meets both of the followings: (i) the operator has a second-class (or first-class) drone pilot certificate; and (ii) the drone used in the operation has been granted second-class (or first-class) airframe approval.[103] In this connection, Category II flights are still possible without a second-class drone pilot certificate by obtaining the MLIT's permission for the flight.[104]

No drone pilot certificate is required for a Category I flight (e.g., a VLOS operation during the daytime over a mountain and below 150 m AGL), or for the operation of drone that weighs less than 100 g (the latter of which does not fall under the definition of "UAVs" under the CAA).

Developments

For purposes of realizing Category III flights (e.g., BVLOS operations over cities without deploying assistant observers), the MLIT issued a first-class type approval for the first time and conducted its first knowledge/practical tests for first-class drone certificate in early 2023, both of which are perquisites for Category III flights under the amended CAA that came into effect on December 5, 2022. These efforts culminated on March 24, 2023, when the first Category III flight was conducted, delivering cargo over a residential area in western Tokyo. The Category III flights will likely expand their operation scope and become permitted in operations over congested areas that are conducted by multiple drones.

Separately, a guideline to promote drone operations over rivers is scheduled to be published in 2023.[105] This will make agricultural use of drones more efficient, by enabling the operation of drones over multiple and dispersed agricultural plots that are connected by a river. Previously, this type of drone operation was typically conducted separately for each agricultural plot, when the plots of different owners were interspersed with one another in a patchwork. The new guideline allows plot owners to fly drones over the rivers adjacent to such patchworks in order to circumnavigate this problem and simplify the drone operations.

99 Article 132-42 of CAA.

100 Article 132-47 of CAA.

101 Article 132-51, Paragraph 1 of CAA.

102 Article 132-85, Paragraphs 1 and 2, and Article 132-86, Paragraphs 2 and 3 of CAA.

103 Article 132-85, Paragraph 3 and Article 132-86, Paragraph 4 of CAA.

104 Article 132-85, Paragraph 4, Item 2, and Article 132-86, Paragraph 5, Item 2 of CAA.

105 Ibid.

Korea

Overview

From 1961 until 2017, Korea's aviation industry was managed under a single legislative act, the *Aviation Act*. But incorporating all aviation-related laws into a single piece of legislation made adapting to the activities of the fast-evolving aviation industry challenging. Recognizing this, in 2017 the Aviation Act was divided into *the Aviation Safety Act* (the Act), *the Aviation Business Act* and *the Airport Facilities Act*.

Like many other jurisdictions, increasing use of drones by civilians and in business applications has presented South Korea with growing regulatory challenges. Legislative regulation of drones was first implemented in Korea by amendment of the Act in 2012. But recognizing that the regulations were lagging behind advances in the drone industry, changes to regulations governing drone use have occurred since that time. Recent developments include the initiation of various drone-related projects and a shift toward stricter regulations by Korean government agencies.

The *Act* required a user/pilot to assess the empty weight (excluding fuel weight but including battery weight) of the drone and the commercial nature of its use to determine whether the drone and the pilot were subject to additional regulatory requirements. Under the then-existing rules, a non-commercial unmanned powered aerial vehicle with an empty weight of 12 kg or less (referred to as an Ultra-light Vehicle in the Act) was subject to almost no regulation. The pilot of an Ultra-light Vehicle was not required to i) register the drone, ii) obtain a drone pilot license, or iii) subscribe to any insurance coverage.

That has now changed, as new enforcement rules have been added to the Act. These rules, implemented on January 1, 2021, demonstrate the government's intention to tighten the requirements for operating drones. The weight requirement is now assessed based on the drone's maximum take-off weight. A non-commercial user with a drone weighing between 250 g to 2 kg must register the drone and complete an online course, and a non-commercial user with a drone weighing more than 2 kg is required to obtain a drone pilot license. For a commercial user, the user license requirements are the same as non-commercial users, but all drones must be registered regardless of their weight. Such a shift toward more stringent requirements naturally has increased the variety of compliance mechanisms and requirements for approvals.

The South Korean government has also taken measures to standardize drone insurance policies. Drone insurance was previously sold as a separate clause of general liability insurance, resulting in inconsistent interpretations among insurers. To address this issue, in January 2023, the Ministry of Land, Infrastructure and Transport set a new standard for drone insurance terms through the public-private drone insurance council. The new standards, now adopted by ten major Korean insurance companies, include clauses for high-risk drones in transportation and rental industries, allowing policyholders to pay lower premiums. The Ministry has also specified which items will not be covered and provided clear definitions of what is considered a liability for damages. The goal of this move is to enhance protection for policyholders and citizens, increase coverage predictability, and promote growth in the drone industry.[106]

Additionally, as part of an effort to tighten regulations, the Korean government recognized the need for a more centralized approach to regulate and support drone technology development. In 2019, the *Act on Promotion of Utilization of Drones and Creation of Infrastructure* was enacted (the *Drone Act*), to go into effect in May 2020. The Drone Act requires the government to establish and renew a five-year master plan aimed at developing the drone industry. Since the Drone Act came into force in May 2020, funding of US$33.7 million has been allocated to promote the development of drone technologies.[107] In November 2020, the Ministry of Public Administration and Security signed a business agreement with seven partnering public and private institutions to create a drone-based emergency response system,[108] and in February 2021, the Ministry of Land, Infrastructure, and Transport designated 33 areas as deregulated zones for drone technology development.[109]

106 http://stock.mk.co.kr/news/view/6278.

107 https://english.etnews.com/20201218200003.

108 http://www.safetimes.co.kr/news/articleView.html?idxno=88047.

109 https://www.yna.co.kr/view/AKR20210210029700530?input=1195m.

In June of 2022, the Korean government announced its intention to utilize drones in the public sector by adding two new provisions to the Drone Act. Later, in November of the same year, another provision was added which mandates the establishment and operation of a "drone information system" by the Minister of Land, Infrastructure and Transport to ensure the safe usage of drones. This new provision is significant because the drone information system must contain comprehensive data on accidents, insurance, pilot certification, business registration, and other relevant information as determined by Presidential Decree. Furthermore, the Minister has the authority to request necessary data or information from relevant agencies and organizations to establish and maintain the information system.

The government's commitment to promoting and improving drone technologies can be further evidenced in the following developments:[110]

- In December 2021, the Korean government published "Plans to Strengthen the Drone Industry's Competitiveness" (the Plan) to promote its measures to secure international competitiveness in the drone market.[111] The Plan aims to push the Korean drone market to be one of the seven leading drone markets in the world (currently within the top ten) by discovering 20 successful drone commercialization models by 2025 and expanding the domestic market size to approximately US$700 million.
- In September 2022, the Ministry of Land, Infrastructure, and Transport announced that it will be receiving additional applications to expand deregulated zones for drones.[112] This second RFP looks to expand the already existing 33 deregulated zones.

It is also important to understand that because South Korea technically is still at war with North Korea, albeit under a ceasefire, additional regulatory complexity exists stemming from the fact that many defense sites, scattered throughout the country, are restricted from use by civilians. To clarify the conditions of use, government agencies began implementing simpler and faster methods for granting licenses and approvals for drone use. The Ministry of Land, Infrastructure, and Transport created an app named Ready to Fly, which shows all the restricted areas and conditions of flight. The Ministry of National Defense launched a website simplifying the process for obtaining an authorization to conduct aerial photography.

110 Article 9(2): The Minister of Land, Infrastructure and Transport shall establish and operate a drone information system... and shall request necessary data or information from the relevant agencies, local governments, public institutions... for the establishment and operation of the information system.

111 https://www.korea.kr/news/policyNewsView.do?newsId=148896841.

112 https://www.korea.kr/news/policyNewsView.do?newsId=148905899#goList.

VLOS and BVLOS regulations

Government agencies with jurisdiction over drones	Region this agency covers (e.g., entire jurisdiction or province/ state)	Role of the agency
Korea Transportation Safety Authority	All South Korea	Conducts on-site inspection and imposes penalties (business registration revocation, suspension, and fines)[113]
Regional Offices of Aviation	Provinces	Registration of aviation business licenses, issuance of safety certifications (only required for drones weighing more than 25 kg), and other related drone business and safety management tasks[114]
Korean Institute of Aviation Safety Technology	All South Korea	Issues safety certifications (only required for drones weighing more than 25 kg)
Ministry of National Defense	All South Korea	Approves flights, approves aerial photography

Regulatory oversight via the drone laws in Korea can be largely differentiated into two categories—those regulations that apply before a flight occurs and those that apply during a flight.

Before flying a drone, the pilot must weigh the drone and determine whether the drone is subject to registration. If the maximum takeoff weight of a non-commercial drone is above 250 g (all commercial drones must be registered regardless of their weight) it must be registered at the Korea Transportation Safety Authority (the KTSA). Once the drone is registered, the KTSA will issue an identification sticker that must be placed, and always appear, on the drone. During or after the registration, the pilot will also need to obtain a relevant pilot license at the KTSA. The type of license required depends on the takeoff weight of the drone. Heavier drones require passing written and practical exams, as well as more extensive flight practice hours, under the supervision of a recognized teaching institution.

Registration of a drone, placing the identification marker and obtaining the necessary pilot license allows a user to fly the drone. However, before flying the drone, the pilot must confirm that he/she will not be flying within a no-fly zone. As mentioned above, information concerning unauthorized or restricted fly zones may be obtained by downloading the Ready to Fly app or obtained through a regional office of aviation. Regardless of the area in which the drone is flown, if a pilot wishes to fly a drone that weighs more than 25 kg, the pilot must obtain i) an approval from the applicable regional office of aviation and ii) a safety certification from the Korean Institute of Aviation Safety Technology.

After complying with all of the aforementioned requirements, the pilot is permitted to fly the drone. However, pursuant to Article 298 of the latest enforcement rules of the Aviation Safety Act, the pilot must ensure that the drone remains within the pilot's visual line of sight at all times (during daylight) and the drone must not fly near a densely populated

113 SOURCE: https://www.korea.kr/news/pressReleaseView.do?newsId=156540739.

114 SOURCE: https://www.korea.kr/news/pressReleaseView.do?newsId=156540739.

area. If a pilot wishes to take pictures or record videos while flying a drone, the pilot must obtain a permit from the Ministry of National Defense. In recent years, the process of obtaining approval to engage in drone photography has become easier. There is now an online approval website and an applicant is more likely to succeed in obtaining approval as regulators have become more comfortable with drones being used for this purpose.

The Ministry of National Defense will conduct an inquiry during the approval process to determine if the areas requested for photography include any restricted facilities.[115]

Liability

Criminal and civil liability

Criminal and civil liability associated with flying drones is mainly addressed by the *Aviation Safety Act* and the *Aviation Business Act*. The maximum criminal liability that may be imposed on a drone pilot is imprisonment up to three years or a fine not exceeding KRW30 million (US$26,400), and the maximum administrative penalty is an administrative fine not exceeding KRW5 million (US$4,400).

If an individual decides to make illegal video recordings or photographs while piloting a drone, possible sanctions may extend further, but under different regulatory regimes. For example, there have been increasing reports of individuals illegally recording and/or photographing others in their homes. Such criminal activity is dealt with under the *Personal Information Protection Act* and the Act on Special Cases Concerning the Punishment, etc. of Sexual Crimes. A person found guilty of breaching such laws may be imprisoned for up to seven years or a fine not exceeding KRW30 million (US$26,400).

Non-compliance with specific regulations/laws

Articles 128 and 166 of the *Aviation Safety Act*: A person operating a drone in a restricted flight area and does not have the required equipment for safe flight and rescue activities in the event of an accident is subject to a fine not exceeding KRW1 million

Articles 123 and 166 of the *Aviation Safety Act*: A person who fails to report changes to the vehicle's details, including cancellation of a vehicle's report number, to the Minister of Land and Infrastructure is subject to an administrative fine not exceeding KRW300,000.

Articles 131 and 161 of the *Aviation Safety Act*: Anyone who operates a drone while under the influence of alcohol or drugs is subject to imprisonment with labor for up to three years, or a fine not exceeding KRW30 million (US$26,400).

Articles 122 and 161(3) of the *Aviation Safety Act*: A person who fails to satisfy drone registration and filing requirements is subject to imprisonment with labor for up to six months, or a fine not exceeding KRW5 million (US$4,400).

Articles 48 and 78 of the *Aviation Business Act*: A person operating a commercial drone business (e.g., spraying pesticide or taking photographs by using a drone) without registration is subject to imprisonment with labor for up to one year, or a fine not exceeding KRW10 million (US$8,800).

Articles 71 and 80 of the *Aviation Business Act*: A person using an unregistered drone for commercial purposes is subject to imprisonment with labor for up to six months, or a fine not exceeding KRW5 million (US$4,400).

Articles 127 and 161 of the *Aviation Safety Act*: A person operating a drone within restricted airspace, without obtaining approval from the regional office of aviation and the Ministry of National Defense, is subject to a fine not exceeding KRW2 million (US$1,760).

115 https://www.korea.kr/news/policyNewsView.do?newsId=148909676&call_from=rsslink.

Articles 129 and 166 of the *Aviation Safety Act*: A person operating a drone without observing matters prescribed by the Ordinance of the Ministry of Land Infrastructure and Transport is subject to an administrative fine not exceeding KRW2 million (US$1,760). This could include:

- Flying over a densely populated area;
- Flying within a no-fly zone; or
- Flying after sunset.

Articles 124 and 166 of the *Aviation Safety Act*: A person operating a drone without obtaining the required safety certification is subject to an administrative fine not exceeding KRW5 million (US$4,400).

Articles 125 and 166 of the *Aviation Safety Act*: A person operating a drone without obtaining the required pilot license is subject to an administrative fine not exceeding KRW3 million (US$2,600).

Articles 70 and 84 of the *Aviation Business Act*: A person operating a drone without subscribing to required insurance and who fails to submit data confirming the purchase of aviation insurance or submits false data thereof is subject to an administrative fine not exceeding KRW5 million (US$4,400).

Data privacy and security

Data privacy and security in Korea generally are regulated by the *Personal Information Protection Act* (the PIPA), and location information is regulated by the Act on the Protection, Use, etc., of Location Information. Unfortunately, privacy and security laws specifically related to drones have not been introduced yet, and the absence of specific drone laws related to data privacy and security has potentially left civilians exposed to blind spots in the law, or at least ignorant of laws that might relate to them.

Article 25 of the *PIPA* provides that "no one shall install and operate any visual data processing device so as to look into places which are likely to noticeably threaten individual privacy [...]," and Article 2 of the same *Act* provides "personal information includes information that identifies a particular individual by his or her [...] image." Article 44 and Article 45 of the *Act on Promotion of Information and Communications Network Utilization and Information Protection* (the *Information Protection Act)* provides that, "No user may circulate any information violative of other person's rights, including invasion of privacy and defamation, through an information and communications network" and a "person who manufacturers or imports devices that connect to the information and communication network shall take protective measures to secure the reliability of the information and security of the information and communications networks."

Pursuant to Article 25 and Article 2 of *PIPA,* all photographs and recordings taken by drones that show any individual's face or identifying characteristics could be in breach of the regulation and, pursuant to Article 44 and Article 45 of the *Information Protection Act,* distribution of such photographs or videos could also be prohibited. However, Article 2(7) of the *PIPA* provides that the term "visual data processing devices means [...] devices continuously installed at a certain place to take pictures of persons or images of things" and drones do not fall within this definition because drones are not continuously installed at a certain place. Therefore, an individual's privacy and security are not protected against any misuse of drones and cameras.

An individual would have to bring a claim under the breach of individual publicity/portrait rights (*Cho-sang Kwon).* It is generally understood that Article 17 (*the right and freedom to privacy)* of the Korean Constitution guarantees an individual's portrait right. However, inconsistent case precedents on portrait rights add confusion and uncertainty.

Further, from a drone pilot's perspective, confidently adhering to the current Korean rules and regulations presents a host of challenges. Practically, to avoid violations, a pilot will require at least some understanding of rules related to statutes like the *PIPA,* the *Act on the Protection,* Use, etc. of Location Information, the *Aviation Safety Act* and *Protection of Military Bases and Installations Act.* This increased probability of innocent or negligent breach of the law, and the uncertainty created by blind spots in the regulations, has made enforcement and commercial viability more difficult.

Unmanned traffic management

Korea has seen steps taken by the government and in the private sector to develop a UTM system and drone use BVLOS.

For example, in April 2017, the Korea Institute of Aviation Safety Technology (KIAST), a government agency created under the Ministry of Land, Infrastructure, and Transportation to research and develop aviation technologies, implemented a five-year project to develop a UAS (unmanned aircraft system) Traffic Management system.[116] The UAS Traffic Management project aims to design and establish a low altitude unmanned aerial vehicle traffic management system that supports safe and efficient operation of unmanned aerial vehicles. This project was conducted in conjunction with various other private companies and national institutions, such as Korean Telecom, Metabuild Co., Ltd., Uconsystem Inc, Davo E&C, BluezenDrone Co., Ltd., Seoul National University, Korean Aerospace University, Korea Advanced Institute of Science and Technology and Korea Aerospace Research Institute. In addition to the UAS Traffic Management project, KIAST has set up a support hub for drone businesses to promote and nurture the domestic drone industry. KIAST provides labs, test sites, office space, marketing and funding for drone-related start-ups.[117]

On November 5, 2020, the Ministry of Public Administration and Security signed a business agreement with seven partnering entities and institutions[118] (Seongnam City, Seongnam Fire Station, Bundang Fire Station, 55th Division of the Korean Army, Sujeon Police Station, Jungwon Police Station and SK Telecom) to create an emergency drone-based multi-control system. The system aims to deploy drones to emergency sites to provide real-time accurate information and reduce the average emergency response time. A fund of US$443,000 has been dedicated to this project, and completion was expected to be around December 2021. There has been no further news or development information reported on this project.

On December 17, 2020, the Ministry of Science and ICT announced that a five-year fund of US$33.7 million has been designated for the development of drone-related technologies, such as counter-drone technology, an emergency report system and an autonomous BVLOS system.[119] Because confirmation of the fund occurred relatively recently, specific details regarding how the fund will be allocated and progress made to date has not yet been reported.

On December 2020, drones developed by Pablo Air successfully shipped medical supplies to two islands. The drones flew from Inchon New Port (management pier) to Yeongheungdo Island and Jawoldo Island, a 50-mile round trip journey in one hour and 20 minutes.[120] Founded in 2018, Pablo Air is one of the leading developers of unmanned aerial software and hardware. Its core business is the development of drone swarm platforms and related solutions. In 2019, Pablo Air's potential was recognized by Lee Soo-man, the chief producer of SM Entertainment, and the company secured KRW3 billion in Series A funding. Pablo Air attracting such interest also could be seen as evidence of the private sector's growing interest in drone technology.

In July 2022, the Ministry of Land, Infrastructure, and Transport announced that the government is drafting a bill to set up guidelines to enable the commercialization of drones as an urban transportation system.[121] Once passed, this will be the first legislation to regulate a drone transportation system in the world.

116 https://www.kiast.or.kr/en/sub06_02.do.

117 https://www.kiast.or.kr/en/sub06_03.do.

118 http://www.safetimes.co.kr/news/articleView.html?idxno=88047.

119 https://english.etnews.com/20201218200003.

120 https://www.unmannedairspace.info/latest-news-and-information/three-different-communication-technologies-used-for-korean-50-mile-bvlos-flight/.

121 https://pulsenews.co.kr/view.php?year=2022&no=665844.

Counter-drone technology

Increased accessibility of drones has exposed civilians to greater danger created by negligent or malicious use of drones. Growing concerns have initiated government agencies to develop/import counter-drone technology with domestic and foreign companies.

In May 2018, Department 13, a Maryland-based unmanned-aircraft mitigation specialist company, agreed to an exclusive distribution deal to sell counter-drone technology in Korea.[122] The distribution deal was made so Department 13's anti-drone system could be distributed to the Korean military, local airports, manufacturers and corporations.

In June 2019, SK Telecom, Silla University, the 53rd Homeland Defense Infantry Division of the Korean Army and Hanbit Drone demonstrated their jointly developed anti-drone system.[123] The anti-drone system encompasses detection, identification, tracking, neutralization and removal. The demonstration showed a jamming device as one of the methods of neutralization. The jamming device is currently used by the Korean Army, but its commercial application faces further regulatory hurdles. Counter-drone measures that use jamming devices and software exploitation are regulated by the *Radio Waves Act*. Unless expressly approved by the Minister of Science and ICT, Article 58 of the *Radio Waves Act* prohibits approval of any equipment that "interferes with other communication." Therefore, under the current Korean legislation, counter-drone devices that rely on interfering with a drone's methods of communication are prohibited to civilians.
In conjunction with the development of counter-drone technology, recent amendments made to the *Airport Facilities Act* showed the legislator's awareness of the need for a counter-drone system. On December 8, 2020, Article 56 of the *Airport Facilities Act* was amended to provide that unauthorized drones flying near an airfield may be "eradicated, crashed, or captured." Unfortunately, the included wording did not differentiate or acknowledge different methods of counter-drone technology.[124]

With North Korea actively developing drones for military use, most notably deploying them to spy on South Korean military installations, South Korea's Agency for Defense Development (ADD) has been partnering with the private sector to develop counter-drone technology. In January 2022, ADD and Hanwha successfully developed and tested a counter-drone system that uses laser technology to disable hostile drones fired from portable surface-to-air equipment[125]. In February 2022, LIG Nex1 and the Korean government announced their plans to produce electronic warfare equipment to prevent North Korean drones from entering South Korean airspace.[126] The latest development came in February 2023 when the South Korean government announced their plans to phase in an "anti-drone system" to prevent drone terrorism in critical national infrastructure. The government will prioritize the implementation of the anti-drone system in critical facilities based on their importance and will also actively pursue research and development in anti-drone technology.[127]

122 https://internetofbusiness.com/department-13-agrees-south-korean-deal-for-counter-dronee-tech/.

123 https://www.electronicsweekly.com/news/business/korea-makes-anti-dronee-system-2019-06/.

124 SOURCE: https://www.korea.kr/news/policyNewsView.do?newsId=148911845.

125 https://www.unmannedairspace.info/counter-uas-systems-and-policies/south-korea-tests-directional-infrared-counter-drone-technology-from-hanwha-to-disable-incoming-missiles/.

126 https://www.kedglobal.com/aerospace-defense/newsView/ked202208220012.

127 https://www.korea.kr/news/policyNewsView.do?newsId=148911845.

Drone operator qualification requirements

Article 125 of the *Enforcement Rule of the Aviation Safety Act* identifies four different types of drone operation licenses.

Drone type	Weight	Requirements
Type 1 drone license	For drones that have maximum takeoff weight above 25 kg but below 150 kg	Must pass a multiple-choice exam, practical exam and have 20 hours of flight experience
Type 2 drone license	For drones that have maximum takeoff weight above 7 kg but below 25 kg	Must pass a multiple-choice exam, practical exam and have 10 hours of flight experience
Type 3 drone license	For drones that have maximum takeoff weight above 2 kg but below 7 kg	Must pass a multiple-choice exam and have six hours of flight experience
Type 4 drone license	For drones that have maximum takeoff weight above 250 g but below 2 kg	Must complete an online course

The above requirements are generally intended for commercial drone use. Non-commercial drones with a maximum takeoff weight below 250 g do not require any qualification of operators

Developments

Korea has seen local companies realize their vision and technology to stay ahead in the fast-growing drone market. On January 2019, Nearthlab, a drone-based wind turbine inspection company, successfully conducted a safety inspection of wind farms owned by Korea Southern Power Co., Ltd.[128] Pablo Air currently holds the record for the longest drone delivery flight in Korea, and it was the first Korean company that successfully performed a drone art show with 100 drones using swarm flight technology at the 2019 Drone Regulatory Sandbox Fair.[129] However, with over 90 percent of drones coming from overseas markets,[130] Korean companies' success in maintaining their competitiveness has been challenging. In recognition of such hardship, various types of government projects and support are being implemented.

The Ministry of Science and ICT's US$33.7 million fund is part of a five-year plan to develop drone-related technologies.[131] This 41% increase in funding, compared to the previous year, shows the government's commitment toward supporting the development of drone technology, and such commitment can be further evidenced by the recent developments made by the Ministry of Land, Infrastructure, and Transport. On February 10, 2021, the Ministry of Land, Infrastructure, and Transport (Minister Byeon Chang-heum) announced that the government will designate 33 areas nationwide as "special deregulated zones for drones."[132] The aim of assigning deregulated zones is to ensure that new drone infrastructures and services may be tested and implemented with minimum regulatory challenges. These special deregulated zones will either exempt or ease regulations on matters such as safety certifications and flight approval procedures. A total of 15 local governments are participating in this program, and each local jurisdiction plans to implement different drone services, such as environment monitoring, transportation and logistics, facility inspections, counter-drone systems, etc. Therefore, any drone-based system or technologies developed through this program will enjoy lowered regulatory hurdles and efficiency.

128 https://drive.google.com/file/d/1q7HAQB_mGDLO2g-j6E2URSXShtscppPO/view.

129 https://www.prnewswire.com/news-releases/pablo-air-becomes-the-first-korean-company-to-have-succeed-in-a-57-5-km-package-deliver-with-1-hour-and-56-minutes-flying-time-using-a-dronee-300978195.html.

130 https://www.investkorea.org/ik-en/bbs/i-308/detail.do?ntt_sn=487638.

131 https://english.etnews.com/20201218200003.

132 https://www.yna.co.kr/view/AKR20210210029700530?input=1195m.

An example of such efforts being materialized is the recent R&D corporation agreement signed between Korean Air, Incheon International Airport Corporation (IIAC) and the Korea Aerospace Research Institute (KARI) on August 5, 2021. The agreement was signed to establish a safe and efficient drone transportation management system and the three organizations will conduct joint R&D to develop Korea's first drone industry.[133] According to a report published by the Ministry of Land, Infrastructure and Transport, passenger drones are expected to be available in Korea in 2025 and autonomous drones by 2035.[134]

It is evident that the Korean government is designating increasing amounts of funding for the development of drone-related technologies and lowering barriers to entry into the drone market. The type of projects under development show that the government is focusing more on core software technology rather than hardware. This strategy appears to have taken note of recent trends in the tech industry, as well as Korea's neighboring countries which have competitive manufacturing capabilities. With the government's support, start-ups and small to medium-sized businesses will be able to develop their drone technologies more efficiently for the next few years. However, in recent years, a growing concern has been expressed over the practical implications of the innovations due to the stringent and lengthy safety testing requirements in the current legislation. There have not been any significant deregulatory developments made to the current legislation, but the government has shown its intent to do so through the expansion of the deregulated zones and selection of a Regulatory Sandbox (in April 2022, MOLIT selected nine local governments as Drone Demonstration Cities and 14 drone companies to participate in a Regulatory Sandbox).[135]

Lastly, in March 2023, the Ministry made an announcement declaring the first year of K-drone delivery. To prepare for the commercial launch of drone deliveries, the Ministry plans to integrate essential components such as a drone identification system and drone flight path into the delivery system. The primary objective of this integration is to improve the safety and efficiency of both the hardware and software used in drone delivery. The long-term goal is to promote the growth of the drone delivery industry and establish a sustainable business model.[136]

133 https://asianaviation.com/korean-air-signs-uam-research-deal/.

134 https://koreajoongangdaily.joins.com/2021/09/29/business/industry/airtaxi-passengerdronee-uam/20210929162238130.html.

135 https://www.commercialuavnews.com/regulations/the-impact-of-drones-in-south-korea-for-the-enterprise.

136 https://www.korea.kr/news/pressReleaseView.do?newsId=156557775.

JARUS

The Joint Authorities for Rulemaking on Unmanned Systems (JARUS) is an international expert group specifically focused on the drone sector. JARUS is comprised of 63 member countries who contribute experts for the development of its publications. The European Union Aviation Safety Agency (EASA) and EUROCONTROL also contribute to the development of JARUS work products. JARUS holds two Plenary Meetings each year. Its first spring plenary session was held on April 17-21, 2023.

JARUS recently reconstituted the working group structure to form four working groups: (i) operation, organization and personnel, (ii) airworthiness, (iii) safety and risk management and (iv) automation concept of operations. These working groups consult with stakeholders and produce publications aimed at providing guidance, model regulation and standards, and recommendations to national aviation authorities. These reports are subject to comment through internal and external consultation before being finally published.

JARUS mandate on drone regulations

Similar to the ICAO, JARUS focuses largely on the harmonization of regulations across national aviation authorities. Unlike ICAO, it is not an international government organization, but rather an association of experts from civil aviation authorities around the world. JARUS aims "to recommend a single set of technical, safety and operational requirements for all aspects linked to the safe operation of the Unmanned Aircraft Systems (UAS)." According to JARUS, "this requires review and consideration of existing regulations and other material applicable to manned aircraft, the analysis of the specific tasks linked to RPAS and the drafting of material to cover the unique features of UAS."

Industry Stakeholder Body

As part of its consultation process, JARUS works with the aviation industry sector through the Industry Stakeholder Body (ISB) (formerly Stakeholder Consultation Body (SCB). The ISB is a self-governing association of aviation industry organizations and companies, established to provide expertise and advice to support the JARUS Work Program, JARUS Working Groups and deliverables. ISB members represent all sectors of the aviation industry and acts as a forum to promote stakeholder interests and a platform to facilitate the creation of balanced deliverables. It works directly with JARUS through the ISB Steering Committee and working group experts.

JARUS publications

JARUS publishes a variety of guidance materials that have informed the regulatory framework adopted by nations around the globe. These publications include:

SORA (Package) and Standard Scenarios – recommends a risk assessment methodology to establish a sufficient level of confidence that a specific operation can be conducted safely.

The SORA system is accompanied by a series of Annexes:

- Annex A: Operations manual – collecting and presenting system and operations information for a specific UAS operation;
- Annex B – Integrity and Assurance Levels (SAIL) for mitigations used to reduce intrinsic ground risk classes;
- Annex C – Strategic Mitigations Collision Risk Assessment;
- Annex D – Tactical Mitigations Collision Risk Assessment;
- Annex E – Integrity and Assurance Levels (SAIL) for Operational Safety Objectives (OSOs);
- Annex F – Ground Risk Collision Model;
- Annex G – Air Risk Collision Model;
- Annex H – SORA and UTM; and
- Annex I – Glossary of Terms.

In December 2022, JARUS published for external consultation SORA version 2.5, which includes the main body and revisions to Annexes B, E, F and I, and an explanatory note addressing these revisions.

The final version on SORA 2.5 is expected by the end of 2023. Thereafter, JARUS will focus on developing a more accurate air risk model. It will update Annex C and Annex D and draft a new Annex G, Air Risk Model. SORA 3.0 will include improvements on the usability in all areas based on field experience and guidance material on achieving more international harmonization. SORA 3.0 will also include new Annex J, Notes to Aviation Authorities, with tailored training materials for authorities to apply the SORA.

CS-UAS – aims at providing recommendations for states to use for their own national legislation concerning "Certification Specification for Unmanned Aircraft Systems."

In October 2022, JARUS published for internal consultation CS-UAS Annex C, Additional requirements for UAS, which contain functions that are performed by High Complex Systems (HCS) including AI, Machine Learning, Neural Networks etc. The comment period ended on November 28, 2022.

UAS RPC CAT A and CAT B – provides recommendations to competent authorities (national authorities or Regional Safety Oversight Organisations) to use their own national legislation concerning uniform remote pilot competency for operations in the Open Category and Specific Category.

GM to JARUS recommendation UAS RPC CAT A and CAT B – provides JARUS guidance material on the qualification for an entity that a competent authority may recognise as a provider for theoretical knowledge examination and practical skill assessment.

AMC RPAS 1309 (package) – Document developed as an integral part of a type-certification process. It is a means of compliance for drones to a 1309 airworthiness requirement modeled from the US Federal Aviation Regulations.

New Zealand

NEW ZEALAND

Overview

The Civil Aviation Act 1990 (**CA Act**) and the Civil Aviation Rules (Rules) made under the CA Act currently regulate the use of drones in New Zealand. Under the Rules, most recreational and commercial drones on the market would fall under the definition of 'remotely piloted aircraft' (**RPA**) being unmanned aircraft that is piloted from a remote station and:

- Includes a radio-controlled model aircraft; but
- Does not include a control line model aircraft or a free flight model aircraft.

Drones are regulated and managed by the Civil Aviation Authority (**CAA**). Additionally, a working group, the Unmanned Aircraft Integration Leadership Group (**Leadership Group**), established in August 2018, includes members from the Ministry of Transport (**MOT**), Airways New Zealand, the Ministry of Business, Innovation and Employment (**MBIE**), as well as CAA. These government and industry bodies are involved in regulating and innovating drone technology in New Zealand.

Following the establishment of the Leadership Group in late 2019, MBIE launched a new program for Airspace Integration trials,borne with the vision to make New Zealand a location of choice for the development, testing and market validation of advanced unmanned aircraft and adjacent technologies. The program is currently planned to be carried out until 2024. The published industry partners have grown with 11 industry partners in total. Current industry partners are available here.

New Zealand's civil aviation legislation will soon be replaced by the Civil Aviation Act 2023 (**new CA Act**) which comes into force on April 5, 2025, which was introduced to the New Zealand Parliament on September 8, 2021 after a five-year review of the existing civil aviation legislation[137] to address calls from the aviation industry. The new CA Act will repeal and replace the CA Act and the Airport Authorities Act 1966 when it comes into force and, along with the new civil aviation rules that the Minister of Transport is required to create and certify by April 5, 2025, will regulate drone use in New Zealand.

The new CA Act does this by defining RPA operators as 'pilots-in-command'. At a high level, Drone Operators will have to ensure the safe operation and maintenance of the drone they are responsible for and have a duty to notify relevant actors (for example, the relevant air traffic control service or the Director of Civil Aviation) if an emergency occurs. Failure to comply with the notification requirements without reasonable excuse is an offence liable on conviction to a fine not exceeding NZ$15,000.[138]

137 Civil Aviation Bill 2021 Bill Digest.

138 Section 17 of the new CA Act

VLOS and BVLOS regulations

Government agencies with jurisdiction over drones	Region this agency covers. (e.g., entire jurisdiction or province/state)	Role of the agency
• Civil Aviation Authority of New Zealand	• Nationally	• Regulates the aviation sector, including drones
• Airways New Zealand	• Nationally	• National air navigation service provider
• Ministry of Business, Innovation and Employment	• Nationally	• Radio Spectrum Management is a sub-part of MBIE and regulates the use of spectrums and spectrum licencing in New Zealand
• Ministry of Transport / Waka Kotahi – NZ Transport Agency	• Nationally	• Regulate the transport sector, in charge of the Civil Aviation Act, rule, policy setting, and other legislative work on regulating drones

According to a recent survey conducted in June 2020 on the use of drones in New Zealand on the use of drones in New Zealand, most drone use falls under the purview of Part 101 of the Rules.

A person who operates an aircraft to which this rule applies must, at all times:

- Maintain visual line of sight (**VLOS**) with the aircraft;
- Be able to see the surrounding airspace in which the aircraft is operating; and
- Operate the aircraft below the cloud base.

Part 101 of the Civil Aviation Rules only applies to drones with a gross weight of less than 25 kg that can fully comply with the rules in Part 101. To operate any drone over this weight, and for operations that cannot comply with Part 101, the operator must be certificated under Part 102.

Under Part 101.215(b), a person must not operate a drone with a gross mass of between 15 kg and 25 kg unless the aircraft and any modification made to it is:

- Constructed under the authority of, or inspected and approved by, an approved person or organization defined in rule 101.202; and
- Operated under the authority of an approved person or organization defined in rule 101.202.

There are several key requirements under Part 101 for an operator of a drone to comply with:

- Not operate an aircraft that is 25 kg or larger and always ensure that it is safe to operate;
- At all times, take all practicable steps to minimize hazards to persons, property and other aircraft:
- Fly only in the daylight unless operation is indoors or a shielded operation;
- Give way to all crewed aircraft;
- Be able to see the aircraft with your own eyes (e.g., not through binoculars, a monitor, or smartphone) to ensure separation from other aircraft (or use an observer to do this in certain instances);
- Not fly the aircraft higher than 120 m (400 ft) above ground level (unless certain conditions are met);
- Have knowledge of airspace restrictions that apply in the area you want to operate;
- Not fly closer than 4 km from any aerodrome (unless certain conditions are met);
- When flying in controlled airspace, obtain an air traffic control clearance issued by AirShare (unless it is a shielded operation);

- Not fly in special use airspace without the permission of the administering authority of the area (e.g., military operating areas or restricted areas);
- Have consent from anyone you want to fly above; and
- Have the consent of the property owner or person in charge of the area you want to fly above.

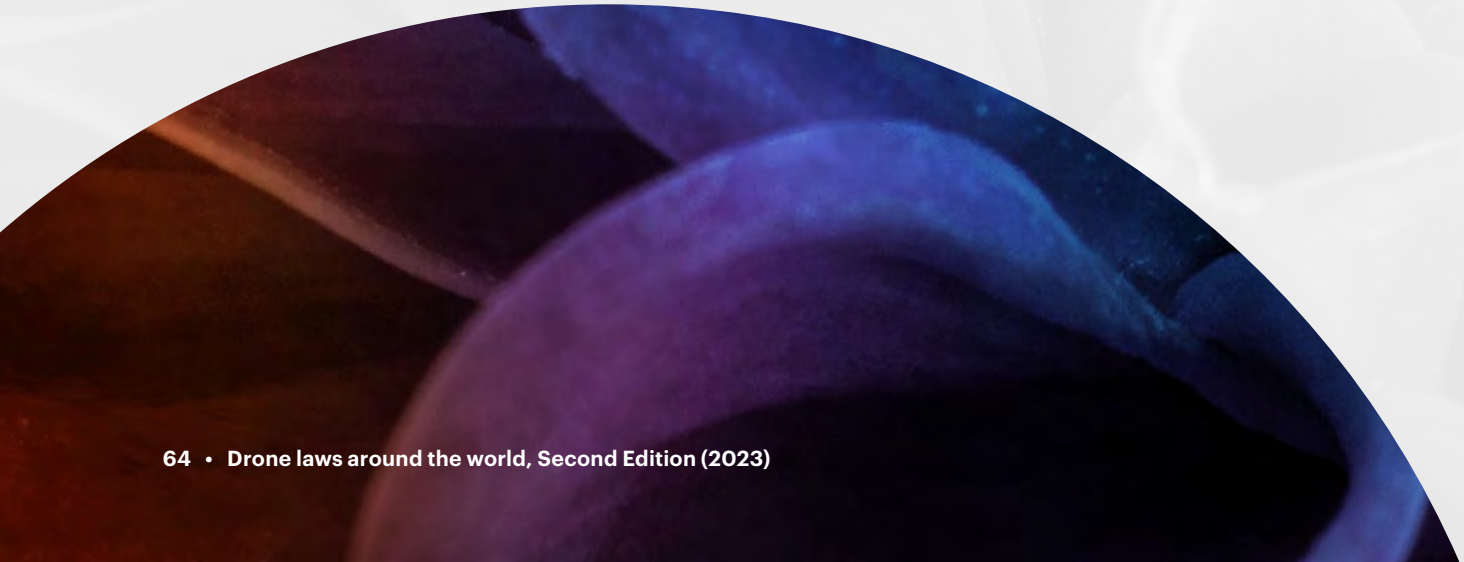
Some exemptions apply to the above, primarily if appropriate consent is obtained or the flight is under an appropriate licence, for example:

- A person may operate a drone within 4 km of an aerodrome if:
  - The operation is undertaken in accordance with an agreement with the aerodrome operator or authorization from AirShare, depending on the type of aerodome;
  - Each pilot has an observer in attendance while the aircraft is in flight; and
  - The aircraft is not operated at a height of more than 120 m (400 ft) above ground level unless the Director has approved the operator to operate the aircraft above 120 m (400 ft) above ground level;
- A person may operate over people or property if they have obtained the relevant person's consent or those affected.

BVLOS operations are not allowed under Part 101.209 of the Rules. While Part 102 of the Rules does not expressly prohibit BVLOS operations, there are several challenges presented by these types of operations that make complying with the Rules more difficult. Additionally, from the Part 102 Advisory Circular issued by the CAA in July 2015 (no updated version has been released), BVLOS operations will unlikely be approved by the CAA either. The CAA states in the circular that the standard operating environment is to operate within an unaided visual line of sight, meaning that the operator can see the aircraft without using an instrument such as binoculars or a screen. A strong safety case would have to be presented to mitigate the risks associated with BVLOS operations to make a successful application for a Part 102 Unmanned Aircraft Operating Certificate (discussed below). Features of the safety case would include:

- Identification of the airspace class to be used and associated requirements and how they will be met;
- Ability to provide separation from other traffic, such as segregated airspace or a technological solution (e.g., seek, detect and avoid systems); and
- Mitigate risk to persons, property and terrain.

Drones being flown using first-person view, or from a remote device that requires the pilot's attention, still require an observer to be present to maintain unaided VLOS with the drone under Part 101 Rules. First-person view operations without an observer are considered BVLOS operations. They require operators to address the safety case considerations of an application for a Part 102 Unmanned Aircraft Operating Certificate, as above.



Liability

Criminal liability

The legal regime in New Zealand is moving towards aligning drone technology with the law through the new CA Act. Despite the definition made under the Rules (above), the definition of 'aircraft' under the CA Act does not distinguish between drones and other aircraft. The new CA Act intends to close this gap by clarifying who is responsible for the operation and safety of the aircraft under the rules, as Pilot-in-command (PIC), which is primarily responsible, must be on board the aircraft under the CA Act. As per the new CA Act,, rules made under the Act will specify who is responsible when the PIC is not on board the aircraft. This means that once the new CA Act comes into force, drone operators—as PIC—will be held to the same duties and obligations as other PIC.

The Crimes Act 1961 covers most crimes in New Zealand, with additional crimes being held in the Summary Offences Act 1981 and other legislation. Currently, the Crimes Act 1961 and the Aviation Crimes Act 1972 do not offer explicit exceptions regarding drones. By way of example, an entity seeking to interrupt a drone that was veering too close to a rescue helicopter (unless authorized by the new CA Act as discussed above) might be liable for interfering with a computer system, arson or causing damage to an aircraft. It is also against the law to peer into people's homes and record any activity under the Summary Offences Act 1981. Most breaches of the Crimes Act, Summary Offences Act, Aviation Crimes Act, the new CA Act (once it becomes law) and the Rules would result in a fine being imposed. Still, it may be possible for other sentences, such as imprisonment or community service, to be also imposed. In 2016, a man was successfully prosecuted for operating a drone aircraft in breach of the Rules – namely, operating in controlled airspace without permission and operating a drone aircraft in a way that unnecessarily endangered people's lives. The new CA Act addresses this issue by increasing the enforcement powers of the police and CAA response officers ('Enforcement Officer'). An Enforcement Officer can detain, seize and destroy a drone if it reasonably believes the drone's operation:

- Is an offence under civil aviation legislation;
- Is an imprisonable offence under any other Act; or
- May endanger people or property.

The Crimes Act sections 216G-216J makes it an offence to record an intimate visual recording of a person without their knowledge and consent. Drones armed with cameras or other recording equipment may record people in private spaces without their knowledge. 'Recording' includes live streaming even where the recording is not saved to any hard drive. In that case, the drone operator would be liable for up to three years in prison.

Section 145 of the Crimes Act sets out the offence of criminal nuisance (an unlawful act or omission that the person knew would endanger the lives, safety, or health of the public or any individual's life, safety, or health). Inappropriate drone use that breaches the Rules, especially in controlled airspaces, could endanger the public's or individual's lives. The operator could be liable for a sentence of up to one year in prison.

The New Zealand Police have indicated that if a drone were to be used to assist a criminal act (such as surveillance, distraction, intimidation, etc.) the police would charge the drone operator with that crime. The operator would then be liable for being an accessory to the unlawful Act and face additional charges relating to drone use.

It is against the Rules to operate a drone over private property without permission. Still, a person who is not an Enforcement Officer (once the new CA Act comes into force) cannot prevent a drone from operating over their property by preventing its continued flight (shooting it down). If a person did this, it would breach provisions in the Summary Offences Act, Crimes Act and, in the case of firearms use, the Arms Act 1983.

Removing the drone from the air could cause damage to people or property by preventing the operator from having control over its flight and landing. That person could then be liable for nuisance or for endangering the lives of others.

Civil liability

Potential civil liability implications to consider concerning drones may include the following:

- Nuisance, trespass and negligence:
    - In New Zealand, a person injured in an accident may receive coverage under the Accident Compensation scheme (**ACC**) and cannot recover money from the person who caused the injury. ACC would likely cover most negligence-related incidents involving drones and personal injury. The drone operator would not be liable under tort but may still face criminal prosecution and Worksafe investigations.
    - Negligence involving property damage would be actionable in New Zealand. A drone operator could be liable for negligence where the damage to the property was reasonably foreseeable, such that the operator owed a duty of care not to damage the property. There would also need to breach that duty, causing loss. This may include drones falling and damaging property, scaring livestock and causing livestock to cause other damage.
    - Trespass is covered by the Trespass Act 1980. A breach of this Act includes trespassing onto the property after being warned to leave or stay off or any disturbance of domestic animals (including livestock) by means of a vehicle. A drone going over private land and disturbing domestic animals or the operator trespassing onto the land after a warning could result in a fine of up to NZ$1,000 or up to three months imprisonment.
- Privacy Torts:
    - New Zealand has two privacy torts: invasion of privacy by the publicity given to private facts established by the Court of Appeal in Hosking v Runting[139] and invasion of privacy by intrusion into seclusion by the High Court in C v Holland[140].
    - Invasion of privacy by the publicity given to private facts occurs when facts surrounded by a reasonable expectation of privacy are publicised in a highly offensive way to an objectively reasonable person.
    - Invasion of privacy by intrusion into seclusion requires an intentional and unauthorized intrusion into seclusion involving infringement of a reasonable expectation of privacy that is highly offensive to a reasonable person.
    - Although the elements of both torts may first appear highly relevant to drone operators, the precedents in New Zealand and other common law jurisdictions on the application of privacy torts do not yet provide clear guidance on when and how drone operations can fall under these torts.
    - Until there is New Zealand authority on the application of privacy torts to drone operations in New Zealand, filming and observation of individuals may be reasonable as long as they are not highly offensive.
- Privacy Act 2020:
    - As discussed in detail in Data Protection and Privacy section below the Privacy Act may be breached if the drone operator is an agency. If the drone is capable of making recordings, then the agency must comply with the provision of the Privacy Act in terms of telling people they are being recorded, getting consent (if necessary) and ensuring that the recordings are not released to any unauthorized person.
- Radiocommunications Act 1989 (and its associated regulations/ standards):
    - The Radiocommunications Act 1989 makes it an offence to transmit radio waves except under a spectrum licence or general user spectrum licence. Every person who commits an offence under the Radiocommunications Act or against

139 Hosking v Runting [2005] 1 NZLR 1 (CA).

140 C v Holland [2012] NZHC 2155; [2012] 3 NZLR 672.

any regulations made under it, where no other penalty is provided, shall be liable on conviction to a fine not exceeding NZ$30,000 for an individual or NZ$200,000 for a body corporate.
Where the offence is a continuing offence, a further fine not exceeding NZ$1,000 per day for the period the offence continues may be imposed.

Non-compliance with specific regulations/laws

Civil Aviation Act 1990 – governs New Zealand's civil aviation system and sets the overall framework for aviation safety, security and economic regulation. The Act outlines offences and penalties, which include operating an aircraft in a careless manner and trespass, which may also apply to drones.

With the expansion of the PIC definition to include operators of drones (as per the new CA Act), new offences will extend to operators of drones.

Under the new CA Act, it is a strict liability offence to:

- Carelessly operate any aircraft, subject to a fine of up to NZ$30,000 for individuals and NZ$100,000 for other persons;
- Operate, maintain, or service an aircraft, do any other act in respect of an aircraft (or cause others to do the same) in a manner that causes unnecessary danger to any other person or any property, subject to a fine of up to NZ$150,000 for individuals, and NZ$1,500,000 for other persons (acting recklessly doubles the fines and individuals are also subject to imprisonment for up to 5 years);
- Intentionally operate an aircraft without reasonable excuse in controlled airspace or restricted area, and with the knowledge or recklessness as to whether appropriate authorization is held or not, subject to a fine up to three month imprisonment and/or NZ$10,000 fine for individuals, and up to NZ$100,000 for other persons;
- Provide false information (knowingly or recklessly) regarding the safety of an aircraft, subject to a fine of up to 12 months imprisonment and/or NZ$120,000 fine for individuals and up to NZ$1,000,000 for other persons;
- Fail (by the PIC) without reasonable excuse to comply with the notification requirements in the event of an accident or incident as defined by the new CA Act, subject to a fine of up to NZ$30,000 for individuals and NZ$100,000 for other persons.
- Fail (by the PIC) without reasonable excuse to comply with the notification requirements regarding breaches of civil aviation legislation that are committed during an emergency, subject to a fine of up to NZ$15,000; and
- Fail (by the operator of an aircraft) without reasonable excuse to provide identifying information of the PIC, subject to a fine of up to NZ$30,000 for individuals and NZ$100,000 for other persons.

Additional offences for breaches of the Rules can also be prescribed under regulations.

Non-compliance with the Civil Aviation Rules is a strict liability offence and may result in the enforcement of fines, as prescribed under Schedule 1 of the Civil Aviation (Offences) Regulations 2006. For example, not complying with Rule 101.209 (maintaining VLOS of aircraft) may, on conviction, result in a fine of up to NZ$1,250 for individuals or up to NZ$7,500 for body corporates. The maximum fines for breaching Part 101 are NZ$5,000 for individuals and NZ$30,000 for body corporates.

Radiocommunications Regulations (Prohibited Equipment - Radio Jammer Equipment) Notice 2011, discussed in greater detail in question 6, below, prohibits the use of radio jamming equipment that interrupts radio communications. The repercussions of this relate to agencies' abilities to control rogue drones.

Data privacy and security

The Privacy Act 2020 relates to the collection, storage, use and disclosure of information about an identifiable individual (**personal information**) in New Zealand. While the New Zealand Privacy Commission is yet to release a privacy policy strictly relating to drones, the Privacy Act applies to the use of drones whenever it is collecting information.

An organization or individual that is collecting personal information must comply with the Information Privacy Principles (**IPPs**) in the Privacy Act.

However, nothing in the IPPs applies in respect of:

- The collection of personal information by an agency that is an individual; or
- Personal information that is held by an agency that is an individual;

Where that personal information is collected or held by that individual solely or principally for the purposes of, or in connection with, that individual's personal, family or household affairs; however, this exemption ceases to apply once the personal information concerned is collected, disclosed, or used, if that collection, disclosure or use would be highly offensive to an ordinary reasonable person. This means if personal information is collected by an individual using a drone and collection would be highly offensive to an ordinary reasonable person, the IPPs and the provisions of the Privacy Act will apply to that collection.

Agencies may only collect personal information for a lawful purpose connected with a function or activity of the agency. They may do this only if the information collection is necessary for that activity.

Drones have the potential to be intrusive when fitted with cameras, and IPP 3 provides that generally, when an agency collects personal information from the individual concerned, such as a recording of that individual, they must take reasonable steps to ensure that the individual the personal information is about is aware of, at least:

- The fact that the information is being collected;
- The purpose for which the information is being collected;
- The intended recipients of the information;
- The name and address of the agency collecting the information and the agency that will hold the information (related parties should also be identified);
- The consequences (if any) for that individual if all or part of that information is not provided;
- The rights of access to and correction of personal information as provided under the IPPs; and
- If the collection of the information is authorized or required by or under law, the particular law and whether the disclosure is voluntary or mandatory.

Drone operators should take reasonably practicable steps to notify people that camera-equipped drones are active in the area, who is responsible for them and for what the footage will be used. This could be as simple as posting a sign, but will be dictated by the situation's specific circumstances.

Drone operators also need to make sure they are not collecting information in an unfair way or in a way that intrudes unreasonably on someone's personal affairs. Notification does not excuse operators from this aspect of the Privacy Act. For example, it would be unfair to hover outside someone's bedroom window regardless of whether the resident was notified. Organizations and individuals must care about how the drone images are used and to whom they are shown.

If images or video was taken using a drone (and generally) are published on the internet without the prior consent of an identifiable individual, it may be a breach of the Harmful Digital Communications Act 2015.

Part 101.207 of the Rules is particularly relevant to privacy concerns related to drones operated over individuals and private property, although it was initially introduced to address safety concerns[141]. Under the Part 101 Rules, drones must not be operated in airspaces above persons who have

141 Shelley, Andrew V --- "Proposals to Address Privacy Violations and Surveillance by Unmanned Aerial Systems" [2016] WkoLawRw 11; (2016) 24 Waikato Law Review 142 (nzlii.org).

not given consent for the aircraft to operate in that airspace and above property, unless prior consent has been obtained from any persons occupying that property or the property owner.

Unmanned traffic management

The private sector has also been active in this area. Following two near misses at Auckland Airport in 2018, Operational Solutions Limited, in partnership with Airways New Zealand and Auckland Airport, has worked on a proof-of-concept drone detection system trialled at Auckland Airport to jointly develop a world-leading Counter Unmanned Aerial Systems (**CUAS**) (discussed below) and UTM System.

The proof of concept system at Auckland Airport consists of the OSL Command and Control / Intelligent fusion software (**FACE**), Aveillant Gamekeeper holographic counter drone radar and artificial intelligence-enabled camera technology. As it evolves, this system will be capable of detecting drones entering airspace that pose potential threats to airport operations, including the ability to identify the nature of the threat. By combining this CUAS capability with a UTM product, (in this case, the Airshare system from Airways New Zealand), it will also be possible to facilitate and authorize drone flights to operate safely in the airspace around airports. OSL was also recently confirmed as the prime contractor and system integrator for Heathrow Airport's CUAS system in the UK.

Counter-drone technology

Under the Radiocommunications Regulations (Radiocommunications Regulations (Prohibited Equipment - Radio Jammer Equipment) Notice 2011), the jamming of radio communications is prohibited unless the person holds a licence allowing the use of radio jammer equipment. The only entity currently licensed to operate jamming devices is the Department of Corrections. This means equipment that can jam drone control signals can only be used at prisons or other Department of Corrections facilities.

In February 2020, Operational Solutions Limited signed a memorandum of understanding with Airways New Zealand to develop a counter-drone detection system jointly. The company's Command and Control/Intelligent fusion software is being trialled at Auckland Airport along with Aveillant Gamekeeper holographic radar and artificial intelligence-enabled camera technology. In a press release, Operational Solutions Limited stated:

> **As the system evolves, it will be capable of detecting drones entering airspace that pose potential threats to airport operations, including the ability to identify the nature of the threat. By combining this C-UAS capability with a UTM project, in this case, the Airshare system from Airways New Zealand, it will also be possible to facilitate and authorise drone flights to operate safely in the airspace around airports.**

At this stage, it is unclear whether Airways New Zealand will be made a 'permitted person' under the regulations. Management of UAS in the future, including how to control errant drones, was discussed, in part, in a joint paper between the CAA and Radio Spectrum Management, including how to control errant drones in the future. The paper was released in August 2020 and related to dedicated spectrum band plans and licensing for unmanned (remotely piloted) aircraft.

The new CA Act establishes new drone intervention powers to support rules to provide for the safe and effective integration of drones into the civil aviation system and respond to serious misuse of drones. The new powers will enable Enforcement Officers to intervene against drones with no person on board that are being operated in a manner that is an offence under civil aviation law or used in the commission of an imprisonable offence under another act. The powers range from preventing take-off to seizure or detention of the drone or its controlling mechanism and destruction of the drone. The power to seize or detain a drone in operation includes the power to use reasonable means (including electronic, mechanical or physical) to bring the drone under control of the person seizing

or detaining it,[142] as long as the power is exercised reasonably and the person exercising the power believes on reasonable grounds that preconditions for the exercise of that power have been satisfied.[143] Any detention or seizure of a drone may be maintained for only as long as the Enforcement Officers considers it necessary to prevent the danger to people or property or the commission of an offence.[144]

The new CA Act will, when it comes into force, introduce additional powers for Enforcement Officers to interfere with, detain, seize and even destroy (in exceptional circumstances). The power includes using reasonable means to bring the drone under control of the person seizing or detaining it, including electronic, mechanical, or physical technologies.

Drone operator qualification requirements

If a drone operator is operating a drone under Part 101 of the Rules, they do not need a licence to fly a drone. Several key things are required under Part 101 for an operator of a drone to comply with:

- Not operate an aircraft that is 25 kg or larger and always ensure that it is safe to operate;
- At all times, take all practicable steps to minimize hazards to persons, property and other aircraft;
- Fly only in daylight;
- Give way to all crewed aircraft;
- Be able to see the aircraft with your own eyes (e.g., not through binoculars, a monitor or smartphone) to ensure separation from other aircraft (or use an observer to do this in certain cases);
- Not fly the aircraft higher than 120 m (400 ft) above ground level (unless certain conditions are met);
- Have knowledge of airspace restrictions that apply in the area you want to operate;
- Not fly closer than 4 km from any aerodrome (unless certain conditions are met);
- When flying in controlled airspace, obtain an air traffic control clearance issued by Airways;
- Not fly in special use airspace without the permission of the administering authority of the area (e.g., military operating areas or restricted areas);
- Have consent from anyone you want to fly above; and
- Have the consent of the property owner or person in charge of the desired flight area.

If a drone operator wants to operate a drone outside Part 101 of the Rules, that person must have a valid Part 102 Unmanned Aircraft Operator Certification.

A person/ entity operating a drone within 4 km of an aerodrome is required to be:

- A holder of (or under the direct supervision of the holder of) a pilot qualification;
- Under the supervision of a remotely piloted aircraft instructor; or
- A holder of a pilot license or certificate under Part 69 or Part 149.

If a person operates a drone under a Part 102 Operator Certificate, the Civil Aviation Authority will require that person to undergo training (see Part 102 Advisory Circular for further information). According to Rule 102.11, an unmanned aircraft operator certificate applicant must provide an exposition acceptable to the Director. The exposition must address certain matters, having regard to the nature, degree and risk of the intended operation and includes such things as:

- The identification of a person who will have primary responsibility for the operation;
- Procedures for reporting information to the CAA;
- Operating requirements for personnel licensing, qualifications, training and competency,

142 Section 318 of the new CA Act.

143 Section 321 of the new CA Act

144 Section 320 of the new CA Act

including pilot and support crew qualifications, training or medical requirements;

- Procedures for the maintenance of aircraft and measures to ensure continued airworthiness;
- The initial airworthiness standard that must be met;
- Identifying any person who is to have control over the exercise of the privileges under the certificate;
- Details of the physical locations to be used in operation;
- A hazard register identifying the known and likely hazards to people, property and other aircraft of the proposed operation and an assessment of the associated risks for each identified hazard;
- A description of the risk management or risk mitigations measures that can be implemented;
- Details of the number and specifications of the aircraft to be used, including any identification system used on the aircraft (e.g., colour schemes, unique identification numbers markings);
- Details of the control system to be used to pilot the aircraft;
- Inflight procedures, including minimum distances from persons or property;
- Procedures for controlling, amending and distributing the exposition; and
- Any other approvals that are required to conduct the proposed operation.

A person operating a drone outside of 4 km from an aerodrome does not need a licence. However, they are required to have knowledge of the Part 71 airspace designations and restrictions in the area they intend to fly.

Additionally, an organization or individual that carries on business supplying the services of drones (i.e., commercial photographers using drone technology) does not require a licence to operate drones in New Zealand.

Developments

In July 2019, the New Zealand Government published a paper about integrating drones into the New Zealand aviation system. The paper's focus was to provide the sector with a clear understanding of the Government's role and its strategic direction and priority areas to achieve the safe integration of drones into the aviation and broader transport systems. The intention was to outline a pathway to integration to provide clarity to the sector about steps the Government will take to ensure risks are addressed, and benefits are realised for New Zealand and the sector as quickly as possible.

In August 2019, MBIE and MoT commissioned a study to quantify the potential benefits of drones to the economy and to support cross-government work towards efficiently integrating drones into the transport system.

In late 2019, MBIE launched a new program for Airspace Integration trials – the program was borne with the vision to make New Zealand a location of choice for the development, testing and market validation of advanced unmanned aircraft and adjacent technologies. The program is currently planned to be carried out until 2024. Current industry partners can be found here.

The Government's intention with establishing the Leadership Group, introducing the Airspace Integration trials and partnering with private industry players is in recognition of the need for a coordinated cross-government (both local and central) and industry approach to fully consider and address all the potential benefits and risks associated with drone integration. The Leadership Group will provide strategic guidance and oversight of the work to safely integrate drones into New Zealand's aviation and transport systems. The pathway to integration was categorised under the following headings:

- **Regulation** – recognising the importance of effective regulation on integration is crucial; the landscape needs to be flexible, enforceable, proportionate, equitable, consistent with relevant international standards and practices and be able to evolve to changing circumstances and new information on the regulatory system's performance.
- **Funding and investment** – recognising that the requirements of the aviation and transport systems will change will mean that consideration will be needed to be given to what investment is needed to support the vision, as well as who should fund it.
- **Infrastructure and technology** – investment in infrastructure and technology will be needed in the short term. Decisions on these investments will require analysis and stakeholder input. This investment will need to include upgrading existing infrastructure and technology in addition to new ones.

- **Research and development (R&D)** – the drone sector is R&D intensive. To fully realise the benefits regulatory interventions and investments in infrastructure have, the development of R&D capabilities will be of primary importance.

New Zealand drone research paper – in June 2020, the CAA, Ministry of Transport and MBIE commissioned Colmar Brunton (an independent research company) to survey recreational users, commercial users and non-users of drones. The survey covered areas where knowledge gaps existed about drone use in New Zealand by the above agencies. The survey posited four new rules surrounding drone use:

- Geo-fencing the areas where drones cannot operate without permission. This would involve using GPS in drones to prevent them from entering restricted areas (e.g., around aerodromes);
- Compulsory remote identification capability on drones to send out drone identification information during a flight;
- Compulsory registration of drones above a certain threshold (e.g., 250 g); and
- Compulsory training for those wanting to operate a drone.

In April 2020, the CAA also released a "Share the Skies" safety campaign following the release of the drone research paper aimed to reinforce the CAA rules for drone users in New Zealand.

In August 2020, a joint paper between the Civil Aviation Authority of New Zealand (CAA) and the Radio Spectrum Management (RSM) team at MBIE was released concerning dedicated spectrum band plans and licensing for unmanned (remotely piloted) aircraft. The paper presents preliminary views of the regulators, as it is predicted that the status quo of all drones operating on the shared, non-protected spectrum is not sustainable. MBIE sought feedback on these views from interested government agencies, the Aeronautical Navigation Service Provider and the New Zealand Unmanned Aircraft community on the dedicated spectrum for Command and Control (C2) links within the terrestrial domain. The paper also discussed in-depth how fixed-band or alternative spectrum arrangements can assist with implementing BVLOS operation of drones.

In April 2021, the MOT published the Discussion Document – Enabling Drone Integration, where the Ministry drew particular interest to UTM as a potential long-term solution for managing drone traffic in New Zealand.

The Ministry suggests a four-phase implementation of several measures leading up to a UTM system (which enables BVLOS operations):

- Changes to the Rules:
  - Replacing consent requirements under Part 101 with 'safe distance' requirements or Rule (see question 2 for details on Part 101);
  - Tightening Rules on visual line of sight but relaxing spotter/observer requirements for FPV drones;
  - Requiring basic pilot qualification from drone operators through mandatory online testing focused on aviation safety, security and operating conditions for Part 101 pilots and
  - Introducing drone registration requirements (mandatory notification of all drones weighing above 250 g);
- Remote ID requirements;
- Geo-awareness:
  - Creating a single standardised map; and
  - Using geo-awareness technology on certain drones or for certain operations (e.g., BVLOS).

The MBIE has developed New Zealand's Aerospace Strategy and published it for public consultation in early September 2022. The New Zealand Government has also announced funding to support the strategy, which includes:

- NZ$3 million for research projects under the Government's Airspace Integration Trials Programme (which involves the development of a UTM system); and
- NZ$3.7 million for the Civil Aviation Authority to establish an Emerging Technologies Program.

New Zealand's civil aviation legislation will soon be replaced by the new CA Act, which was introduced to the New Zealand Parliament on September 8, 2021 after a five-year review of the existing civil aviation legislation[145] to address calls from the aviation industry. The new CA Act will repeal and replace the CA Act and the Airport Authorities Act 1966 when it comes into force.

The new CA Act is extensive, containing 489 sections and ten schedules. It aims to modernise and future-proof New Zealand's civil aviation legislation and improve safety, security, emissions and economic outcomes within the civil aviation sector. The new CA Act also seeks to promote compliance using various regulatory tools, including revising penalty levels to provide deterrence and aligning them with comparable legislation.

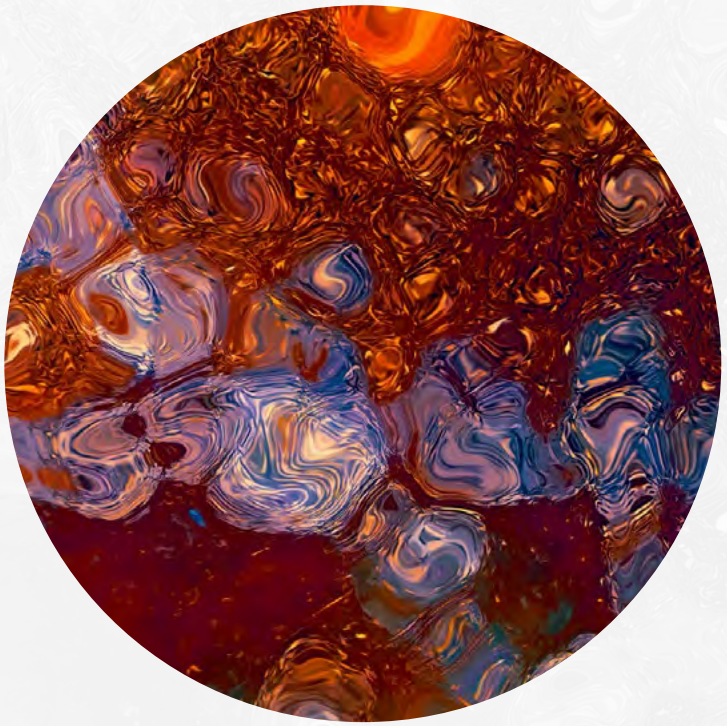
The new CA Act incorporates amendments intended to account for new and emerging technologies and the responsibilities a person has while operating drones, and provides new intervention powers for police constables and specially authorized people to respond to serious misuse.

Pilot in command – unmanned and autonomous aircraft

The CA Act is designed with the assumption that there is a **PIC** who has ultimate responsibility for the safety and control of the flight. The CA Act specifies PICs' duties, and certain powers and responsibilities in relation to those duties. The current definition of PIC is not well suited for new and developing aviation technology where a traditional pilot may not be present on the aircraft. The new CA Act extends the duties, powers and obligations of the PIC to the operators of drones by allowing rules made under the Act to specify who is responsible for the operation and safety of the aircraft under the rules when the PIC is not on board the aircraft.

Definition of 'accident' to include unmanned aircraft

The CA Act requires parties to notify the CAA only when an accident involves manned aircraft. The lack of an equivalent requirement for accidents involving drones limits the CAA's ability to investigate these accidents, understand the safety risks arising from the operation of these aircraft and thereby regulate them effectively. The new CA Act makes changes to require notification of accidents involving drones to address these concerns. The new CA Act, however, acknowledges the difference between the level of harm that can be caused by or to a drone and the harm caused in relation to a conventional aircraft. For an incident to be considered an accident under the new CA Act, the drone must have either caused fatal or serious injury to a person or the drone itself sustains significant damage or structural failure. Damage that is limited to propellers or damage resulting from hail and bird strikes is not considered damage or structural failure that reaches the threshold of an accident under the new CA Act.



145 Civil Aviation Bill 2021 Bill Digest.

Powers to detain, seize and destroy drones

After frequent recent instances of drones around the globe operating in contravention of civil aviation law causing significant risk and disruption to other aircraft, aviation operations and the general public (such as the Gatwick incident in late 2018),[146] increased enforcement powers to ensure compliance with the civil aviation legislation and the safety of the general public is found necessary.[147]

The current provisions authorize the detention of aircraft, but do not expressly authorize the seizure of an aircraft operated in contravention of the CA Act or the Rules. Law enforcement agencies who take action against manned or unmanned aircraft that threaten persons or property are instead exercising their law enforcement functions (including preventing crime, keeping the peace and maintaining public safety) and rely on the availability of defences and prosecutorial discretion.

To address the lack of specific extended powers for drones, the new CA Act extends the Director's existing powers to these aircraft, and introduces additional powers for Enforcement Officers to interfere with, detain, seize and even destroy (in exceptional circumstances).

These powers set out in section 313 and 314 of the new CA Act empower the Director of Civil Aviation (**Director**), or any person to whom the Director delegates the power, to take immediate action in the event the decision maker has reasonable grounds to believe that the use may endanger persons or property. The Director or the delegate may take action without a warrant if prompt action is necessary. Detentions and seizures may be maintained for only such time as considered necessary in the interests of safety and security, but may be retained as evidence.

In addition to the Director's powers, the new CA Act empowers Enforcement Officers appointed by the Director to [148]:

- Enter a place, vehicle or other thing and search for the aircraft;
- Prevent the aircraft from taking off;
- Seize or detain the aircraft and anything being used, or that may be used, to control the aircraft, including the power to use reasonable means (including electronic, mechanical or physical) to bring the aircraft under the control of the person seizing or detaining it; and
- Destroy the aircraft

only to the extent necessary to prevent the offending from being committed or continuing, or to avert the danger, if they have reasonable grounds to believe that an aircraft that is designed to be operated without a pilot on board:

- Operated in the commission of an offence under civil aviation legislation;
- Used in the commission of an imprisonable offence under any other act; or
- Operated in a manner that may endanger people or property;

and it is necessary to take action to avert the danger or to prevent the offending from being committed or continuing.

These powers include using reasonable means (including electronic, mechanical or physical) to bring the aircraft under the control of the person seizing or detaining it.[149]

146 The mystery of the Gatwick drone | Gatwick airport | The Guardian.

147 Civil-Aviation-Bill-Commentary-document (transport.govt.nz).

148 Section 316 of the new CA Act.

149 Section 318 of the new CA Act.

Remaking civil aviation rules

Once the new CA Act comes into force, the Minister of Transport must certify draft civil aviation rules (which include rules applying to drones) which will come into effect after the CA Act is repealed. The draft rules must contain all ordinary rules under the current CA Act and any changes necessary or desirable to ensure that the new rules are consistent with the new CA Act. In this light, it would be reasonable to expect Part 101 and 102 rules to be modified to accommodate the new definitions, terminology and extended enforcement powers introduced by the new CA Act.

The MOT recommended the following key changes (among others) to the Rules in its discussion paper:

- Replacing consent requirements under Part 101 with 'safe distance' requirements or Rule (see question 2 for details on Part 101);
- Tightening Rules on VLOS but relaxing spotter/observer requirements for FPV drones;
- Requiring basic pilot qualification from drone operators through mandatory online testing focused on aviation safety, security and operating conditions for Part 101 pilots; and
- Introducing drone registration requirements (mandatory notification of all drones weighing above 250 g).

Singapore

Overview

As Singapore is a small, highly urbanised island city state, the operation of drones, or unmanned aircraft, is tightly regulated. Drones exceeding 250 g in mass have to be registered. Depending on the weight of the drone, the location and height the drone is flown and the purpose for flying (recreation, education or business), there are different licensing requirements.

Since February 1, 2021, a pilot of an unmanned aircraft that has a total mass exceeding 1.5 kg, but not exceeding 7 kg, for a recreation or education purpose must be at least 16 years of age and hold an formal unmanned aircraft (UA) basic training certificate or an UA pilot licence. A pilot of an unmanned aircraft that has a total mass exceeding 7 kg or for any non-recreational or non-educational purpose must hold a UA pilot licence.

Within four months of the new regulatory regime, as of May 31, 2021, about 12,000 UA have been registered, close to 800 persons have obtained a UA basic training certificate and close to 700 persons have obtained a UA pilot licence. As at March 15, 2022, more than 230 individuals and organizations have been granted an operator permits (generally where UA are used for a business or for a non-recreational or non-educational purpose).

On March 12, 2021, trials of an air traffic control system for unmanned aircraft were successfully completed and a Centralised Flight Management System for UA was launched on June 1, 2022. The system was the culmination of a request for proposals issued in 2017 by the Ministry of Transport and Civil Aviation Authority of Singapore.

This is a timely development given the increased interest in unmanned aircraft usage by both the public sector (e.g., use of drones by the National Parks Board to monitor crowds in parks to ensure safe distancing, Singapore Police Force to patrol industrial estates during the circuit-breaker lockdown period, Public Utilities Board to inspect canals and National Environment Agency to inspect dengue mosquito breeding sites) and private sector (use of drones for shore-to-ship deliveries).

To foster and facilitate more applications, in September 2021, the Singapore Land Authority launched a 3D map to help pilots visualize no-fly zones and to plan their flight paths.

The cost of regulating the use of UA has increased due to the UA industry maturing, as can be seen from the increased number of recreational and commercial UA activities, as well as increased complexity of UA commercial operations. Therefore, the Civil Aviation Authority of Singapore increased the fees for UA permits in December 2022, with further increases to come in January 2024.

VLOS and BVLOS regulations

Government agencies with jurisdiction over drones	Region this agency covers (e.g., entire jurisdiction or province/state)	Role of the agency
Civil Aviation Authority of Singapore	All of Singapore	Registration and regulation of unmanned aircraft, pilots and operators.

Drones are regulated in Singapore principally by the Air Navigation Act 1966 and the Air Navigation (101 — Unmanned Aircraft Operations) Regulations 2019. There are also various Advisory Circulars related to UA issued by the Civil Aviation Authority of Singapore.

Permits

No further permits are required if the drone is flown by a person:

1. Below 200 ft above mean sea level;
2. Outside any restricted area or danger area;
3. Outside 5 km of any aerodrome;
4. Within the person's VLOS for:
    i. A recreational purpose if the drone has a total mass of 25 kg or less;
    ii. An educational purpose where mass is 7 kg or less.

A drone operator permit and Class 1 activity permit must be obtained to operate a drone:

1. That has a total mass exceeding 25 kg for any purpose;
2. That has a total mass exceeding 7 kg, but not exceeding 25 kg for an educational purpose; and
3. Of any total mass in the course of business, or for a purpose that is neither a recreational purpose nor an educational purpose.

A Class 2 activity permit must be obtained to operate a drone:

1. That has a total mass of 25 kg or below for a recreational purpose;
2. That has a total mass of 7 kg or below for an educational purpose;
3. The drone is operated higher than 200 ft above mean sea level, or within any restricted or danger area, or within 5 km of any aerodrome; and
4. That has a total mass of 7 kg or below for an education purpose and and the drone is operated higher than 200 ft above mean sea level, or within any restricted or danger area, or within 5 km of any aerodrome.

The failure to comply with the permit requirements is an offence subject to a fine not exceeding S$50,000 and/or to imprisonment for a term not exceeding two years. The penalties are increased to a maximum fine of S$100,000 and/or five years' imprisonment for repeat offenders.

Training or licensing

A person must not act as a drone pilot of a drone that has a total mass exceeding 1.5 kg, but not exceeding 7 kg, for a recreational purpose or an educational purpose, unless the person is at least 16 years in age and holds a drone basic training certificate or holds a drone pilot licence.

A person must not act as a drone pilot of a drone of any mass in the course of business or for a purpose that is neither a recreational purpose nor an educational purpose, or a drone of a total mass exceeding 7 kg for any purpose, unless the person holds a drone pilot licence.

The failure to comply is an offence subject to a fine not exceeding S$50,000 or to imprisonment for a term not exceeding twoyears. The penalties are increased to a maximum fine of S$100,000 and/or five years' imprisonment for repeat offenders.

A UA pilot must ensure that the unmanned aircraft is within VLOS at all times (directed, unobstructed, unaided and up to a limit of 400 m), unless the UA pilot licence allows the pilot to operate the drone BVLOS.

The failure to comply is an offence subject to a fine not exceeding S$50,000 or to imprisonment for a term not exceeding two years or to both. The penalties are increased to a maximum fine of S$100,000 or five years' imprisonment for repeat offenders.

The CAAS has an Advisory Circular on Beyond Visual Line of Sight Operations for Unmanned Aircraft providing an overview of its assessment methodology for approval of BVLOS operations.

Registration

All unmanned aircraft with a total mass exceeding 250 g must be registered. Upon registration, the registration label must be permanently affixed on the drone.

Failure to comply is an offence subject to a fine not exceeding S$10,000 and/or to imprisonment for a term not exceeding six months.

Protected areas

If a drone flies over any part of a protected area, the operator of the drone is guilty of an offence.

If a drone takes a photograph of a protected area using equipment on board, the operator of the drone and the person taking the photograph, if not the operator, are both guilty of an offence.

The penalty for each offence above is a fine not exceeding S$50,000 and/or to imprisonment for a term not exceeding two years. The penalties are increased to a maximum fine of S$100,000 or five years' imprisonment for repeat offenders.

A person who operates an unmanned aircraft outdoors within the boundaries of any prohibited area is guilty of an offence. The penalty is a fine not exceeding S$50,000 and/or to imprisonment for a term not exceeding two years. The penalties are increased to a maximum fine of S$100,000 and/or five years' imprisonment for repeat offenders.

Carriage of prohibited items

It is an offence if a person operates a drone anywhere (including indoors) carrying a prohibited item (including weapons, explosive substances, fireworks, radioactive or other hazardous material). The punishment is a fine not exceeding S$100,000 and/or to imprisonment for a term not exceeding five years.

Discharge from unmanned aircraft

It is an offence if a person operates a drone anywhere (including indoors) and the unmanned aircraft discharges anything (whether gaseous, liquid or solid) when flying. The penalty is a fine not exceeding S$50,000 and/or imprisonment for a term not exceeding two years. The penalties are increased to a maximum fine of S$100,000 and/or five years' imprisonment for repeat offenders.

It is not a defence that no individual dies or is hurt, no property is destroyed or damaged or no hazard is caused to another aircraft, or to any person or any property.

Dangerous activity

If a person does any act, or causing or permitting any act involving an unmanned aircraft, and knowing that or reckless as to whether, when so acting or causing or permitting the act, the life or property of another person could be endangered or the person could be endangered shall be guilty of an offence. The penalty is a fine not exceeding S$100,000 and/or to imprisonment for a term not exceeding 10 years.

Liability

Criminal liability

Criminal liability is founded on statute – laws passed by the legislature. The principal statute is the *Penal Code* which defines general criminal offences and their punishment, as well as exceptions and defences. The use of drones to commit such criminal offences are governed by the Penal Code. Specific offences arising from the use of drones are found in other statutes, such as the *Air Navigation Act* that regulates the use of unmanned aircraft, as well as the *Hijacking of Aircraft and Protection of Aircraft and International Airports Act 1978*.

Civil liability

Civil liability is based on both common law – judge made law established by precedent—and on statute. Civil liability may arise from the tort of negligence, trespass and nuisance and the statutory tort of harassment. Usually, liability only arises if there was negligence or the act was intentional. However, the *Air Navigation Act* provides that if damage or loss is caused by the use of an unmanned aircraft, the damage or loss shall be recovered without proof of negligence or intention, except where the damage or loss was caused by or contributed to the negligence of the person who suffered the damage or loss.

Accident reporting

A drone pilot must notify the Authority by the quickest available means upon becoming aware of an accident associated with the operation of a drone resulting in serious injury to the drone pilot, serious injury or death of any other person or damage to any property. Failure to do so is an offence subject to a fine not exceeding S$50,000, and is increased to a maximum fine of S$100,000 for repeat offenders.

Data privacy and security

Data privacy is regulated in Singapore by the *Personal Data Protection Act 2012*. It governs the collection, use and disclosure of personal data by organizations. No obligations are imposed on individuals acting in a personal or domestic capacity.

The Personal Data Protection Commission issued Advisory Guidelines to illustrate the application of the PDPA. One section concerns drones that capture personal data of individuals through photography, video or audio recording or otherwise.

Unless excepted, such individuals should be informed of the purposes for which their personal data will be collected, used and disclosed and their consent obtained before it is collected by the drones. The notices should be placed so that individuals are made sufficiently aware that personal data is being collected by drones, providing them the choice not to enter.

One exception is the collection, use and disclosure of personal data that is publicly available. Thus, the use of a drone to collect personal data in a public place (e.g., a park, a shopping mall) does not require consent.

Centralised flight management system

From June 1, 2022, all UA weighing more than 250 g and operated by permit holders must transmit data on their location and activities to a Centralised Flight Management System. Building on this, the Civil Aviation Authority of Singapore plans to develop a fully digital unmanned aircraft traffic management system with a goal to integrate with air traffic management for manned aircraft in the future.

A UA operator permit holder must subscribe to the Centralised Flight Management System service at all times during the validity of the permit and also ensure that each UA exceeding 250 g operated under the permit transmits flight telemetry. The failure to do either is an offence subject to a fine not exceeding S$10,000 and/or to imprisonment for a term not exceeding six months.

A UA pilot who flies a UA must comply with every instruction given by the Centralised Flight Management System service, the failure of which is an offence subject to a fine not exceeding S$10,000 and/or to imprisonment for a term not exceeding six months.

Counter-drone technology

Tampering with an aircraft, including a drone, that may endanger the safety of the aircraft or any person or property, is an offence under the *Air Navigation Act*. The penalty is a fine not exceeding S$100,000 and/or imprisonment for a term not exceeding five years.

Under the *Telecommunications Act*, it is an offence to import any radio-communication jamming device operating in any frequency band unless authorized. It is also an offence to possess any radio communication equipment without a licence. The penalty for both offences is a fine not exceeding S$10,000 or to imprisonment for a term not exceeding three years.

Where an unmanned aircraft is being operated in a manner that contravenes the *Air Navigation Act* or any aviation safety subsidiary legislation, or poses a serious and an imminent risk to safety of the public, an authorized person may exercise powers to prevent the further contravention or to prevent or stop the actual or imminent risk to public safety. Such powers include directing the operator to end the flight or to fly it in the manner specified by the authorized person, assuming control of the unmanned aircraft by such force as is necessary, and to seize the unmanned aircraft and any component of the unmanned aircraft system.

Developments

In September 2020, the Singapore Academy of Law published its Report on the Attribution of Civil Liability for Accidents Involving Autonomous Cars. The report only addressed the use of autonomous vehicles in cars and did not address any other forms of autonomous vehicles, such as drones. This exclusion was premised on the fact that autonomous cars are likely to see broader mainstream adoption as opposed to drones. The Report also expressly did not consider criminal liability.

Given the launch of the Centralised Flight Management System, the increasing interest in drone usage by the public and private sector and the pace of technological improvements, it may not be long before autonomous drones become commonplace. Indeed, a test flight of a manned air taxi that is intended to be autonomous in the future was conducted in October 2019, followed by an announcement in February 2022 of plans to fly a fleet of 10 to 20 air taxis to popular tourist destinations in Singapore by 2024.

It is expected that the necessity to review the existing legal framework for both civil and criminal liability in relation to the use of autonomous drones will take place sooner rather than later.

Industry Focus: Counter-drone and security

Drones are disruptors – both by creating solutions to old problems and creating new problems. This dichotomy is apparent.

Counter-drone measures are largely illegal for use by private landowners. Governments and law enforcement are essentially the only actors with the authority to use radio frequencies to jam or interfere with drones in flight (either through software infiltration or physical means). However, detection systems are generally legal and becoming more common-place, either as permanent fixtures around sensitive sites or as temporary measures to protect against drones for a specific period of time.

Beyond making good business sense to protect intellectual property and trade secrets, installing a drone detection system may have a legal imperative for landowners who owe a duty of care to those who attend on their properties. Airports are a prime example of areas where ensuring the safety of those entering and exiting the property is a key consideration. Since drones are a known hazard if operated near aircraft in critical phases of flight, airports may have a positive obligation to take steps to ensure that the airspace they utilize is safe.

Counter-drone measures are important for more areas:

- Airports
- Critical infrastructure sites
- Power generating and distribution facilities
- Government buildings
- Prisons

United Kingdom

Overview

Prior to the United Kingdom's withdrawal from the European Union, all UK aviation was ultimately governed by the EU's aviation agencies and the EASA in particular. Following Brexit, the UK's Civil Aviation Authority (CAA) now has full responsibility for the regulation of all aspects of aviation in the UK.

Despite leaving the European Union, much of the existing EU law governing aviation in the UK has been retained as UK domestic law[150]. Accordingly, the regime governing the use of drones in the UK currently remains closely aligned with the EU position, with the Implementing Regulations and the Delegated Regulations (both defined below) providing the primary legislative framework for drone operation and production in the UK.

The UK Government has identified drones as a key area of future development. Efforts are ongoing to safely integrate drones into UK airspace, as well as to effectively manage the risks arising from illegal usage of drones (including through the criminalisation of certain uses of drones in the Air Traffic Management and Unmanned Aircraft Act 2021). Additionally, in September 2022, the Law Commission commenced a project to review the UK's legislative framework to understand how the law must develop to facilitate the introduction of autonomous drones in a safe manner.

Drone regulations

Government agencies with jurisdiction over drones	Region this agency covers. (e.g., entire jurisdiction or province/state.)	Role of the agency
Civil Aviation Authority	UK	The CAA is the UK's independent specialist aviation regulator and is responsible for the management of UK airspace, airports and aircraft; the licencing of pilots; and the regulation and enforcement of all aspects of aviation security standards. Part of the CAA's remit is the regulation of drones in the UK, with the CAA being responsible for the licensing and safe operation of drones, as well as providing authorization for usage of drones for certain commercial purposes.
Ofcom	UK	Ofcom is the communications regulator in the UK, and is, among other things, responsible for the allocation and management of radio spectrum in the UK.
Information Commissioner's Office (the ICO)	UK	The ICO is responsible for the regulation of data protection matters in the UK, including the processing of personal data (e.g., images from a camera on a drone).

150 CAA - UK-EU Transition: Aviation Safety (January 2021).

The regulatory regime governing the use of drones in the UK is set out in a number of key pieces of legislation, which have outlined below:

Legislation	Description
Air Navigation Order 2016[151] (the ANO)	The ANO is the main legislation which governs all general aviation activities in the UK and contains a number of provisions which are applicable to drone operations, including airworthiness requirements, registration obligations, operational obligations and prohibited behaviours (and penalties for breaches).
Commission Implementing Regulation (EU) 2019/947 of May 24, 2019 on the rules and procedures for the operation of unmanned aircraft (Retained EU Legislation)[152] (the Implementing Regulations)	The Implementing Regulations set out the three categories of drone operations (Open, Specific and Certified), as well as detailed provisions relating to the operation of drones within each of these categories (including pilot licensing requirements).
Commission Delegated Regulation (EU) 2019/945 of March 12, 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems (Retained EU Legislation)[153] (the Delegated Regulation)	The Delegated Regulations set out requirements relating to the design, manufacture, import and distribution of drones in the UK.
Commission Implementing Regulation (EU) No 923/2012 of September 26, 2012 laying down the common rules of the air and operational provisions regarding services and procedures in air navigation (Retained EU Legislation)[154] (also known as the Standardised Rules of the Air (SERA))	SERA details common rules of the air and operational provisions regarding services and procedures in air navigation. SERA applies to all air traffic, including drones.
Regulation (EC) No 785/2004 on insurance requirements for air carriers and aircraft operators[155] (the Insurance Regulations)	The Insurance Regulations set out the minimum insurance requirements for air carriers and aircraft operators.
CAA: **CAP 722** – Unmanned Aircraft System Operations in UK Airspace - Guidance[156]	CAP 722 is a guidance note which has been prepared by the CAA which contains information relevant to the development, manufacture and operation of drones in the UK, summarizing the obligations contained in the key legislation detailed above.
Wireless Telegraphy Act 2006	Prohibits the use of radio spectrum without either a licence from Ofcom or an exemption.
Data Protection Act 2018, and the General Data Protection Regulation (EU) 2016/679, as retained in UK law by the European Union (Withdrawal) Act 2018 (the UK GDPR)	Sets out detailed rules which apply when organizations process personal data.
Health and Safety at Work etc. Act 1974[157] (H&SWA)	The H&SWA is the primary piece of legislation covering occupational health and safety in the UK.

151 CAA - Air Navigation Order 2016.

152 CAA - CAP 1789A: Consolidated version of Regulation (EU) 2019/947 as retained (and amended in UK domestic law) (28 June 2022).

153 CAA - CAP 1789B: The UAS Delegated Regulation: UK consolidated text (8 January 2021).

154 SERA - Standardised Rules of the Air (CAA).

155 Regulation (EC) No 785/2004 of the European Parliament and of the Council of 21 April 2004 on insurance requirements for air carriers and aircraft operators .

156 CAA - CAP 722: Unmanned Aircraft System Operations in UK Airspace - Guidance (5 November 2020).

157 Health and Safety at Work etc. Act 1974.

Categories of drone operations

The Implementing Regulations separate drone operations into three distinct operational categories depending on the level of safety risk (the three categories being Open; Specific and Certified), and set out specific rules which apply to drone operations in each category.

Open category

The Open category applies to drone operations where the various operational risks are lowest. Accordingly, drones falling within the Open category are subject only to basic operational requirements. In particular, no prior operational authorization is required from the CAA to undertake drone operations within the Open category.

When operating a drone within the Open category, there are a number of operational restrictions which apply:

- Operations must be conducted on a VLOS-only basis, meaning that the drone should not be flown more than 500 m from the pilot, and remain within the pilot's direct line of sight at all times. The use of binoculars, telescopes or any other image enhancing devices to extend the line of sight are not permitted;
- Drones must **not** be flown higher than **120 m** AGL, unless flying over an artificial object, such as a building, provided that the drone operator has obtained adequate consent to do so, and in such cases the drone shall be entitled to fly up to 15 m higher than that artificial object; and
- Drones must not be flown over people and kept a safe distance from people during operation (the specific distance requirements will depend on the "subcategory" of the drone, which is considered in further detail below).

The Open category only applies to drones with a maximum take off mass (MTOM) of less than **25 kg**. In addition, there are three subcategories of drone within the Open category and there are certain specific rules which apply only to each subcategory (including pilot licensing requirements and rules on the permitted proximity to other people for each flight). The subcategories relate to the following drone system classes (as more fully described in the Annex to the Delegated Regulation):

- Subcategory A1 – Classes **C0** (MTOM of less than 250 g) and **C1** (MTOM of less than 900 g);
- Subcategory A2 – Class **C2** (MTOM of less than 4 kg); and
- Subcategory A3 – Class **C3** (MTOM of less than 25 kg).

Further details of the specific operational restrictions for each subcategory within the Open category can be found in Section A1 of CAP 722 and Part A of the Annex to the Implementing Regulations.

Specific category

The Specific category applies to medium-risk operations, which are categorised as any operations which present a greater risk than under the Open category or where at least one element of the operation falls outside the Open category's set boundaries.

Operations under the Specific category can cover VLOS, EVLOS and BVLOS.

EVLOS operations involve the use of additional human observers who keep the drone within their line of sight at all times, even if the pilot of the drone itself does not have visual sight of the drone. BVLOS refers to all other situations where neither the pilot nor any additional human observers have a direct line of sight of the drone while it is airborne. This lack of line of sight necessitates the use of alternative means of collision avoidance to ensure that the drone can be flown safely, such as "Detect and Avoid" capabilities, which provide the pilot with information and detail about the flight in real time, to a level of detail equivalent to what a pilot would otherwise have when operating in VLOS.

In many cases, the CAA will require BVLOS operations to be operated under the Certified category.

To conduct drone operations under the Specific category, the operator must have received operational authorization from the CAA.

Operators are able to submit applications for operational authorization online.[158] Any operational authorization granted by the CAA will set out the rules and restrictions which apply to the authorized operation.

Prior to making an application for operational authorization, operators must undertake a *Safety Risk Assessment* which will provide details of the proposed drone operation, how the operation will be undertaken, technical details of the drone which is to be used and set out a risk assessment demonstrating how the operations will be conducted in a safe manner. The CAA has made a number of pre-defined risk assessments available for use in connection with certain operational authorization applications.[159] Further guidance on completing Safety Risk Assessments can be found in Section 3 of CAP 722A.[160]

Specific operating risk assessment

In February 2023, the CAA outlined its timeframe for introducing the Specific Operating Risk Assessment (SORA) process developed by JARUS. A risk assessment methodology to establish a sufficient level of confidence that a specific operation can be conducted safely, SORA will be used as an Acceptable Means of Compliance (AMC) to Article 11 of UK Regulation (EU) 2019/947. No regulatory change will be required to implement it.

Nonetheless, the UK SORA implementation project will be comprehensive and detailed, developing training courses for UAS operators and eventually supplanting current operational authorizations. The CAA have said that the UK SORA will be ready for consultation from Q1 2024, with implementation planned for Q3/Q4 of the same year.

In the meantime, it has told those who wish to fly in the Specific category to continue to use the methodology and templates outlined in CAP 722A[161].

Certified category

The Certified category applies to higher-risk operations, which is understood to mean drone operations which present an equivalent risk to that of manned aviation. As a consequence of the increased risk levels, drone operations in the Certified category are subject to the same regulatory requirements as manned flights.

CAP 722 provides a number of specific situations where drone operations must be conducted in the Certified category, including, use of drones to transport people, flying large drones over assemblies of people or the carriage of dangerous goods. The CAA also has the power to designate any applications made under the Specific category as requiring operation under the Certified category after having considered the risk assessment provided by the drone operator.

Many drone operations conducted under the Certified category, including where operations are operated on a BVLOS basis, will require segregated airspace to ensure the safe operation of the drone by removing the risk of collisions with other airspace users. In the UK, this is achieved through the designation of "Danger Areas," either on a temporary or permanent basis. Applications for any such airspace segregation are assessed by the CAA on a case-by-case basis through the Airspace Change Process.[162]

At the date of publication of this guide, the UK's regulations relating to the Certified category are still under development. Accordingly, the principles set out in equivalent manned aviation regulations (including the ANO in particular) regarding airworthiness, operations and licensing will regulate the Certified category.

Where authorization is required under the Certified category, early engagement with the CAA is recommended to ensure that the CAA has adequate time to consider and process any applications for airspace segregation.

158 https://applications.caa.co.uk/CAAPortal/servlet/SmartForm.html?formCode=UAS.

159 CAP 722H - Specific Category Operations: Pre-defined Risk Assessment Requirements, Guidance & Policy

160 CAA - CAP 722A: Unmanned Aircraft System Operations in UK Airspace - Operating Safety Cases (23 July 2019).

161 Specific Operating Risk Assessment.

162 Further information can be found in CAA - CAP 1616: Airspace Change (1 March 2021).

Airspace restrictions

The CAA uses a regime of "airspace restrictions" to safely and effectively manage UK airspace. These restrictions can be permanent or temporary, and will typically apply near any airport, in highly built-up areas or areas used for military purposes. When piloting a drone (of any category) it is important to be aware of any airspace restrictions in the proposed area of operation. NATS UK maintain an online map with up-to-date airspace restrictions applicable to drones, which should be consulted prior to undertaking any drone operations.[163]

Airworthiness

The specific requirements which apply to the design and manufacture of drones which are to be operated in the UK are set out in the Delegated Regulations. From January 1, 2023, all new drones placed onto the UK market for use in the Open category must meet the product standards and criteria to be placed within one of the formal "classes" of drone (e.g., C0, C1, C2 and C3), which are based on the weight and capabilities of the drone.

Liability

Criminal liability

The CAA is responsible for the management of the UK's airspace and enforcing security standards and is not responsible for monitoring and taking action against criminal uses of drones. The police are responsible for investigating and prosecuting criminal usage of drones.

The ANO sets out a number of "prohibited behaviours" which apply to all aviation activities in the UK, including the prohibition on endangering the safety of any aircraft (Section 240, ANO) or endangering any person or property through use of an aircraft (Section 241, ANO). Breaches of the ANO can result in fines or imprisonment, depending on the nature of the breach (Section 265, ANO).

The UK has also recently brought into force the Air Traffic Management and Unmanned Aircraft Act 2021[164], which introduces a number of specific criminal offences relating to the improper use of drones.

A criminal offence may also be committed where a drone is used in a manner which amounts to harassment. For harassment to be committed in the UK, the drone pilot must pursue a course of conduct which: (a) amounts to harassment; and (b) they know, or ought to know, such conduct amounts to the harassment of the other.[165] Harassment includes alarming the person or causing them distress. A course of conduct must involve conduct on at least two occasions. It is a defence if the drone pilot can prove that their conduct was *reasonable* in the circumstances.

Health and safety

Where the drone operator is a company, it must additionally comply with its obligations under the H&SWA, which imposes a broad duty on companies to ensure the health, safety and welfare of their employees at work (for example, by providing adequate training, information and supervision to employees and by ensuring the safety of the working environment).

Failure to discharge any duty imposed on them by the H&SWA is a criminal offence, and it is important to note that liability under the H&SWA arises from the failure itself, regardless of whether that failure actually causes any harm. Breaches of the H&SWA are strict liability offences, so can be prosecuted without having to establish that the offender intended to commit the breach.

Health and safety breaches are typically punished by fines and there is no upper limit on the size of the fine which can be imposed. When such breaches are committed by individuals, it is also possible for custodial sentences to be handed down in situations where the severity of the breach, and the individual's culpability for that breach, has rendered the imposition of a fine or community sentence inappropriate.

163 https://nats-uk.ead-it.com/cms-nats/opencms/en/uas-restriction-zones/.

164 Air Traffic Management and Unmanned Aircraft Act 2021.

165 Section 1(1) of the Protection from Harassment Act 1997.

Civil Liability

The CAA has the power to issue fines for breaches of any aviation rules, or any licences or authorizations which it has granted.

Where the use of a drone causes damage to property or injury to any person, then the injured party may be able to seek a remedy from the pilot and/or operator of that drone under tort law. Tort law provides civil remedies, typically in the form of financial compensation, in situations where one person suffers damage due to the fault of another.

Additionally, improper usage of drones by operators could give rise to a variety of other civil liabilities under various laws (e.g., breaches of data protection laws could result in a fine being issued by the UK's data protection regulator, the ICO).

Insurance

In accordance with the Insurance Regulations, drone operators must ensure that they have in place adequate insurance coverage at a level appropriate for their usage and no less than the mandatory amount for their classification of drone.[166] Failure to have in place adequate insurance will also be a breach of any operational authorization issued by the CAA. It is not necessary to have insurance in place for drones which have a MTOM of less than 20 kg which are being used for solely for recreational purposes.

Data privacy and security

The processing of personal data within the UK is governed by the Data Protection Act 2018 and the UK GDPR.

Where a drone has the capability to record video or photographs, or is equipped with other sensors or detection equipment, that drone has the potential to be capturing the personal data of individuals. In such situations where the drone is capturing personal data, the operator of that drone will be a controller of that personal data (unless the operator is using the drone for personal purposes only) and must comply with its obligations under data protection law.

In addition, any usage of drones which are equipped with any form of surveillance technology must be done in compliance with the UK Surveillance Camera Code of Practice.[167] Some of the key principles set out in this Code of Practice state:

- That the use of surveillance cameras must always be for a specified purpose in pursuit of a legitimate aim, and such usage must be a necessary and proportionate means of achieving that legitimate aim;
- Surveillance systems must always be used in a transparent manner, including publishing the details of a designated point of contact to enable individuals to make complaints or obtain further information about the surveillance activities;
- The operator of the system must have clear rules and policies in place to govern the usage of the surveillance system, and proper governance procedures should be in place so that there is clear allocations of responsibility and accountability for the use of the system; and
- The surveillance system should only store information which is strictly necessary for the stated purpose and access to the stored information should be restricted.

Where drone operators are using the drones to collect personal data, they must provide details of the data processing to the individuals whose personal data is being captured. It is the expectation of the ICO that all data controllers take steps to provide this information.[168] In practice, this can take the form of visible notices in the areas of operation informing individuals in the area that their personal data may be captured and providing details on where further information can be found (for example, public notices can provide QR codes which link out to the operator's online privacy notice).

Due to the invasive nature of drones with recording capabilities, the ICO expects the operators to provide strong justification for the use of the drones in this manner. This should be considered and documented in a "Data Protection Impact

166 Further information can be found at: https://www.caa.co.uk/aircraft-register/registration-information/mandatory-insurance-requirements-for-aircraft/.

167 Biometrics and Surveillance Camera Commissioner: Amended Surveillance Camera Code of Practice (3 March 2022).

168 CO - Guidance on video surveillance.

Assessment" (DPIA). A DPIA is a process through which the operator will be able to consider what personal data it is likely to collect through the drone operations and assess the impact that any such proposed data processing activities will have on the rights and freedoms of the individuals whose data may undergo processing. The DPIA should at a minimum, describe the data processing activity and its purposes, assess whether it is necessary and proportionate to process personal data, assess the risks to the rights and freedoms of individuals and set out any mitigation measures which should be put in place to address these risks. The ICO has a right to request a copy of DPIAs; so any completed DPIA should be retained on file by the operator.

Unmanned traffic management

CAA traffic management strategy

In the UK, the CAA have published a strategy paper outlining their recommendations for the creation of a policy framework designed to facilitate a unified approach to the safe integration of drones into UK airspace.[169] This paper makes a number of key recommendations aimed at facilitating the introduction of a suitable traffic management system for drones in the UK. This would lay the groundwork for the establishment of an effective traffic management system for both manned aircraft and drones across all phases of operations.

Some of the key recommendations from the strategy paper are:

- That the existing laws governing airspace management are updated to create a single legal framework applicable to all aircraft; and
- Further research and development to better understand the safety and cyber security risks associated with commercial drone usage and how these can be managed and mitigated by an effective traffic management system.

The UK Government has now awarded grants to a number of companies to undertake early-stage research into the safe integration of drones into UK airspace. The CAA has also considered the integration of drones into UK airspace and has set out its strategic vision for airspace modernization in the recently published Airspace Modernization Strategy 2023-2040.[170]

BVLOS testing

In 2020, the UK government awarded funding to an Aircraft Innovation Centre at Goodwood Aerodrome, Sussex.[171] The Centre will run flight tests to mix unmanned drones with regular manned air traffic. The intention is to demonstrate BVLOS drone operations in non-segregated airspaces. Typically, to fly a drone on a BVLOS basis in the UK, a temporary danger area (TDA) will be set up to segregate that drone operation from other aircraft. As the use of drones increases, TDAs are viewed within the industry as impractical. The project aims to deliver an environment and operating conditions in which drones do not require a TDA to operate, providing data and insights which can be used by the CAA to develop their approach to airspace management and the safe integration of BVLOS drones into the existing mixed-use airspace over the coming years.

Remote identification

Remote identification refers to a drone feature which broadcasts identification information that can be received by third parties. The purpose of remote identification is to assist the CAA, law enforcement and security agencies to identify rogue drones, pilots or operators who appear to be operating in an unsafe manner and drones flying in restricted areas. Remote identification should allow for each drone's unique registration number to be broadcast while in operation, so that this information can be obtained without securing physical access to the drone itself.

In the UK, all drones other than those in Class C0 (<250 g) must have remote identification capabilities, which need to be switched on at all times when the drone is in operation.[172]

169 CAA - CAP 1868: A Unified Approach to the Introduction of UAS Traffic Management (December 2019).

170 CAP1711: Airspace Modernisation Strategy 2023–2040 (23 January 2023).

171 https://www.aerospacetestinginternational.com/news/drones-air-taxis/uk-site-to-run-trials-of-unmanned-drone-traffic-management-system.html .

172 Section 4.4 of CAP 722.

Counter-drone technology

Ever since drone sightings brought widespread disruption to Gatwick Airport in 2018[173], counter-drone technology has been a key focus in the UK. In 2019, the UK Government published the "UK Counter-Unmanned Aircraft Strategy,"[174] which set out the government's strategy to mitigate against the malicious and criminal use of drones in a proportionate manner, so as not to stifle the innovation and the positive benefits of legitimate and safe usage of drones.

The government's strategy is to reduce the risk arising from the illegal use of drone by developing a comprehensive understanding of the risks posed by improper drone usage, adopting a wide range of tools and processes which can be used to reduce the risk of the illegal usage of drones, working with the counter-drone industry to develop suitable counter-drone products and providing appropriate enforcement powers to the police to enable them to tackle illegal usage of drones.

A number of UK airports have now invested in anti-drone technology to provide greater protection against drones being used illegally to disrupt air traffic.[175]

At an individual level, members of the public are encouraged to call the police if they encounter an issue relating to the unsafe use of drones.

The private use of radio frequency jammers, including for the purposes of disabling drones, is prohibited in the UK. It is a criminal offence under the Wireless Telegraphy Act 2006 to use any apparatus, including jammers, for the purposes of deliberately interfering with wireless telegraphy (radio communications) in the UK.[176] The maximum penalty is two years' imprisonment and/or an unlimited fine.

Drone operator qualification requirements

The registration requirements in the UK draw a distinction between the "operator" and the "flyer" of a drone. The "operator" is the person who owns or is responsible for the overall operation of the drone and can be a legal or natural person. The "flyer" is the pilot of the drone who has responsibility for the actual flight of that drone.

Both the "operator" and the "flyer" must both register with the CAA (even where the "operator" and "flyer" are the same person) prior to conducting any drone operations. Drones under 250 g are exempt from registration unless equipped with a camera.

Commercial operators of drones must have registered for an "Operator ID" to own drones (in addition to any separate operational authorizations which may be required from the CAA to undertake certain activities using those drones). Registration can be completed online.[177]

Pilots of drones operating under the Open category must pass the CAA's online theory test, register for a "Flyer ID" and hold an "Operator ID".

Pilots of drones operating under the Specific category must have the "General VLOS Certificate," which provides the remote pilot with all basic competency requirements to safely operate VLOS drones within the Specific category. Additional modules can be undertaken by the remote pilot to develop their skills in specific operational situations (such additional qualifications may be required by the CAA as a condition to granting operational authorization on complex operations under the Specific category).

Qualification requirements under the Certified category have not yet been confirmed by the CAA.

173 https://www.theguardian.com/uk-news/2018/dec/21/gatwick-airport-reopens-limited-number-of-flights-drone-disruption.

174 UK Government: UK Counter-Unmanned Aircraft Strategy (October 2019).

175 https://www.airport-technology.com/news/heathrow-airport-installs-anti-drone-technology-to-detect-threats/.

176 Section 68 of the Wireless Telegraphy Act 2006.

177 https://register-drones.caa.co.uk/organisation/register.

Developments

UK Government – ambition statement

In July 2022, the UK Government published "Advancing airborne autonomy: use of commercial drones in the UK," which set out the government's ambitions for the commercial adoption and use of drones over the next decade.[178]

The government's vision is that by 2030 "commercial drones will be commonplace in the UK in a way that safely benefits the economy and wider society." The government believes that the widespread adoption of drones could deliver an uplift of as much as £45 billion to the UK's GDP by 2030 and provide cost savings, reduce carbon emissions and reduce risks arising from hazardous working environments.

The ambition statement identifies a number of sectors which it believes have the greatest potential use cases for commercial drone operations. In particular, increased adoption in the delivery sector has been forecast to be worth an additional £10 billion to the UK economy by 2030, and there is significant scope for greater usage in the engineering and construction industries. Additionally, commercial drones can be used to great effect by emergency services, allowing for both faster response times and increased safety through reducing the time spent in hazardous environments.

The ambition statement also sets out some key "enablers" necessary to maximise the opportunity presented by commercial drones, including:

- Significant investment in "state-of-the-art UK technology," which should initially focus on testing and demonstrating that the technology can be operated safely;
- A regulatory framework which allows for the development of commercial drone operations without compromising safety. This is a priority area of focus for the UK Government, which has committed substantial funding to the CAA to ensure that the CAA has the capacity to support and effectively regulate the growing drone sector;
- Support the drone sector within the UK to ensure that it is a leading hub for the start-up and scale-up of companies focussed on drone development. This will be achieved through national and local initiatives to support universities and businesses operating within the sector and ensuring that the UK has the talent necessary to build, maintain and operate drones at the scale required; and
- Continued public engagement to inform and support public debate on drone use, to ensure that the public understand the potential benefits of commercial drone usage, and to give local businesses the confidence to adopt drone-based solutions.

Law Commission's aviation autonomy project

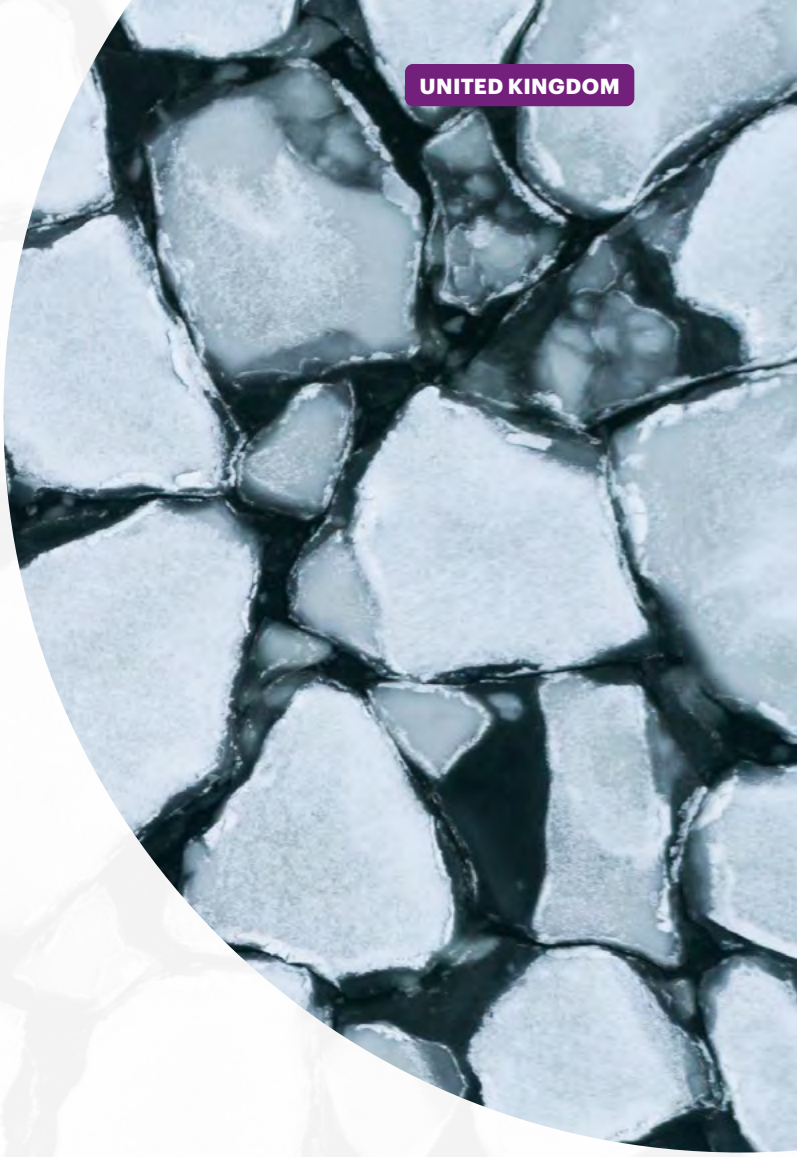
The Law Commission, together with the CAA and the Department for Transport, have commenced a full review of the laws which currently apply to drones and autonomous flight.[179] The purpose of this review is to examine the existing legal framework to identify the legislative changes which would be required to enable the safe deployment of autonomous flight technologies in the UK. The project will involve consultations with key stakeholders within the aviation and technology sectors, and it is expected that the Law Commission will publish their findings by the end of 2023.

Ofcom consultation

Ofcom is the UK's communications regulator, with responsibility for managing the allocation and use of the UK's radio spectrum. As the radio spectrum is a finite resource, proper management of the spectrum is essential for the safe and efficient functioning of all wireless services. Drones currently rely on an exemption to Ofcom's licencing regime for access to certain radio frequency bands. These currently allocated frequency bands only allow for operation using lower power telecommunication technologies,

178 HM Government - Advancing airborne autonomy: use of commercial drones in the UK (18 July 2022).

179 Law Commission - Aviation autonomy project.



which work well with VLOS operations but are not suited to BVLOS drone operations (which primarily rely on mobile or satellite technology).

Ofcom has acknowledged that the current frequency bands are not suitable for BVLOS drone operations and has recently closed a consultation with interested stakeholders to consider Ofcom's proposed solutions to address these issues and to ensure that the radio spectrum in the UK is suitably equipped to allow for the increased adoption of BVLOS drone operations in the future.[180]

In the consultation document, Ofcom set out the following proposals:

- A new spectrum licence for drone operators will be created for radio spectrum usage which would allow for BVLOS drone operations;
- The proposed radio spectrum would enable the use of mobile and satellite terminals for the control of drones, as well as the operation of safety equipment which will be vital for the avoidance of collisions when drones are operated BVLOS;
- The new licence would be subject to an annual fee of £75; and
- The existing licence exemption regime would remain in place for low-power drone operations, which would ensure that existing VLOS drones on the market today can continue to operate.

Following the completion of the consultation, Ofcom has started offering spectrum licences for the use of essential drone safety and communications equipment.[181] The availability of new radio spectrums for use by drone-specific technologies will allow companies operating in this sector to implement cutting edge technologies, on a designated spectrum, which will allow sophisticated drones to travel for longer, at higher altitudes, and over greater distances, as well as increasing the safety of such flights.

Further details of Ofcom's new approach to authorizing the usage of drone-specific radio equipment can be found in the Ofcom publication "Spectrum for Unmanned Aircraft System".[182]

Applications for licences to operate radio equipment on the new designated spectrums can be made directly to the Licensing Team at Ofcom. Full details of how to apply for a licence, and the terms and conditions of any such licence, are set out in the Ofcom publication "Spectrum for Unmanned Aircraft Systems".[183]

180 Ofcom - Consultation: Spectrum for Unmanned Aircraft Systems (10 June 2022).

181 Ofcom: "New commercial drone services cleared for new year take-off" (16 December 2022).

182 Ofcom - Spectrum for Unmanned Aircraft Systems(UAS) (16 December 2022).

183 Ofcom - Spectrum for Unmanned Aircraft Systems (UAS) licence (20 January 2023).

United States of America

Overview

The Federal Aviation Administration (FAA) issued Part 107 in 2016, the first comprehensive regulation of commercial operations of small drones (not to exceed 55 lbs.).[184] Part 107 authorizes commercial drones operations without the drone having either a type or airworthiness certificate, such operations are subject to a number of conditions and limitations.

Key limitations are operating within the VLOS of the remote pilot, during daytime, below 400 ft AGL, not directly over people and only in uncontrolled airspace. Part 107 does allow drone operators to obtain a waiver to operate at night, over people and BVLOS, as well as obtain authorization to fly in controlled airspace.

Part 107 does not permit a waiver to conduct package delivery BVLOS for compensation. In 2020, FAA released a final rule authorizing operations over people (OOP), subject to several conditions and limitations.[185] The drone must obtain certification before it may be flown over an assembly of people. The FAA also released a final rule requiring commercial and recreational drones to be equipped with remote identification (remote ID).[186] Drones must be equipped with remote ID broadcast technology by September 16, 2023. After December 16, 2022, companies may not manufacture a drone unless that drone is subject to an FAA-accepted Declaration of Compliance, attesting to complains with the rule (Part 89), and an FAA-accepted Means of Compliance (MOC). ASTM Remote ID Standard 3586-22 is the only MOC FAA has accepted to date. Model and recreational operations within designated areas are not required to have remote ID. Operation of a drone with payload over 55 lbs, commonly used to conduct agricultural spraying, may be authorized by exemption under 49 U.S.C. 44807.

The FAA has begun issuing certificates, thereby obviating waivers and exemptions, but has only issued one type and airworthiness certificate to date, except in the experimental category (R&D only), and has issued only four air carrier operating certificates to date.

VLOS and BVLS regulations

Government agencies with jurisdiction over drones	Region this agency covers (e.g., entire jurisdiction or province/state)	Role of the agency
United Stated Department of Transportation	United States	Parent of FAA; grants economic authority to UAS air carriers
Federal Aviation Administration (FAA)	United States	Exclusive safety regulator of UAS, UAS pilots, UAS operators and UAS airspace

Commercial drone operations are governed by 14 CFR Part 107. The rule applies only to "small" UAS. For commercial operation of drones with payload weighing more than 55 lbs, as well as package delivery operations BVLOS for compensation, an exemption under section 44807 is required.

Currently, commercial drone operations are not required to be certificated.[187] Commercial package delivery BVLOS does require an air carrier certificate. FAA is developing Part 23 Special Class airworthiness standards so that it can issue type, production and airworthiness certificates. It has published final special class airworthiness criteria for ten drone models and had published proposed special class airworthiness criteria for several additional models.

184 Operation and Certification of Small Unmanned Aircraft Systems, 81 Fed. Reg. 42064 (June 28, 2016).

185 Operation of Small Aircraft Systems Over People, 86 Fed. Reg. 4314 (Jan.15, 2021).

186 Remote Identification of Unmanned Aircraft Systems, 86 Fed. Reg. 4390 (Jan. 15, 2021).

187 49 U.S.C. 44807(a). This authority is set to expire September 30, 2023, but the sunset will be effective only prospectively. Any authority granted or rule issued before that date, including Part 107, will continue by its terms.

Part 107 includes a number of prohibitions or limitations subject to waiver, including:

- Operations at night are prohibited, but FAA routinely granted waivers to operate at night. In the OOP final rule, FAA now permits operations at night by rule.
- Operations must be conducted within the VLOS of the remote pilot. FAA has granted waivers to operate BVLOS over relatively short distances, requiring one or more visual observers to monitor other aircraft operations in the vicinity, except in very rural and remote locations. First Person View operations are not considered VLOS.
- Operations must not exceed 400 ft AGL, except that operations may be conducted up to 400 ft above a structure.
- A remote pilot may operate only one drone at a time. FAA has granted waivers for multiple drones per pilot and has authorized dronelight shows with several hundred drones operating virtually autonomously within a geo-fenced area.
- Commercial drones may not be operated in prohibited or restricted airspace, except as may be authorized by Air Traffic Control. More broadly, FAA authorization is required to operate in controlled airspace (generally, near commercial service airports). FAA and the drone industry have stood up the Low Altitude Authorization and Notice.
- Capability (LAANC) system to provide real-time online authorization to operate in certain segments of controlled airspace.
- Commercial drone operations may not carry hazardous materials (dangerous goods). Air carriers must obtain special permission to carry hazmat.
- Drones must give the right of way to manned aircraft and may not operate so close to another aircraft as to create a collision hazard.
- Drones may not be operated at a speed in excess of 87 knots (100 mph). FAA may grant a waiver from this speed limit.
- Minimum flight visibility must be no less than three statute miles from the control station, and the minimum distance from clouds must be no less than 500 ft below the cloud and 2,000 ft horizontally from the cloud. FAA may grant waivers from one or more of these limitations; and All drones weighing .55 lbs or more must be registered.

Liability

Criminal liability

A knowing and willful violation of any FAA regulation for which a civil penalty is not provided warrants a criminal penalty.[188]

Civil liability

A person who violates any FAA regulation, including any provision of Part 107, is subject to a civil penalty. Each flight is a separate penalty, and a flight may involve more than one violation. Penalties are greater for commercial operators by a company that is not a small business (US$40,272) than for small businesses or individuals (US$1,771). These amounts are periodically adjusted for inflation.[189]

The FAA also has the authority to revoke or suspend any certificate for a violation of FAA rules. For drones, that would include an aircraft registration certificate, a remote pilot certificate with a small UAS rating and an air carrier operating certificate.

Non-compliance with specific regulations/laws

18 U.S.C. 40A was added in 2018 to make it a crime punishable up to two years in prison for a reckless drone operation that interferes with a wildfire suppression effort or a law enforcement or emergency response effort.

18 U.S.C. 39B was added in 2018 to make it a crime punishable up to one year in prison for a reckless drone operation that interferes with a passenger aircraft in a manner that poses an imminent threat to occupants.

49 U.S.C. 44802 was added in 2018 and provides a civil penalty of US$29,462 (adjusted for inflation) for operating a drone equipped or armed with a dangerous weapon.

There is also a statutory fine,[190] added in 2016, for up to US$24,656 for interfering with wildfire fire suppression, law enforcement or emergency response efforts.

Data privacy and security

There is no Federal law relating to privacy that applies to drones. State and local governments have enacted laws relating to low altitude drone operations, ostensibly to protect the privacy of citizens. These laws may be pre-empted by Federal law. An individual may collect civil action money damages and an injunction against a drone operator for invasion of privacy.

Data privacy and data security laws that may impact drone operations because the operation may collect personal information vary among the 50 states. Some of these laws have been challenged in court. See *National Press Photographers Association v. McCraw,* 2022 WL 939517 (W.D. Texas) (holding Texas law prohibiting capturing of images of individuals or private property as content-based and unconstitutionally vague, and holding prohibition on flying a drone over certain property as unconstitutionally vague and also content-based discrimination that is not narrowly tailored in violation of the First Amendment to the Constitution) (appeal pending).[191]

Unmanned traffic management

The FAA, working with the National Aeronautics and Space Administration (NASA), is developing a UTM system. A pilot program is underway to test BVLOS operations at selected sites, and FAA has published a Concept of Operations document, with 2.0 published and version 3.0 under development. There is no UTM rulemaking underway.

As noted, the FAA published a final rule in January 2021, requiring all drones that are required to register to be equipped with remote ID that employs broadcast technology. Drone manufacturers must comply by December 16, 2022,[192] and drone operators must

188 49 U.S.C. 46316.

189 49 U.S.C. 46301.

190 49 U.S.C. 46320.

191 See also *Long Lake Township v. Maxon,* 2021 WL 1047366 (Mich, Cit. App)(holding Fourth Amendment of the U.S. Constitution violation by Township's use of drones for surveillance without a warrant)

192 With the delay in FAA acceptance of the ASTM Remote ID standard Means of Compliance, the FAA stated that it would not take enforcement

comply by September 16, 2023. The UTM concept of operations contemplates network-based remote ID technology, as well as broadcast technology, while the final remote ID rule does not permit the use of network technology to meet remote ID requirements.

Counter-drone technology

Laws have been enacted in recent years giving counter-drone authority to the Departments of Defense, Energy, Justice and Homeland Security. Passive drone-detection technology is not illegal if it does not interfere with air navigation or FCC-related spectrum. But active measures are prohibited by several longstanding Federal criminal laws. Violation of any of these laws carries a prison term.

- 18 U.S.C. 32 prohibits destruction or damage to an aircraft
- 49 U.S.C. 46502 prohibits the seizing or control of an aircraft by force or violence
- 18 U.S.C. 1030 prohibits access to a computer without authorization
- 18 U.S.C. Chapter 119 prohibits the interception of wire communications
- 18 U.S.C. Chapter 206 prohibits trap and trace devices without a court order
- 18 U.S.C. 1367 prohibits obstructing or interfering with a satellite transmission

Drone operator qualification requirements

Commercial drone operations must be conducted by an individual who has obtained a remote pilot certificate with small UAS rating or who holds a Part 61 airman certificate. To obtain a remote pilot certificate, the individual must pass an aeronautical knowledge and safety test, covering the subjects listed in 14 CFR 107.73, but is not required to pass any flight test. In the OOP final rule, the FAA decided to allow remote pilot certificate holders to complete online training in lieu of passing a recurrent knowledge test.

In 2018, Congress[193] required recreational drone pilots to pass an online aeronautical knowledge and safety test administered by the FAA or a person designated by the Administrator.

Developments

As required by Congress in 2016[194] and in 2018[195], FAA is expected to publish a proposed rule to establish a process to receive and approve requests to restrict drone operations above and near critical infrastructure facilities.

FAA has established a BEYOND program, as a successor to the FAA UAS Integration Pilot Program (IPP), which expired in October 2020. This program is intended to develop standards for BVLOS operations, which will include DAA technology. It is also expected to engage with local communities.

In March 2022, the FAA-established Beyond Visual Line of Sight Aviation Rulemaking Committee (BVLOS ARC) issued a final report and recommendations. FAA has stated that it intends to promulgate several rules to implement the BVLOS ARC recommendations and to authorize BVLOS operations for package delivery, inspection and agricultural operations. No proposed rule has been issued as of this date.

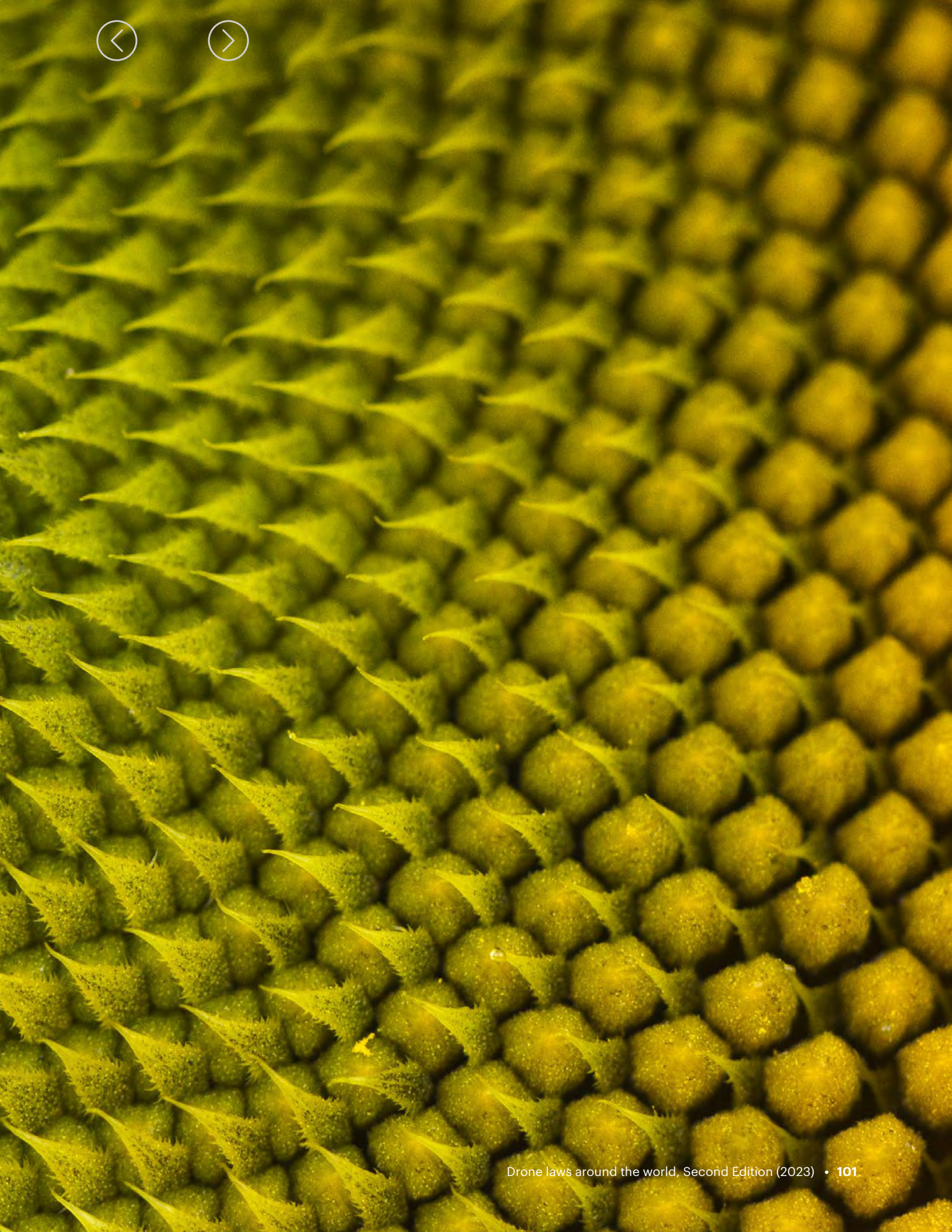
As noted, FAA is working to establish special class airworthiness standards for small UAS models that would support type and airworthiness certification of small drones. The FAA is working on a proposal to cover drones, as well as light sport aircraft in the Modernization of Special Airworthiness Certificates (MOSAIC) rulemaking.

action against any company that produces a drone before December 16, 2022 that is not subject to an FAA-accepted Declaration of Compliance.

193 Section 349 of the FAA Reauthorization Act of 2018.

194 Section 2209 of the FAA Extension, Safety, and Security Act of 2016.

195 Section 369 of the FAA Reauthorization Act of 2018.



Dentons' Comprehensive Legal Services for Drone Operations

No matter where you are in the drone industry, Dentons is with you. Seize the opportunities presented by ensuring profitable, safe and compliant drone operations with comprehensive and proactive legal advice at any stage.

Corporate governance

- Corporate structuring
- Contract drafting
- Internal policies
- User manuals

Risk mitigation

- Litigation
- Regulatory charges
- IP protection

Regulatory compliance

- Drone regulations
- Aeronautics statutes
- Municipal bylaws

Growth

- Financing
- Insurance
- Leasing
- Emerging company support

Data collection and privacy

- Data collection policies
- Cybersecurity
- Privacy breach support

About Dentons

160+
locations

80+
countries

Locations in purple represent Dentons offices.
Locations in blue represent associate firms, offices, jurisdictions of practice from other Dentons' offices or special alliances as required by law or regulation.
Locations in green represent approved combinations that have not yet been formalized.
Locations in gray represent Brazil Strategic Alliance.

80+
languages spoken

US$47,250,000+
value of pro bono and volunteer work

5,900+
Total number of lawyers and professionals

7,490+
All timekeepers

12,500+
Total number of people

Key contacts

Canada

Kathryn McCulloch
Partner, Toronto
D +1 416 863 4385
kathryn.mcculloch
@dentons.com

USA

Gregory S. Walden
Dentons Global Advisors
Washington DC
D +1 202 496 7436
gregory.walden@
dentonsglobaladvisors.com

Australia

Ben Allen
Partner, Sydney
D +61 2 9035 7257
ben.allen
@dentons.com

Anson Pang
Senior Associate, Sydney
D +61 2 9035 7279
anson.pang
@dentons.com

France

Dorothée Griveaux
Partner, Paris
D +33 1 42 68 44 56
dorothee.griveaux
@dentons.com

Roxanne Leclercq
Associate, Paris
D+33 1 42 68 93 91
roxanne.leclercq
@dentons.com

New Zealand

Gunes Haksever
Partner, Auckland
D+64 9 375 1161
gunes.haksever
@dentons.com

Hayley Miller
Partner, Auckland
D+64 9 915 3366
hayley.miller
@dentons.com

Germany

Dr. Ilka D. Mehdorn
Office Managing Partner, Berlin
D+49 30 2 64 73 802
Ilka.Mehdorn
@dentons.com

Italy

Giangiacomo Olivi
Partner and Europe Co-Head of Intellectual Property, Data and Technology, Milan
D+39 02 726 268 00
giangiacomo.olivi
@dentons.com

Antonio Venditti
Associate, Milan
D+39 02 726 268 00
antonio.venditti
@dentons.com

Korea

Kurt Gerstner
Partner, Seoul
D+82 2 2262 6078
kurt.gerstner
@dentons.com

Singapore

Melvin See
Senior Partner, Singapore
D +65 6885 3701
melvin.see
@dentons.com

United Kingdom

Tristan Jonckheer
Partner, London
D+44 20 7246 7089
tristan.jonckheer
@dentons.com

Matthew Gilhooly
Associate, London
D+44 20 7320 6329
matthew.gilhooly
@dentons.com

Andrew Lee
Associate, Seoul
D+82 2 2262 6292
andrew.lee
@dentons.com

ANDERSON MŌRI & TOMOTSUNE

Japan

Eiji Kobayashi
Partner, Tokyo
D +81-3-6775-1074
eiji.kobayashi
@amt-law.com

Yutaro Takahashi
Associate, Tokyo
T: +81-3-6775-1359
yutaro.takahashi
@amt-law.com

ABOUT DENTONS

Across over 80 countries, Dentons helps you grow, protect, operate and finance your organization by providing uniquely global and deeply local legal solutions. Polycentric, purpose-driven and committed to inclusion, diversity, equity and sustainability, we focus on what matters most to you.

www.dentons.com

CSBrand-66216-Global Comparative Drone Guide_18 — 22/08/2023