IFR Drones Ltd/Moonrock Drone Insurance – privacy policy updated May 2018

Contents

Privacy Policy Summary

IFR Drones Ltd, trading as Moonrock Drone Insurance, is an insurance business, and as such is a holder and processor of personal data. IFR Drones Ltd generates its revenue through the sales of niche and specifically worded policies designed for clients and prospective clients, namely commercial drone pilots, who are already operating or may intend to operate commercially using drones, (which are also known as UAV's – Unmanned Aerial Vehicles, SUA's – Small Unmanned Aircraft and RPAS – Remotely Piloted Aircraft System). These EU compliant policies, which were the first in the UK to be built with non-aviation policy wordings, relate to highly specific insurance needs for the nascent drone industry, which are legally obliged to be held by all such clients. IFR Drones Ltd is an appointed representative of Christopher Trigg Ltd, which is authorised and regulated by the Financial Conduct Authority (FCA) – reference number 121488.

A client is further defined as an individual who has previously indicated that they are interested in engaging with IFR Drones Ltd (T/A Moonrock Drone Insurance) with the purpose of us finding them a suitable and legally compliant insurance policy for all their drone operations. Clients will often submit details, which are required for IFR Drones Ltd to comply fully with FCA regulation regarding all policies.

IFR Drones Ltd – **henceforth in this privacy policy to be referred to by its trading name, Moonrock Insurance** is committed to protecting your and your family's personal information.

This Privacy Policy relates to our use of any personal information we collect from you via the following online services:

- Any Moonrock Insurance website that links to this Policy ("Websites");
- Social media or Moonrock Insurance content on other websites;
- Mobile device and TV applications ("Apps");

It also relates to our use of any personal information we collect through other means, such as email, in person or other third party sources.

The information we collect and how we collect it - Information you provide to Moonrock Insurance

We may receive personal information about you, when you contact Moonrock Insurance for example by doing any of the following:

- Requesting or obtaining a quote
- Purchasing a Moonrock Insurance product from us or from one or our partners
- Using the Websites and Apps
- Entering Moonrock Insurance competitions
- Using live chat
- Creating a personal login account (such as one to view/amend your insurance details)
- Telephoning, texting, writing by post or email, or communicating via online channels, such as online chat, to Moonrock Insurance

This information may include:

- Basic personal details such as your name, address, e-mail address, telephone number, date of birth.
- Additional information about your lifestyle and insurance requirements, such as details your home/business, your household, where you intend to operate and any previous legal charges
- Information about your other policies, such as claims history, quotes history.
- Sensitive personal information such as, but not limited to, disclosures about previous criminal convictions.
- Information about your company/employment, including expected turnover
- Your marketing preferences

Information collected from third parties

We use information about you or the operations we insure for you, from publicly available sources such as (but not limited to) the below:

- The CAA's list of Small Unmanned Aircraft (SUA) operators holding a valid CAA permission
- LinkedIn

How we use information to help you

- Administer quotes and policies, including to:
    - improve your experience by reducing the number of questions we need to ask you
    - assess your application for a product, service or quote,
    - understand your risk so as to offer you our best price
    - verify your identity and carry out anti-fraud checks,
    - provide you with premium and payment options,
    - administer your policy, including updating you on and delivering our services
    - handle claims
    - deal with complaints
    - reconnect with you if you move employer or address
- Identify which products may be of interest to you and provide you with information about those products.
- Provide you with tailored offers.

- Offer enhanced services where we believe this would be helpful or of interest e.g. but not limited to, PFCO renewal reminders.

How we share your information outside of the Moonrock Insurance

If you request a quote, or purchase a product or service, your personal information may be shared with and processed by our associated companies, introducers, intermediaries, reinsurers, underwriters and agents, as well as the policy holder (for a corporate policy) and your broker or agent for the purposes of administration.

Your information may be disclosed when we believe in good faith that the disclosure is:

- required by law;
- to protect the safety of our employees, the public or Moonrock Insurance property;
- required to comply with a judicial proceeding, court order or legal process; or
- in the event of a merger, asset sale, or other related transaction; or
- for the prevention or detection of crime (including fraud).

We may share your information with regulatory bodies in the UK or if applicable, overseas, as well as with other insurance companies (directly or via shared databases) to prevent and detect fraud.

Security

We are committed to protecting the confidentiality and security of the information that you provide to us and we put in place appropriate technical, physical and organisational security measures to protect against any unauthorised access or damage to, or disclosure or loss of, your information. You should also be aware that communications over the internet, such as e-mails, are not secure unless they have been encrypted. The Websites may contain links to other Moonrock Insurance and other third party websites. These other websites will be subject to their own privacy policies, which may differ from this Privacy Policy. You should carefully read the privacy policies of these websites before submitting any personal information.

A. Reasons for holding and processing data – "bind policies"

- Moonrock Insurance hold / process data in order to "bind policies" for our clients
- The term "binding policies" is explained as the process whereby binding is, by definition, the act of imposing a duty to keep a commitment. In the insurance industry, binding refers to insurance coverage, and means that coverage is in place, although a policy has yet to be issued.
- In order to bind a policy we need to hold / process data to review a client's eligibility for drone insurance and to assess each client's risk level
- There is an implicit need for us to occasionally share such data with our underwriters in order for them to assess each client's risk level, and for them to ultimately decide whether to agree to bind such client's policies.
- Payment for such policies, by monthly direct debit or otherwise requires us to hold /process data which we share with such facilitators to enable us to "bind policies"
- Such data holding and processing is necessary for compliance for our legal obligation and FCA compliance both of which we need to uphold to "bind policies"

B. Reasons for holding and processing data – "insurance advisory"

- We will identify which products may be of interest to you and provide you with information about those products.
- Provide you with tailored offers.
- Offer enhanced services where we believe this would be helpful or of interest e.g. but not limited to, PFCO renewal reminders.
- As insurance for commercial drone operators is a legal requirement from time to time we may need to update you about any changes with respect to the mandatory insurance
- We may from time to time update our products in accordance with such rules and may even change underwriters and therefore the wording or offerings on our policy – the drone industry is still so nascent that policies are being revised and updated at all times and there is a constant legitimate business interest in informing our clients and potential clients about such details.

C. Legitimate business interest in holding and processing data

- Moonrock Insurance will hold / process data to facilitate the effective introduction of clients, commercial drone pilots and prospective clients to suitable insurance policies.
- A client is defined as an individual who has previously indicated that they are interested in engaging with IFR Drones Ltd (T/A Moonrock Drone Insurance) with the purpose of us finding them a suitable and legally compliant insurance policy for all their drone operations. Clients will often submit details, which are required for IFR Drones Ltd to comply fully with FCA regulation regarding all policies.
- A commercial drone pilot is someone who is or recently has been listed on the CAA's list of Small Unmanned Aircraft (SUA) operators holding a valid CAA permission often referred to as a PFCO, or someone introduced to us by a third party (prospective client) such as an NQE (National Qualified Entity) who are specifically permitted to give potential commercial drone pilots the legally required training and assessments to determine whether or not they are apposite individuals or companies to apply to the CAA to receive their PFCO
- A prospective client may additionally be defined as someone with whom we have been introduced to via social media or an individual with whom we have LinkedIn with
- The process of introducing a client, commercial drone pilots or prospective clients to our legally required and legally compliant policies is considered the core nature of Moonrock Insurance's business. By definition, it is a legitimate business interest of Moonrock Insurance to assist clients/customers or potential clients/customers to us "binding policies" and this would be impossible without the holding / processing of their details (with their consent) and having the ability to pass these on to our underwriters, and our payment service providers.
- Moonrock Insurance will contact clients and prospective clients so that they might be aware of valuable market information relating to attracting and retaining compliant insurance policies.

D. The right to rectify information, withdraw consent or complain

- You will at any stage have the right to rectify your information
- In order to rectify information, please contact your Moonrock consultant by email requesting which information you need to change. If you do not hear back from your Moonrock consultant within 48 hours then please contact Chris Johnson on 01923 712441 chris@moonrockinsurance.com . If you do not hear back from Chris Johnson within 48 hours

then please contact Alan Lok alan@moonrockinsurance.com or Simon Ritterband simon@moonrockinsurance.com
- If you do not know the name of your Moonrock consultant then in the first instance please contact Chris Johnson, our GDPR Manager
- You can change your preferences at any stage through the preference centre (found either on our website or on any email communication we send to you). Here is a link to our preference centre www.moonrockinsurance.com/change_preferences
- Information regarding this will be available easily on our website and in email format should anyone request it

You will at any stage have the ability to withdraw consent

- In order to withdraw consent, please contact your Moonrock consultant by email requesting that you no longer wish for us to handle / process your data. If you do not hear back from your Moonrock consultant with 48 hours then please contact Chris Johnson on 01923 712441 chris@moonrockinsurance.com . If you do not hear back from Chris Johnson within 48 hours then please contact Alan Lok alan@moonrockinsurance.com or Simon Ritterband simon@moonrockinsurance.com
- If you do not know the name of your Moonrock Insurance consultant then in the first instance please contact Chris Johnson
- This process is fully outlined in our privacy policy on our website which you can access via this link https://www.moonrockinsurance.com/Policies/Privacy_policy_Moonrock.pdf

You will at any stage have the ability to complain

- In order to complain, please send an email to Chris Johnson and cc'ing Alan Lok and Simon Ritterband outlining your complaint (email addresses are listed below)
- This email will be responded to within 48 hours
- Chris Johnson 01923 712441 chris@moonrockinsurance.com
- Alan Lok 01923 712441 alan@moonrockinsurance.com
- Simon Ritterband simon@moonrockinsurance.com
- This process is fully outlined in our privacy policy on our website which you can access via this link https://www.moonrockinsurance.com/Policies/Privacy_policy_Moonrock.pdf

E. Data Retention Policy

This data retention policy sets out the obligations of **IFR Drones Ltd** T/A Moonrock Drone Insurance and the basis upon which we shall retain, review and destroy data held by us, or within our custody or control.

This policy applies to our entire organisation including our officers, employees, agents and sub-contractors and sets out what the retention periods are and when any such data may be deleted.

We are registered under the Information Commissioner's Office under registration number **ZA137065**

Objectives

It is necessary to retain and process certain information to enable our business to operate. We may store data in the following places:

- our own servers;
- any third-party servers;
- potential email accounts;
- desktops;
- employee-owned devices (BYOD);
- potential backup storage; and/or
- our paper files.

This policy applies equally to paper, electronic media and any other method used to store personal data. The period of retention only commences when the record is closed.

We are bound by various obligations under the law in relation to this and therefore, to comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully in respect of their personal data under the General Data Protection Regulation ("the Regulation").

The Regulation defines "personal data" as any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person. This Policy sets out the procedures that are to be followed when dealing with personal data and how we aim to comply with the Regulation in so far as it is possible. In summary, the Regulation states that all personal data shall be:

a) processed lawfully, fairly, and in a transparent manner in relation to the data subject;

b) collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the Regulation in order to safeguard the rights and freedoms of the data subject;

f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The Fourth and Fifth Data Protection Principles require that any data should not be kept longer than necessary for the purpose for which it is processed and when it is no longer required, it shall be deleted and that the data should be adequate, relevant and limited for the purpose in which it is processed.

With this in mind, this policy should be read in conjunction with our other policies which are relevant such as our data protection policy and IT security policy.

Security and Storage

All data and records are stored securely to avoid misuse or loss. We will process all personal data we hold in accordance with our IT Security Policy [**OR** take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data].

We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if there is agreement by them to comply with those procedures and policies, or if there are adequate measures in place.

We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

(a) **Confidentiality** means that only people who are authorised to use the data can access it.

(b) **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.

Availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on the Moonrock Insurance's central computer system instead of individual PC's.

From time to time, it may be necessary to retain or access historic personal data under certain circumstances such as if we have contractually agreed to do so or if we have become involved in unforeseen events like litigation or business disaster recoveries.

Destruction and Disposal

Upon expiry of our retention periods, we shall delete confidential or sensitive records categorised as requiring high protection and very high protection, and we shall either delete or anonymise less important documents.

Our team including Chris Johnson, Alan Lok, Simon Ritterband (or any other members of the back office support team at Moonrock Insurance) are responsible for the continuing process of identifying the records that have met their required retention period and supervising their destruction. The destruction of confidential, financial, and personnel-related records shall be securely destroyed electronically or by shredding if possible. Non-confidential records may be destroyed by recycling.

F. Record table for retaining / holding data and data purging timelines

Moonrock Insurance are an insurance policy selling business with a legitimate business interest in holding / processing data. Listed below is a schedule of the type of data we hold, the reason we hold it and the length of time we will retain it. Definitions of different categories of individual whose data Moonrock Insurance hold:

- **Policy Holder:** a client who we are currently working with, have historically worked with or who we may work with

- **Inactive (passive/prospective) client:** a client who we have historically worked with or who we have tried to work with but who hasn't been in contact with us for more than 2 years

- **Current IFR Drones Ltd T/A Moonrock Drone Insurance employee:** an individual who is currently employed by IFR Drones Ltd

- **Historic IFR Drones Ltd T/A Moonrock Drone Insurance employee:** an individual who was historically employed by IFR Drones Ltd

- **Individual Client:** a client holding an active policy with us, who we are currently insuring

Type of data	**Data purging timescale**
Policy Holder	7 years from last contact with client
Inactive (passive/prospective) client	removed after 3 further years of no contact with client
Current IFR Drones Ltd employee	not applicable
Historic IFR Drones Ltd employee	removed 15 years after employment ceased
Individual Client data	removed 7 years after expiration of last policy held with us if no contact from individual client

G. Data purging process

- Every month we will carry out a search of the entire candidate database and remove all those inactive (historic) clients and prospective clients who have not been in contact with us for more than 5 years
- All purged details will be fully deleted from Moonrock Insurance's database and will be non-accessible thereafter

H. Cookies policy, websites terms of use and privacy / transparency policy

We collect information through "Cookies" and other similar technologies (e.g. pixel tags or links), to remember you when you visit the Websites and Apps and so we can improve your online experience to suit your needs. These help us understand how you and others use our Websites and Apps, view our products and respond to our advertising, so we can tailor direct marketing and enhance our overall product and service offering. This also saves you from re-inputting information when you return to the Websites or Apps. When you receive direct marketing from us via email, we may use technology e.g. pixel tags or links to determine your use of and interest in our direct marketing.

This information is retained and used to note your interest in our Websites and Apps, improve customer use experience, determine pricing and/or offer you available discounts.

- To find out more this information can be found on our website or via this link https://www.moonrockinsurance.com/cookies

I. Preference settings / opt in / opt out / unsubscribe links on emails

Managing your marketing preferences

We may:

- provide you with updates and offers for Moonrock Insurance's products and services via marketing tailored to you, whether on your personal login, through online digital services (e.g. online advertising, social media communications), or by direct marketing (e.g. phone, e-mail, text, post); and
- use information we hold about you to help us identify, tailor and package our products and services, determine pricing and offer discounts that may be of interest to you.

We will always give you the opportunity to 'opt out' of direct marketing when you complete a registration with us, request an online quote, purchase a product or service online or receive any email, text or other direct marketing communication.

You can change your marketing preferences at any other time by contacting us on the details given

If you are logged in to your insurance details, we would like to provide you with customised quotes and offers. If you would rather not see these offers, you can change your preference at any time within the Profile section of the login. If you choose to opt out of this type of tailored marketing, you will still see general marketing offers on Moonrock Insurance but will not see any offers that use your personal information. We will not use sensitive personal details (such as information relating to any criminal issues) in order to provide you with marketing, discounts or pricing unless you have given your explicit consent to allow us to use this information for these purposes.

- All emails from IFR Drones Ltd or Moonrock will have preference settings / opt in / opt out / unsubscribe links. These signatures are centrally managed whereby individual users cannot change, amend or edit prior to sending out. This ensures that any recipient of an email can effectively and easily manage how we (Moonrock Insurance) are using their data. This might include updating / changing their preferences or complete removal of all data

Updating your information or changing your marketing preferences

Please let us know if your information changes, as it is important that the information we hold about you is accurate and up to date. You can ask us to update or correct your personal information or opt out of Moonrock Insurance's use of your information for direct marketing purposes by contacting us using any of the following methods:

By Phone: 01923 712441 or +44 01923 712441 (from abroad)
By email: info@moonrockinsurance.com
By post: Moonrock Drone Insurance
1 Norfolk Court
Norfolk Road
Rickmansworth
Hertfordshire WD3 1LA

You can also choose whether you wish to see tailored offers within your login by changing your preferences within your Profile on your personal login.

J. Data protection policy

Our use of personal data and our purpose

Moonrock Insurance sell insurance policies with a legitimate business interest in holding / processing data. Listed below is a schedule of the type of data we hold, the reason we hold it and the length of time we will retain it. Definitions of different categories of data, which Moonrock Insurance may collect, hold and/or process are as follows:

- **Policy holder:** an individual who has held an insurance policy with IFR Drones Ltd T/A Moonrock Drone Insurance who can make a historical claim

- **Active client:** an individual who has previously indicated that they are interested in engaging with Moonrock Drone Insurance with the purpose of us providing them with a "binding policy". They will have submitted details in relation to specific insurance, so that we might be aware that they are keen on hearing about our policies in the future. An active client will be in "active dialogue" with us (by online form submission / email / telephone / text / LinkedIn / other social media platforms). This active dialogue will occur a minimum of once a year. We need to hold data for active clients so that we might provide them with industry updates including legal changes for drone usage and "binding policy" services.

- **Inactive (passive) client:** an individual who has previously indicated that they are interested in engaging with Moonrock Insurance with the purpose of us providing them with "binding policy services". An inactive (passive) client will not have been in contact with us / responded to any contact from us (by email / telephone / text / LinkedIn / other social media platforms) for more than one year but less than 5 years. We need to hold data for inactive (passive) candidates so that we might provide them with "binding policy services" even if they are not actively searching for our insurance (but who haven't withdrawn consent for us to hold their data)

- **Other Prospective Clients:** individuals who may have been introduced to us by specifically related third parties such as NQE's who specifically teach such individuals for the purpose of qualifying for legally required PFCO's as commercial drone pilots (but for the purposes of clarity not including individuals introduced who have no previous relation to drone piloting for the purpose of gaining a PFCO) or people made known to us by publicly published lists such as the CAA list of Small Unmanned Aircraft (SUA) operators holding a valid CAA permission or those who have LinkedIn (or engaged with us only regarding drone piloting and/or insurance via other social media) with us knowing that our (or our director's and employees) homepages in such places clearly demonstrate that we are niche insurers currently only operating to offer insurance for remotely operated vehicles (such as drones/UAV's)

We will keep Personal Information for as long as is necessary for the purposes for which we collect it. The precise period will depend on the purpose for which we hold your information. In addition, as a regulated financial services institution, there are laws and regulations that apply to us which set minimum periods for retention of Personal Information

For example:

- Where we hold Personal Information to comply with a legal or regulatory obligation, we will keep the information for at least as long as is required to comply with that obligation.
- Where we hold Personal Information in order to provide a product or service (such as an insurance policy and claims handling), we will keep the information for at least as long as we provide the product or service, and for a number of years after expiry of the policy and the handling of any related claim.

The number of years varies depending on the nature of the product or service provided – for example, for certain insurance policies it may be necessary to keep the Personal Information for several years after the expiry of the policy. Among other reasons, we retain the information in order to respond to any queries or concerns that may be raised at a later date with respect to the policy or the handling of a claim. Typically, for consumer insurance products, the retention period is seven 7 years.

For further information about the period of time for which we retain your Personal Information, please contact us using the details below

How to find out what information we hold about you

You have the right to request a copy of all the personal information we hold about you in a Subject Access Request. To do this, simply write to us at the address below enclosing a cheque for £10.00 payable to IFR Drones Ltd to cover our administrative costs in dealing with your request. We will take all reasonable steps to confirm your identity before providing you with details of any personal information we may hold about you.

IFR Drones Ltd T/A Moonrock Insurance
1 Norfolk Court
Norfolk Road
Rickmansworth
Hertfordshire WD3 1LA

Data Protection Policy In More Detail

Section A: Overview

1. The reason for this policy

1.2 You have legal rights with regard to the way your personal data is handled.

1.3 In the course of our business activities we collect, store and process personal data about our customers, suppliers and other third parties and therefore, in order to comply with the law and to maintain confidence in our business, we acknowledge the importance of correct and lawful treatment of this data.

All people working in or with our business are obliged to comply with this policy when processing personal data.

2. **Introduction**

2.1 This policy and any other documents referred to in it sets out the basis on which we will process any personal data we collect from data subjects, for example, customers

and business contacts, or that is provided to us by data subjects or other sources.

2.2 In this policy when we say "you' or "your" we are generally referring to the data subjects unless the context requires otherwise.

2.3 It also sets out our obligations in relation to data protection under the General Data Protection Regulation 2016 ("the **GDPR Rules**").

2.4 This policy sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.

2.5 We agree to ensure that all of our directors, employees, consultants and agents comply with this policy.

2.6 We aim to ensure the correct, lawful, and fair handling of your personal data and to respect your legal rights.

3. **The meaning of key Data Protection terms**

3.1 **data** is information, which is stored electronically, on a computer, or in certain paper-based filing systems.

3.2 **data subjects** for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

3.3 **personal data** means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

3.4 **data controllers** are the people who or organisations that determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the Act. We are the data controller of all personal data used in our business for our own commercial purposes.

3.5 **processing** is any activity that involves use of personal data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

4. **Summary of the Data Protection Principles**

This Policy aims to ensure compliance with the GDPR Rules. The GDPR Rules sets out the following principles with which any party handling personal data must comply. All personal data must be:

a) **Processed fairly and lawfully** – it must be processed fairly and lawfully and it must be processed - in relation to you as the data subject - in a transparent manner

b) **Processed for limited purposes and in an appropriate way -** the purposes for which it is collected must be explicit, specified and legitimate

c) **Adequate, relevant and not excessive for the purpose**

d) **Accurate** – as well as being accurate it must be kept up to date with inaccurate data deleted

e) **Not kept longer than necessary for the purpose**

f) **Processed in line with data subject's rights**

g) **Security** – there must appropriate technical or organisational measures to ensure appropriate security

In addition, personal data must not be transferred outside the European Economic Area (the "**EEA**") without **adequate protection.**

Section B: Data Protection Principles

5. **Notifying Data Subjects**

5.1 As part of complying with the principles in para 4 above, if you provide us with personal data we will always try to tell you:

5.1.1 the purpose or purposes for which we intend to process that personal data

5.1.2 the types of third parties, if any, with which we will share or to which we will disclose that personal data

5.1.3 how you can limit our use and disclosure of their personal data

5.1.4 if we receive personal data from other sources.

6. **Lawful, Fair, and Transparent Data Processing**

The GDPR Rules are not intended to prevent the processing of personal data but to ensure that it is done fairly and without adversely affecting your rights. The processing of personal data is lawful if one (or more) of the following applies:

a) **(consent)** the data subject has consented for a specific purpose;

b) **(contract**) if the data subject requests the processing with a view to entering into a contract or the processing is necessary for the performance of a contract

c) **(legal obligation)** if the processing is necessary for the compliance with a legal obligation to which the data controller is subject

d) **(protection)** processing is necessary to protect your vital interests or those of another natural person

e) **(public interest)** it is in the public interest for a task to be carried out which requires such processing, or the task is to be carried out as a result of the exercise of any official authority held by the data controller;

f) **(legitimate interests)** for the legitimate interest of the data controller or the party to whom the personal data is disclosed.

7. **Processed for limited purposes and in an appropriate way**

7.1 In the course of our business, we may collect and process the personal data set out above. This may include personal data we receive directly from you (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, business partners, sub-contractors in technical, payment and delivery services, credit reference agencies and others).

7.2 We will only process personal data for the specific purposes set out above or for any other purposes specifically permitted by the GDPR Rules. We will notify those purposes to you when we first collect the personal data or as soon as possible thereafter.

8. **Adequate, Relevant and not excessive for the purpose**

We will only collect and process personal data for the specific purpose(s) set out above.

9. **Accuracy of Data and Keeping Data Up To Date**

We will keep your personal data accurate and up-to-date. We will check its accuracy regularly. When we find inaccurate or out-of-date data we will take reasonable steps to amend or erase that data.

10. **Timely Processing**

We will only keep your personal data for a period of time which we judge is relevant and necessary taking into account the purpose(s) of collecting the personal data which are specified above.

11. **Processing that is secure**

In addition to the measures above:

11.1 we will make sure that the personal data we collect is securely kept and we stop unauthorised processing and prevent its loss, destruction or damage

11.2 we will ensure that only people who are authorised to use personal data can access it and that we have entry controls to our premises and systems, lockable desks and cupboards for confidential personal data and destruction of hard copy documents and digital storage devices

11.3 all authorised persons must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

Section C: Data Subject Rights

12. You, as a data subject, have the right to information about:

a) who we are

b) the purpose(s) of collecting your personal data and the legal basis for collecting it and what our legitimate interest is for processing your personal data

c) the categories of personal data collected and where is to be transferred, especially if outside the EEA

d) the length of time we hold personal data (or, where there is no predetermined period, details of how that length of time will be determined)

e) your rights as a data subject including your right to withdraw your consent to processing, the right to complain to the Information Commissioner and also things such as details of any legal requirement for processing personal data that may exist and any automated decision-making that we carry out.

We will try to provide this information when we collect the personal data or, if we collect the personal data from another party, when we communicate with you after the personal data is received.

13. **Data Subject Access**

13.1 You may request access to any data held about you by us (a subject access request ("**SAR**")

13.2 We reserve the right to charge reasonable fees for onerous or repetitive requests.

13.3 Data subjects must make a formal request for information we hold about them. This must be made in writing.

13.4 When receiving telephone enquiries, we will only disclose personal data we hold on our systems if the following conditions are met:

a) we will check the caller's identity to make sure that information is only given to a person who is entitled to it.

b) we will suggest that the caller put their request in writing if we are not sure about the caller's identity and where their identity cannot be checked.

14. **Accuracy of personal data: right to rectification**

14.1 We will do our best to ensure that all personal data held about you is accurate and complete. We ask that you notify us of any changes to information held about you.

14.2 You have the right to request that any incomplete or inaccurate information held about you is rectified and to lodge a complaint with us and the Information Commissioner's Office.

14.3 We will respond to requests to rectify within one month.

15. **Right to be forgotten**

You have the right to request the deletion or removal of personal data however requests for erasure can be rejected in certain circumstances.

16. **Right to restriction of Processing**

You can block the processing of your personal data. This means we may be able to store it, but cannot process it further without consent. Restricting data is required where the accuracy of data is challenged - but only until the accuracy has been verified.

17. **Right to data portability**

17.1 If you have provided personal data to us you have the right to transfer it from us to someone else.

17.2 If you request it, we may be required to transmit the data directly to another organisation if feasible. We must respond without undue delay and within one month, or two months if the request is complex.

18. **The right to object**

You have a right to object to the processing of your data. We must stop processing unless we can demonstrate a legal ground for the processing.

19. **Automated decision-making**

19.1 You have the right not to be subject to a decision based on automated processing and it produces a legal effect or other significant effect on you.

19.2 You can request human intervention where personal data is processed using automated decision-making and can ask for an explanation of the decision to use automated decision-making.

20. **Profiling**

If we use your personal data for profiling purposes:

a) We will give you information fully explaining the profiling which will be carried out including its importance and the likely results of that profiling;

b) We will make sure that appropriate mathematical or statistical procedures will be used;

c) We will implement technical and organisational measures which are required to minimise the risk of mistakes and to enable such mistakes to be easily corrected; and

d) We will make sure that all personal data processed by us for profiling purposes will be kept secure so as to avoid discriminatory effects resulting from such profiling.

Section D: Our Other Obligations

21. **How we deal with personal data internally**

21.1 We will:

a) train our employees in relation to our responsibilities under the GDPR Rules

b) ensure that only appropriately trained, supervised and authorised personal have access to personal data held by us; and

c) regularly evaluate and review our collection and processing of personal data and the performance of employees and third parties working on our behalf to ensure that it is in accordance with the GDPR Rules.

21.2 We will keep internal records of personal data that we collect and process including, in relation to that personal data, details of the categories, any transfers, our security measures, our purpose of collection and the duration of retention of that personal data. We will also retain details of all third parties that either collect your personal data for us or that we use to process your personal data.

21.3 We will carry out privacy impact assessments as required by law.

22. **Transferring personal data to a country outside the EEA**

We may transfer personal data to countries outside of the EEA however we will ensure that the transfer is:

a) to a place that the EU has judged to provide adequate levels of protection for personal data

b) to a place that provides adequate safeguards under either an agreement with a public body, rules that bind companies or standard data protection clauses adopted by the EU or some other form of approved code of conduct approved by a supervisory authority or certification or other contractual clauses or regulatory provisions

c) necessary for the performance of a contract between you and us or with a view to creating that contract

d) made with your consent

e) necessary for important public interest reasons, legal claims, to protect your vital interests

23. **Notification of personal data security breach**

23.1 If a personal data security breach occurs, we will manage and respond to it effectively in accordance with GDPR and it must be reported immediately to our Data Protection Officer.

23.2 We will notify the Information Commissioners Office (**ICO**) and any data subject of personal data security breaches to the extent we are required to do so by GDPR.

23.3 If disclosure is not required by GDPR, we will nevertheless investigate closely all the circumstances surrounding the breach and examine the seriousness of the breach and the benefits that might be obtained by disclosure (such as limiting risks of fraud) and we will give careful consideration to any decision to notify the ICO or you, especially if your rights and freedoms as data subjects are affected.

K. Data Security Policy

1. **Introduction**

The security and integrity of their IT Systems is a priority for IFR Drones Ltd / Moonrock Insurance (the "Company"). All employees of the Company and any authorised third parties, including without limitation, sub-contractors, consultants and contractors (together "Users") are expected to comply with this Policy, which is effective from the date above, but subject to being updated from time to time.

2. **Intended purpose**

The purpose of this Policy is to establish a framework for managing risks and protecting the Company's IT infrastructure, computing environment, hardware, software and any and all other relevant equipment ("IT Systems") against all types of threats, internal or external, intentional or unintentional.

3. **Stakeholder Responsibilities**

3.1 **IS2** (the "IT Department" as of May 2018) shall be responsible for carrying out the installation, ongoing maintenance (including without limitation, any upgrades or repairs) and ensuring the security and integrity of the IT Systems, either directly or, via an authorised third party. Accordingly, the IT Department is responsible for data stored on the IT system unless otherwise stated.

3.2 In furtherance of section 3.1 above, the IT Department shall be responsible for:

(a) investigating any security breaches and / or misconduct, and shall escalate to Chris Johnson or Simon Ritterband as appropriate;

(b) regularly reviewing IT security standards within the Company and ensuring the effective implementation of such standards, by way of periodic audits and risk assessments, with regular reports being made to the Company's internal senior management shall be responsible on the condition of the Company's information security and compliance with this Policy;

(c) ensuring organisational management and dedicated staff responsible for the development, implementation and maintenance of this Policy;

(d) providing assistance as necessary to Users to help them in their understanding and compliance with this Policy, as well as keeping all Users aware and up to date with all applicable laws including, without limitation, the GDPR and the Computer Misuse Act 1990.

(e) providing adequate training and support in relation to IT security matters and use of the IT Systems, to all Users
(f) ensuring that the access to IT Systems granted to all Users takes into account their job role, responsibilities and any additional security requirements, so that only necessary access is granted for each User
(g) dealing with all reports, whether from Users or otherwise, relating to IT security matters and carrying out a suitable response for the situation
(h) implementing appropriate password controls, as further detailed in section 5.
(i) maintaining a complete list of all hardware items within the IT Systems. All such hardware shall be labelled and the corresponding data shall be kept by the IT Department;
(j) ensuring that backups of all data stored within the IT Systems are taken, and that all such backups are stored off the Company premises at a suitably secure location; and
(k) ensure compliance with all IT security standards set out in ISO 27001, to the extent such standards are not covered by the obligations set out in section 3.2 (a) – (j)].

3.3 The Users shall be responsible for:
(a) informing the IT Department immediately of any actual or potential security breaches or concerns relating to the IT Systems;
(b) informing the IT Department immediately in respect of any technical or functional errors experienced relating to the IT Systems; and
(c) complying with this Policy and all laws applicable to the Users relating to their use of the IT Systems.

3.4 Users must not attempt to resolve an IT security breach on their own without consulting the IT Department first.

4. **Access to IT Systems**

4.1 There shall be logical access controls designed to manage electronic access to data and IT System functionality based on authority levels and job functions, (e.g. granting access on a need-to-know and least privilege basis, use of unique IDs and passwords for all Users, periodic review and revoking/changing access promptly when employment terminates or changes in job functions occur).

4.2 All IT Systems shall only be accessible by a secure log-in system as deemed suitable by the IT Department. Such suitable systems may include, without limitation, secure passwords, fingerprint identification and facial recognition.

4.3 The IT Department shall conduct regular system audits or event logging and related monitoring procedures to proactively record User access and activity on the IT Systems for routine review.

4.4 IT Systems that are not intended to be part of everyday use by most Users (including without limitation, servers, networking equipment and infrastructure) and any other areas where personal data may be stored (e.g. data centre or server room facilities) shall be designed to:

(a) protect information and physical assets from unauthorised physical access;

(b) manage, monitor and log movement of persons into and out of the relevant facilities; and
(c) guard against environmental hazards such as heat, fire and water damage.

5. **Passwords**

5.1 The IT Department shall implement password controls designed to manage and control password strength, expiration and usage including prohibiting Users from sharing passwords and requiring that the Company passwords that are assigned to Users:
(a) be at least 3 characters in length,
(b) not be stored in readable format on the Company's IT Systems;
(c) must be changed every 365 days;
(d) must have defined complexity;
(e) must have a history threshold to prevent reuse of recent passwords; and
(f) newly issued passwords must be changed after first use.

5.2 Users must keep passwords confidential and not share it with anyone else.

6. **Hardware**

6.1 All Company mobile devices, (including, without limitation, laptops, tablets and mobile telephones), should be kept securely by Users using secure cases, where appropriate. Users should not leave such mobile devices unattended other than at their homes or Company premises.

6.2 All Company non-mobile devices (including, without limitation, desktop computers, workstations and monitors) shall, wherever possible and practical, be secured in place with a suitable locking mechanism.

6.3 Users are not permitted to connect any of their personal hardware to the IT Systems without the express approval of the IT Department in writing.

7. **Software**

7.1 All software installation on to the IT Systems shall be the responsibility of the IT Department. Users are not permitted to install any software on to the IT Systems unless expressly approved in writing by the IT Department.

7.2 All software installed on to the IT Systems shall be kept sufficiently up to date in order to ensure that the security and integrity of the IT Systems is not compromised.

8. **Vulnerability Assessment and Anti-Virus**

8.1 The IT Department shall carry out regular vulnerability assessments, and utilise patch management, threat protection technologies and scheduled monitoring to identify, assess, mitigate and protect against identified security threats, viruses and other malicious code.

8.2 The IT Department shall ensure that the Company uses an up to date reputable anti-virus checking software tool to check the IT Systems and to scan all email attachments before they are opened.
Users may download files from any cloud storage systems, subject to prior approval from the IT Department; and Users shall permit any such files to be scanned for viruses as part of the download process.

8.3 The IT Department shall implement network security controls that provide for the use of enterprise firewalls and layered DMZ architectures, and intrusion detection systems and other traffic and event correlation procedures designed to protect systems from intrusion and limit the scope of any successful attack.

9. **Data Protection**

9.1 The collection, holding and processing of all personal data (as defined in the General Data Protection Regulation 2016("GDPR")) by the Company will be carried out in compliance with (i) the GDPR and (ii) the Company's own Data Protection Policy.

9.2 The IT Department shall ensure there are data security controls which include at a minimum, but may not be limited to, logical segregation of data, restricted (e.g. role-based) access and monitoring, and utilisation of commercially available and industry standard encryption technologies for personal data that is:

(a) transmitted over public networks (i.e. the Internet) or when transmitted wirelessly; or

(b) at rest or stored on portable or removable media (i.e. laptop computers, CD/DVD, USB drives, back-up tapes).

9.3 All emails containing personal data must be encrypted

9.4 Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted.

9.5 Where personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data.

9.6 If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it.

9.7 No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the letter and spirit of this Policy and of GDPR (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken).

9.8 The IT Department shall ensure operational procedures and controls to provide to provide for the secure disposal of any part of the IT Systems or any media to render all information or data contained therein as undecipherable or unrecoverable prior to final disposal or release from the Company's possession.

9.9 Where any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. Hardcopies should be shredded, and electronic copies should be deleted securely

9.10 The IT Department shall ensure that it has in place appropriate technical and organisational measures, to protect against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data, appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures (those measures may include, where appropriate, pseudonymising and encrypting personal data, ensuring confidentiality, integrity, availability and resilience of its systems and services, ensuring that availability of and access to personal data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the technical and organisational measures adopted by it).

9.11 All personal data stored electronically should be backed up daily with backups stored onsite AND/OR offsite. All backups should be encrypted

9.12 All electronic copies of personal data should be stored securely using passwords and data encryption.

9.13 Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of Chris Johnson and/or Alan chris@moonrockinsurance.com or alan@moonrockinsurance.com to ensure that no data subjects have added their details to any marketing preference databases including, but not limited to, the Telephone Preference Service, the Mail Preference Service & the Email Preference Service. Such details should be checked at least annually

9.14 Only Users that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Company.

9.15 All Users that have access to, and handle personal data on the Company's behalf, shall adhere to the Company's Data Protection Policy.

10. **Business Continuity**

The Company shall have in place adequate business resiliency/continuity and disaster recovery procedures designed to maintain any information and the supply of any service and/or recovery from foreseeable emergency situations or disasters.

11. **Email and Internet**

Please refer to the Company's policy on Email and Internet usage in respect of email and internet use on the IT Systems

12. **Training**

Security awareness training for Users shall be provided by the IT Department. Training will be provided at different levels for different Users based on their role. Users may request retraining after 2 years

Breaches of this policy

If you consider that this policy has not been followed in respect of personal data about yourself or others you should raise the matter with your Chris Johnson, Alan Lok or Dominic Trigg.

- Chris Johnson 01923 712441 at chris@moonrockinsurance.com
- Alan Lok 01923 712441 alan@moonrockinsurance.com
- Dominic Trigg 01923 712441 dom@moonrockinsurance.com

L. Changes to this Privacy Policy

We may amend this Privacy Policy from time to time for example, to keep it up to date or to comply with legal requirements. You should regularly check this Privacy Policy for updates. If there will be any significant changes made to the use of your personal information in a manner different from that stated at the time of collection, we will notify you by posting a notice on our Website.

M. Staff training for GDPR

At all times we will train present and future staff to understand and act compliantly with all matters contained in this policy

- All staff will be trained on using Moonrock Insurance's CRM (Capsule) so that any clients/ prospective clients details are processed in compliance with GDPR
- All staff will be trained on using Moonrock insurance's CRM (Capsule) so that any client contact is made in a manner compliant with GDPR
- All staff will be trained as to what action to take in the event that any client/prospective client wishes to amend or rectify their information, withdraw consent or complain.
- in relation to the last point, all staff are aware of the following key internal contacts and that they need to inform the key contacts within 48 hours of any request
    - Chris Johnson 01923 712441 at chris@moonrockinsurance.com
    - Alan Lok 01923 712441 alan@moonrockinsurance.com
    - Simon Ritterband simon@moonrockinsurance.com