**Privacy Policy**

*Last updated: 01 June 2026*

**1. Introduction**

Your privacy and the security of your personal data are our top priority. We take them very seriously. We make every effort to ensure that the personal data of our Users is processed in accordance with the applicable provisions of Polish and EU law.

This Privacy Policy explains how we process the personal data of Users of our Services, and in particular:

- Who is the controller of your personal data
- What data we process and whether the processing of such data is necessary for the electronic services we provide
- For what purposes and on what legal basis we process data
- How long we process data
- What rights you have as a data subject
- To whom we disclose data
- How you can contact us

This Privacy Policy also fulfils the information obligations referred to in Articles 13 and 14 of the GDPR.

**2. Definitions**

For the sake of clarity and precision of this Privacy Policy, the following definitions are used:

| Term | Meaning |
|---|---|
| **Data** | personal data (described in detail in further sections of this Privacy Policy) of individuals to whom the information obligation is fulfilled through the ongoing provision of information contained in this Privacy Policy; |
| **Client** | the end-user of the Service who has entered into an agreement with the Controller. Publicly available data of Users is made available to the Client; |
| **We / Controller** | UAV Labs spółka z ograniczoną odpowiedzialnością with its registered office in Olsztyn, ul. Towarowa 20B, entered into the Register of Entrepreneurs kept by the District Court in Olsztyn, 8th Commercial Division of the National Court Register under KRS number 0000906700, REGON 389210463, NIP 7393955075, with share capital of PLN 10,000 — the entity providing this Privacy Policy and acting as the Controller of the Data; |
| **Platform** | the online platform available at dronefra.com, through which we communicate with Clients and provide the Services; |

| Term | Meaning |
|---|---|
| **Privacy Policy** | this privacy policy, constituting fulfilment of the information obligations referred to in Articles 13 and 14 of the GDPR; |
| **GDPR** | Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC (General Data Protection Regulation); |
| **You / Your** | you — the person whose Data we process in accordance with this Privacy Policy; |
| **Services** | the services we provide consisting of ..... *(tu wstawisz opis usług, gdy będzie gotowy)* |

**3. Information About the Controller**

The Controller provides a tool in the form of an IT platform designed for in-depth analysis of unexpected situations that go beyond standard brand-related activities in the online environment.

**4. Roles of the Parties and Responsibility for Data Processing**

The Platform is solely a tool that enables the analysis of information you have made publicly available on social media, relating to the image of our Client's brand. Our role in processing your Data is limited to obtaining such Data and preparing an analysis of that information. Clients who use our Platform become data controllers within the meaning of the GDPR with respect to the analyses and information made available to them through the Platform.

**What does it mean to be a Data Controller?**

The Controller determines the purposes and means of processing your personal data — that is, how your Data held by the Controller will be used. The Controller is also responsible for ensuring the security of your data.

The Controller provides Services in the form of an analytical platform enabling Clients to analyse publicly available information originating from social media and other online sources.

Depending on the nature of the Service, the purpose of processing, and the configuration of the Platform, the Controller and the Client may act as:

- independent data controllers,
- joint controllers within the meaning of Article 26 GDPR,
- or in a controller–processor relationship.

The scope of responsibility of each party is determined individually, taking into account the actual influence on the purposes and means of processing personal data.

**The Controller is responsible in particular for:**

- designing and maintaining the Platform's infrastructure,
- defining the technical methods of data processing,

- developing analytical tools and data-analysis models,
- ensuring the security of data processing,
- defining the basic retention periods for technical and operational data,
- implementing privacy by design and privacy by default measures.

**The Client may be responsible in particular for:**

- defining the business purposes of analyses,
- selecting the scope of monitored topics, brands, or keywords,
- defining reporting parameters,
- making decisions regarding the use of analysis results,
- determining retention periods for data exported outside the Controller's Platform.

The Controller does not make business decisions regarding actions taken by Clients based on the analyses generated by the Platform.

If the nature of cooperation between the Controller and the Client justifies recognising the parties as joint controllers, they will conclude an appropriate arrangement under Article 26 GDPR specifying the allocation of responsibilities for fulfilling obligations under data-protection law.

**Analytical Models**

The Controller may use analytical, statistical, or algorithmic models for classifying and aggregating data. These models are designed and maintained by the Controller, while the Client may define analytical parameters or reporting scope available within the Service.

The Controller regularly reviews analytical models with regard to:

- compliance with the data-minimisation principle,
- proportionality of processing,
- accuracy of analyses,
- data security,
- limiting the risk of excessive profiling of individuals.

**5. Data Retention Period and Responsibility for Retention**

The Controller determines the retention periods for data processed within the Platform's infrastructure to the extent necessary to:

- ensure continuity of Service delivery,
- maintain system security,
- fulfil legal obligations,
- establish, pursue, or defend legal claims,
- ensure the integrity of analyses and reports.

The Client is independently responsible for the retention periods of any data, reports, or analyses exported outside the Controller's Platform environment if such materials are used for the Client's own business purposes as a separate data controller.

Upon completion of the Services, the Controller deletes or anonymises data in accordance with the adopted retention policy, unless further storage is required by law or justified by the need to protect the Controller's rights.

**6. Legitimate Interest of the Controller**

We process the data of social media users on the basis of Article 6(1)(f) GDPR, i.e., the legitimate interest of the Controller, which consists of:

- analysing publicly available content relating to brands and business entities,
- monitoring brand reputation,
- analysing consumer trends and interactions,
- ensuring the security and quality of the analytical services we provide.

Before commencing processing, we perform a **balancing test**, taking into account:

- the public nature of the data,
- the reasonable expectations of social media users,
- the impact of processing on the rights and freedoms of data subjects,
- the data-minimisation and pseudonymisation measures applied.

We ensure that the processing does not infringe the fundamental rights and freedoms of the individuals whose data is processed.

**7. Personal Data**

We collect personal data from our Clients and Users of the Services for our own purposes, such as providing and administering the Services.

More detailed information on the processing of such personal data can be found in the section **Client Data** below.

To provide our Services, we analyse user profiles and other information that we receive directly from social media platforms such as Facebook, Twitter, LinkedIn and others, via the application programming interfaces (APIs) of those platforms, or based on Data collected in another manner with their consent. This information we process includes both non-personal data, such as various statistics and indicators, as well as personal data of users of those platforms. When data is obtained directly from the relevant platforms, the purpose of processing is to develop and continuously improve our Services and to offer them to Clients through our online Platform. All Data obtained in this manner has been made publicly available by you.

More information on the processing of such personal data can be found in the section **Social Media User Data** below.

**8. Voluntary Provision of Data**

We collect only the Data from our Clients and their representatives that is necessary for the performance of a given agreement. Failure to provide the data required to conclude and perform the agreement will prevent us from entering into or executing the agreement with you. This also applies to Data that we must collect due to legal obligations (e.g., invoicing data).

Where we request your consent to process personal data, such consent is entirely voluntary. If you do not grant the requested consent, we will not undertake the actions to which that consent relates. You may withdraw your consent at any time. Withdrawal of consent does not affect the lawfulness of processing carried out prior to its withdrawal.

In the case of social media user data (as described here), the data we process has been voluntarily made public by you, and we use it only within the limits defined by the platforms on which you are a user.

**9. Client Data**

**Data Collection**

We collect your personal data when you:

- register for the Services by completing an online registration form,
- log in to the Services using your username (email) and password or other authentication methods available on the Platform,
- voluntarily provide such data in any other way, e.g., by completing and submitting forms available through the Platform,
- enter into an agreement with us.

When creating an account on the Platform, we will ask you to complete a registration form in which you provide your first name, last name, email address, company name, and job title.

If our Client is an entity other than a natural person, individuals who log in to the Platform on its behalf become data subjects to the extent described above. If the Client provides us directly with personal data of persons authorised to access the Services, the Client must have all necessary consents for processing and transferring such personal data to us and must fulfil the information obligations towards those individuals as required by law.

As a rule, we do not intend to process special categories of personal data.

If special category data is incidentally disclosed in publicly available content analysed by the Platform, we implement technical and organisational measures to limit further processing of such data to the minimum necessary to ensure the functionality of the Service.

We do not use special category data for profiling, scoring, or making decisions about individuals.

**Sources of Data and Methods of Collection**

For some processing operations, we do not obtain personal data directly from the data subjects.

Data may be obtained from:

- publicly available profiles and content published on social media,
- publicly available posts, comments, and materials published on online platforms,

- application programming interfaces (APIs) provided by online platform and social media providers,
- data publicly shared by internet users,
- data provided by the Controller's Clients in connection with the use of the Services.

We collect only data that is:

- publicly available,
- shared in accordance with the privacy settings chosen by the user,
- or data whose processing is permitted under applicable law.

We do not take any actions aimed at bypassing user privacy settings or accessing non-public data.

If personal data has not been obtained directly from the data subject, we fulfil the information obligations under Article 14 GDPR, taking into account the nature, scope, context, and purposes of processing.

In cases permitted by law, we may limit the scope of information provided if:

- providing such information proves impossible,
- would require disproportionate effort,
- or could prevent or seriously impair the achievement of processing purposes,

while implementing appropriate safeguards for the rights and freedoms of data subjects, including public availability of this Privacy Policy.

**10. Purpose and Legal Basis of Data Processing**

**Purpose – Scope – Legal Basis**

| **Purpose of Processing** | **Scope of Data** | **Legal Basis** |
|---|---|---|
| **To ensure better service. For the purposes of analysing and improving our Services, our servers may automatically record information when a user visits our Platform or uses certain Services. Such data may also be processed using cookies.** | URL; IP address; browser type and language; date and time of your request or activity on the site. | Performance of a contract with you (if you are our direct client – a natural person) [Art. 6(1)(b) GDPR] or our legitimate interest in providing Services to our Clients [Art. 6(1)(f) GDPR] (where our Client is your company or organisation and you are an authorised user). |

| Purpose of Processing | Scope of Data | Legal Basis |
|---|---|---|
| **Communication. We may process data of Clients or their representatives (individual Platform users) to communicate with them, e.g., when assisting with account setup or administration, providing customer support, sending technical notifications, updates, reminders, security alerts, and other service-related messages.** | first and last name; email; company name; job title; phone number; if webchat is connected to Facebook Messenger — publicly visible data such as profile picture and username. | Contract performance [Art. 6(1)(b) GDPR] or legitimate interest [Art. 6(1)(f) GDPR]. |
| **Contact form and webchat. Communication may occur via a contact form or webchat, which can be linked to Facebook Messenger. These tools enable quick responses regarding the Services.** | first and last name; email; company name; phone number; Messenger public profile data. | Your consent [Art. 6(1)(a) GDPR]. |
| **Ensuring security of the Services. We process personal data to ensure the security, protection, and reliability of the Platform, including detecting, preventing, and responding to fraud, abuse, security threats, and technical issues.** | first and last name; email; company name; job title; phone number; user activity tracking to detect anomalies. | Legitimate interest in ensuring secure provision of Services [Art. 6(1)(f) GDPR]. |
| **Protection of our rights or the rights of third parties.** | name; email; company name; job title; phone number; address; financial data (e.g., bank account number); other data provided by the counterparty. | Legitimate interest in protecting the rights of the Controller or third parties [Art. 6(1)(f) GDPR]. |
| **Marketing and sales. We may contact you regarding news, events, Services, features, or special offers, provided we have your consent.** | name; email; company name; job title; phone number. | Your consent [Art. 6(1)(a) GDPR]. |

**11. Categories of Data Recipients**

Recipients of personal data may include:

- authorised employees and associates of the Controller,

- providers of IT, hosting, cloud infrastructure, and system security services,
- providers of analytical and communication tools used by the Controller,
- entities providing legal, audit, or advisory services,
- entities supporting the Controller in maintaining and developing the Platform,
- Clients of the Controller using analytical Services — only to the extent necessary to provide the Service,
- public authorities or law-enforcement agencies where required by law.

We limit the scope of data shared with recipients to the minimum necessary for the intended processing purposes.

**12. Data Protection Impact Assessment (DPIA) and Risk Management**

We implement organisational and technical measures to ensure that personal data processing complies with GDPR principles, in particular **privacy by design** and **privacy by default**.

For processing operations that may result in a high risk to the rights or freedoms of individuals, we conduct a **Data Protection Impact Assessment (DPIA)** in accordance with Article 35 GDPR.

A DPIA may be carried out in particular with respect to:

- monitoring publicly available social media content,
- profiling or analysing user behaviour,
- using analytical or algorithmic tools,
- large-scale data processing,
- analysing data from multiple sources,
- detecting communication anomalies or potential crisis situations,
- processing data that may indirectly concern individuals requiring special protection, including minors.

**13. Data Protection Impact Assessment (DPIA) – continued**

As part of the impact assessment, we analyse in particular:

- the nature, scope, context, and purposes of processing,
- the necessity and proportionality of processing,
- the potential impact of processing on the rights and freedoms of individuals,
- the risk of excessive interference with privacy,
- the risk of misclassification or excessive profiling,
- the risk of unauthorised access to data,
- the effectiveness of the technical and organisational safeguards applied.

We implement appropriate risk-mitigation measures, in particular:

- minimisation of the scope of data,
- pseudonymisation and anonymisation where possible,
- data-retention limitations,
- access restrictions,
- system-security monitoring,
- regular reviews of analytical models,
- mechanisms limiting the possibility of identifying individuals.

We regularly review data-processing operations and update data-protection measures in line with technological developments, the nature of the Services, and identified risks.

We may use analytical tools incorporating elements of machine learning, statistical analysis, or automated data classification.

Before implementing new analytical functionalities, we assess their impact on privacy and the rights of data subjects, taking into account in particular:

- the risk of excessive profiling,
- the risk of discrimination or misclassification,
- the transparency of analytical models,
- the adequacy of the scope of processed data,
- compliance with the data-minimisation principle.

We implement procedures ensuring human oversight over analytical systems and limiting the risk of incorrect or disproportionate actions affecting individuals.

We take into account the special need to protect minors' data when designing and developing Platform functionalities.

We do not design Services to monitor children's activity or create behavioural profiles of children.

If, in the course of providing the Services, incidental processing of minors' data occurs, the Controller applies additional measures to reduce the risk of violating their rights and freedoms, in accordance with the principles of privacy by design and the best interests of the child.

**14. Data Retention Period**

We process your Data only for the period necessary to achieve the purposes set out in this Privacy Policy or in the service agreement, unless longer storage is required by law (e.g., for tax or accounting purposes or other legal obligations) or is necessary to establish, pursue, or defend legal claims. In such cases, we store only the data necessary for those purposes and only for the period required by the applicable limitation periods.

Before the expiry of the above period, we may cease processing your data and delete it in the following situations:

- where the legal basis for processing is the Controller's legitimate interest;

- where the legal basis is the Controller's legal obligation — only for the period necessary to fulfil that obligation;
- where consent is withdrawn, if consent was the basis for processing.

**15. Data Sharing**

In certain situations, we share your Data with third parties. Recipients may include:

- our authorised employees and associates who require access to perform their duties;
- entities to which we outsource services related to data processing, such as subcontractors, law firms, courier companies;
- in the case of social media user data — certain Data may be shared with users of our Service. Such Data is limited to what is necessary to provide the Service and consists solely of information you have previously made public;
- public authorities, including the Police, the National Revenue Administration, and law-enforcement bodies, where required by law.

**16. Transfer of Data Outside the EEA**

We do not anticipate transferring Data to third countries outside the EEA. If such a transfer becomes necessary, all legal requirements will be met.

If Data is to be transferred to a recipient located in a third country that does not ensure an adequate level of protection, we will apply appropriate safeguards, such as Standard Contractual Clauses approved by the European Commission, unless:

- you provide explicit consent for the transfer, or
- the European Commission issues an adequacy decision for that country.

**17. Profiling and Absence of Automated Decision-Making**

Profiling means automated processing of Data to evaluate certain personal aspects of an individual, in particular to analyse or predict aspects relating to performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location, or movements.

To provide the Service, we use profiling in certain cases. This means that through automated data processing, we assess selected factors relating to individuals to analyse their behaviour or predict future behaviour.

We use partially automated data-analysis methods that may constitute profiling within the meaning of Article 4(4) GDPR.

Profiling involves analysing publicly available information from social media and other online sources for the purposes of:

- identifying communication trends and patterns,
- analysing user interactions with brands or businesses,
- assessing the reach and nature of public statements on specific topics or brands,
- detecting potential crisis situations or communication anomalies,

- generating aggregated statistical analyses and reports for Clients.

Categories of data that may be analysed include:

- publicly available social media identifiers,
- usernames,
- profile photos,
- content of public posts,
- publication dates and times,
- activity and interaction data,
- engagement metrics,
- technical data related to Platform usage.

Profiling **is not used** to:

- make decisions producing legal effects for individuals,
- automatically restrict access to services,
- assess creditworthiness,
- evaluate economic situation,
- assess health,
- assess personality traits,
- make decisions significantly affecting individuals.

We implement organisational and technical safeguards to reduce risks, including:

- data minimisation,
- limiting analyses to publicly available data,
- pseudonymisation where possible,
- retention limitations,
- access controls.

Analysis results are supportive and analytical in nature and always require human assessment. We do **not** use solely automated decision-making within the meaning of Article 22 GDPR.

At no stage do we use profiling to make automated individual decisions.

**18. Sensitive Data**

As a rule, the Controller does not process sensitive personal data, i.e.:

- data revealing racial or ethnic origin,
- political opinions,

- religious or philosophical beliefs,
- trade-union membership,
- genetic data,
- biometric data,
- health data,
- data concerning sexuality or sexual orientation.

Such data may be processed only incidentally if you have made it publicly available yourself — e.g., by posting content on social media that reveals sensitive information. The Controller never profiles individuals based on sensitive data. The Platform also does not include functionalities enabling the creation of personal profiles based on such categories.

**19. Children**

Our Services are not directed at children and are not designed to monitor children's activity on social media.

We do not intentionally profile children or use children's data to make decisions or create behavioural analyses.

If we become aware that data relates to a person below the age requiring special protection under applicable law, we will take appropriate measures to limit further processing, in accordance with data-minimisation and privacy-by-design principles.

**20. Your Rights and the Data Protection Officer**

In connection with our processing of your Data, you have several rights. The person responsible for contacting you regarding the exercise of your rights is the Data Protection Officer (DPO), appointed as: **[____]**.

You may contact the DPO:

- by email: **iod@dronefra.com**
- by post: Data Protection Officer, UAV Labs sp. z o.o., ul. Władysława Trylińskiego 14 lok. 1, 10-683 Olsztyn.

When contacting us, please provide your contact details and preferred method of communication, and in the case of phone contact — a convenient time to reach you. This will help us respond more efficiently.

You have the right to:

- request access to your Data and the right to rectify or delete it ("right to be forgotten"),
- object to processing for direct-marketing purposes — such an objection results in immediate cessation of processing for marketing purposes,
- object, on grounds relating to your particular situation, to processing based on legitimate interest — unless we demonstrate compelling legitimate grounds,
- data portability (for data processed under a contract or consent),

- restrict processing,
- withdraw consent at any time, where consent is the basis for processing. Withdrawal does not affect the lawfulness of processing carried out before withdrawal.

The supervisory authority for data protection in Sweden is: **Integritetsskyddsmyndigheten (IMY), Box 8114, 104 20 Stockholm, Sweden** Current information on exercising data-subject rights is available at: **www.imy.se**