PRIVACY POLICY

VER. 1.0 – 17 FEB 2023

§1 – Definitions

LOTva – non-registered and informal organization of virtual aviation passionate, simulating operations of LOT Polish Airlines in flight simulator.

LOTva Board – supervising persons, with duties assigned by so-called CEO.

Communication channels – methods of communication between LOTva members and persons responsible for the processing of your personal data in the LOTva. LOTva's specific communication channels are:

- e-mail – communication by e-mail with all addresses from the lotva.org domain,
- Discord – official LOTva channel on Discord platform,
- communication platforms – all interactive forms available on the lotva.org website.

Authorized member of the LOTva – a person who was granted access to the data protected by this document.

The keywords in this document should be interpreted as follows:

MUST – this word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification,

MUST NOT – this phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification

SHOULD – this word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course,

SHOULD NOT – This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label,

MAY – This word, or the adjective "OPTIONAL", mean that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

Definitions based on the RFC-2119 requirements specification.

§2.1 - Scope

The privacy policy and the definition of personal data protection are aimed at:

- comply with the law specified in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 / EC (general regulation on data protection) and Act of December 14, 2018 on the protection of personal data processed in connection with the prevention and combating of crime (Journal of Laws of 2019, item 125),
- comply with the obligation specified by the VATSIM Data Protection and Data Handling Policy of May 25, 2018, with amendments of June 9, 2020 and later,
- maintaining good practices for the protection of personal data of members and the Board and all others who use LOTva services.

§2.2 – Type of data

LOTva collects personal data of its members both directly and through the use of third party data transfers.

§2.3 – Type of data collected directly

When you use our services, additional data is collected about you. This allows us to ensure the smooth running of our services and provide you with the desired user experience. These data include:

- saving and archiving posts, statements, saved settings and completed forms, polls and votes posted on LOTva communication channels,
- information about the IP address used in the LOTva communication channels,
- records of progress in training courses conducted by the LOTva,
- history of disciplinary proceedings and actions taken,
- communication between members, including those outside the board.

Communication channels, including our forum, have the function of collecting any data in the form of free text. Any personal data voluntarily submitted in this way by any persons (e.g. personal data such as telephone numbers or addresses) will be stored, even if hidden from public access. This data is then only available to a limited number of authorized persons.

§2.4 – Type of data collected by third parties

When a member uses the LOTva services or when a member requests to join the LOTva, the data is transferred from VATSIM or other third parties through internal communication channels to LOTva in order to ensure the smooth functioning of our services and to ensure the highest standards of services provided. These data include:

- full name,
- VATSIM CID,
- e-mail address,
- data on the timeframe and duration of logins to website

- When using the official Discord messenger server, LOTva collects the following data: Unique ID number and User Name assigned to Discord messenger account, discord avatar

§2.5 – Policy provisions

The LOTva is committed to:

- compliance with the objectives listed in §2.1 and good practices resulting from the processing of personal data,
- respect the rights of the individual, including:
  - the right to access to information,
  - the right to rectification,
  - the right to objection,
  - the right to be forgotten,
- conducting a transparent privacy policy,
- provide instructions to persons responsible for data processing in order to carry out activities in accordance with this policy,
- informing the persons whose data are processed about any possibility or suspicion of unlawful disclosure of their personal data,

§3 – Liability

LOTva Staff

The LOTva Staff is generally responsible for the protection of personal data and the compliance of the relevant standards of services provided by the LOTva with this privacy policy. The current composition of the Staff is available on the website.

Internal Data Protection Officer

The Data Protection Officer is appointed as the person responsible for ensuring compliance with this privacy policy.

Current Internal Data Protection Officer is available on website.

§4.1 – Security scope

This section applies to all LOTva services and servers belonging to or provided to LOTva, including: personal data servers, statistical data or web servers.

§4.2 – Security measures

LOTva takes standard steps to secure your data, such as TLS encryption when accessing your data using a web browser. Additional security settings are used to allow only authorized users to access the server. Passwords (with the exception of the VATSIM network password, which is never transferred to the LOTva) are stored as encrypted strings, preventing them from being displayed in plain text.

§4.3 - Risks

Four main sources of threats to the security of data stored by the LOTva have been identified. These are:

- phishing attacks, i.e. intentional forcing of unauthorized access to data stored on the server,
- unauthorized access by malware of infected systems used by authorized members of the LOTva,
- bugs in the software, allowing unauthorized (even accidental) access to data stored on the server,
- access by unauthorized LOTva members.

The elimination of the first two threats consists in:

- verifying all persons prior to granting access with knowledge of this privacy policy,
- encouraging authorized members to follow good security practices in their personal systems.

The third risk is limited by the appropriate phase of tests of the implemented software.

The last risk is mitigated by logging access and rolling back changes made by those who misuse previously granted access.

§5 – Saving and storing data

§5.1 - Scope

Most of the data used by the LOTva is transmitted directly through the internal VATSIM communication channels.

The data indicated in §2.3 and §2.4 of this policy are stored only in the event of a justified need, specified in §9.

§5.2 – Stored data update

Personal data stored by LOTva are synchronized within the SSO (Single Sign-On) internal personal data exchange channels. Therefore, the data is not updated directly on the LOTva servers, it is received from third servers. The concerned LOTva member should address requests for data updates to the relevant VATSIM authorities.

§5.3 – Stored data

Data is stored in standard file systems and databases. Access to these systems is controlled by secure direct access to control applications or via a secure web interface. Access is then controlled and protected against unauthorized access by standard measures such as access control based on limiting the access rights of individual access accounts.

§5.4 – Data storage period

LOTva is obliged to store data in accordance with the Data Protection Policy and their processing of the VATSIM network. Removal requests may be processed by LOTva in accordance with §9, however, the removal of some processed data may require the intervention of VATEUD, VATEMEA or directly VATSIM, as the request may be outside the powers of the persons responsible for LOTva.

§5.5 - Archiving

Data archiving by LOTva does not include data stored on servers other than those belonging to LOTva. Data on these servers is stored for a specified period of time and then archived in accordance with §2.3 or completely deleted.

§6 – Transparency of data protection

LOTva makes every effort to ensure that all members know what data and for what purpose their personal data is collected.

As specified in this document, data is collected to ensure the smooth functioning of the LOTva so that members can enjoy the functionality of the VATSIM network together.

§7 – The right to access to information

§7.1 - LOTva Responsibility

Requests for disclosure of information about processed personal data are within the competence and responsibility of the designated Internal Data Protection Officer.

The Data Protection Officer must fulfil the requests consistent with the submitted application within one month of receiving such a request.

The Internal Data Protection Officer confirms the receipt of the application, responding immediately after receiving the application: to the applicant or the person submitting the application on behalf of the applicant. Based on the reply to the applicant about the initiated process, it is possible to set a date from which the monthly obligation period for reviewing the application begins.

If, not mentioned in this document, circumstances prevent the Internal Data Protection Officer from reviewing the application, the period of fulfilling the requests may be extended once by one month, provided that the applicant is informed about the situation. The exact period of extension is indicated and the reasons for extending the period of fulfilling the requests are provided.

The application may be rejected by the Internal Data Protection Officer in the event that:

- the request comes from a person not authorized to manage the subject data (e.g. a request for data of the wrong person),
- there is no possibility to verify the identity of the person making the request,
- does not refer to data held by the LOTva as defined in this document,
- refers to data deleted in accordance with pt. 5.5 of this policy.

§7.2 – Request submit procedure

Requests for disclosure of information about the processed personal data in the form of an application should be sent to the following e-mail address: staff@lotva.org.

If any member or responsible person receives anything that may be considered a request for data disclosure, they should immediately inform the Internal Data Protection Officer.

§7.3 – Identity veryfication

If you send a request for personal data, you must confirm your identity in order to start processing the request.

The Internal Data Protection Officer, prior to starting the application processing process, is required to verify the identity of the person submitting the application. However, this inspector may not, as part of confirming identity, allow the storage of further identifying and personal data (e.g. he cannot request a photocopy of an identity document, but may request its presentation, also in digital form)

The exception to the formal confirmation is the acquaintance of the person submitting the request by the Officer.

The correctness of the identity verification is the responsibility of the Officer, however, the method of formalizing the identity confirmation lies with the applicant.

§7.4 - Charges

LOTva does not charge any fees for the processing or sharing of data based on requests to provide information about the processed personal data.

§8 – Right to be forgotten

Acting on the basis of the applicable law mentioned in point 2.1, LOTva undertakes to delete data at the request of the applicant. The request to delete data is processed in the same way as the right to access to information described in pt. 7. The procedure for submitting a request, verifying identity and determining the fees related to the procedure is set out in §7 of this policy.

Requests with a request to delete data should be sent to staff@lotva.org

§9 – Legal basis

LOTva ensures that it has a legitimate interest in collecting and storing the personal data described above. The reasons for this claim are as follows:

- LOTva is a voluntary community, promoting flight simulations and virtual air traffic control, and all members who wish to join have an obvious interest in such activities.
- Collected data is the minimum required to allow the smooth and optimal functioning of the VACC, solely for the enjoyment of its members.
- The data is necessary to enable the LOTva Staff and VATSIM Staff to properly manage the VA, both in their day-to-day operations and in circumstances where the member(s) may be operating in a manner contrary to the rules and regulations governing VA or VATSIM network.

§10 – Policy changes

Responsible for the compliance of this document in accordance with applicable law lies with the Internal Data Protection Officer.