DATA PROTECTION AND HANDLING

WARNING

Information contained in this document is
intended for flight simulation purposes only.

Table of Contents

1 Control Pages

1.1 Document Identification

Document Identification	
Type	Policy
Version	1.4
Issue Date	20 JUL 2015
Identification	VATSIM-POL-Data Protection and Handling

1.2 Revision Records

Revision Number	Date	Description of Change	Author
1.0	14 APR 2018	Initial Release	BoG
1.1	09 JUN 2020	Updated document to remove requirement for parental consent and minor corrections	BoG
1.2	01 MAY 2021	Updated Section 1.2	DD
1.3	01 JAN 2023	Periodic update	AC
1.4	20 JUL 2025	Periodic update	BoG

1.3 Related Documents

Document Name	Document Identification
Privacy Policy	VATSIM-POL-Privacy

2 Purpose

The purpose of this policy is to achieve the following:

- to comply with the law, particularly the EU General Data Protection Regulations
- to ensure good data protection practice
- to protect users, staff, and other individuals
- to protect the organization

3 Applicability

This policy applies to:

- Any current or former user of VATSIM who has been issued a VATSIM Certificate Identification (CID) number

4 Definitions

Elevated Data Access: Access to data, including personal data, that a standard user would not have access to.

Member: An account holder / user is considered a member of the VATSIM community. Being considered a member of the VATSIM community does not under any circumstances convey or grant any rights of ownership, management or authority over VATSIM.

5 Policy

5.1 Policy Statement

VATSIM has an unequivocal commitment to:

- comply with both the law and good practice
- respect individuals' rights including:
  - The right of access
  - The right of rectification
  - The right to object
  - The right to suspend processing
  - The right of erasure
- be open and honest with individuals whose data is held
- provide training and support for staff who handle personal data, so that they can act confidently and consistently
- notify the relevant data protection authorities voluntarily, even when not required

5.2 Types of Data

VATSIM collects a range of data on users, both at the time of joining and while a user is connected to the VATSIM network for the purpose of ensuring the efficient and safe functioning of the network. This data includes:

- The user's full name
- Their general geographic location (but not specific address)
- Their age (but not specific birthdate)
- Their history of connections to the network, including security information (including, but not limited to, IP data) to protect the integrity of the network
- The simulated Air Traffic Control and/or Pilot rating they have obtained with the VATSIM network
- Positions of responsibility held within the network, including level of access
- Their history of any breaches of the VATSIM User Agreement, Code of Regulations and/or Code of Conduct, to which all users agree to be bound by upon joining

In addition, whilst connected to the network, information specific to their simulated aviation operation at that time is collected. This data may be transferred to other organizations to facilitate greater situational awareness within the simulation. The only personal information that is transmitted in this manner is the user's name, CID number and network rating. Users are also optionally able to enter a location into the various clients on connection; this can be either their real or a simulated location at the discretion of the individual user.

In addition to operational data, on rare occasions, VATSIM may request, collect, and temporarily hold documentation to prove name and/or age.

6 Responsibilities

6.1 Data Protection Officer

There is no appointed Data Protection Officer within VATSIM as the organization does not regularly process data on a large scale, due to the nature of the data that is collected and controlled, and the circumstances in which it is collected.

6.2 Specific Department Heads

Several members of the Board of Governors have specific responsibilities to oversee others accessing personal data collected by VATSIM:

- VPs of Regions – Regional and Divisional Staff
- VP Membership – Membership Staff
- VP Conflict Resolution – Conflict Resolution Staff
- VP Supervisors – The VATSIM Supervisory teams

- VP Technology – Control of and access to stored data

Other members of the Board of Governors may from time to time be tasked with specific responsibilities pertaining to the control and storage of data.

6.3 Staff and Volunteers

All staff are required to read, understand, and accept any policies and procedures that relate to the personal data they may handle in the course of their work within VATSIM as detailed in this policy. VATSIM expects the highest standard of probity from all staff at all levels. No access to data is to take place unless there is a valid network related reason for such access. All access is monitored and regularly audited.

6.4 Enforcement

VATSIM has a zero-tolerance policy towards inappropriate access to data. Any such access will normally result in the individual concerned being prohibited from having further elevated data access for a minimum period of 10 years. This may also preclude the user concerned from holding positions of responsibility within the network.

7 Security

7.1 Scope

VATSIM's Security policy applies to all servers belonging to or donated to the VATSIM network, including, but not limited to Network FSD Servers, Data Servers, Statistic Servers, or Web Servers.

7.2 Setting security levels

VATSIM operates on a segmented security approach, where only the access required with approval by the VATSIM Board of Governors to complete a required job function is granted.

VATSIM employs access monitoring systems to ensure that access is not being abused and can be tracked back to a specific individual.

7.3 Security measures

VATSIM employs industry-standard security to include, but not limited to, QUIC and TLS for in-transit encryption, AES-256 quantum resistant encryption at rest, and end-to-end encryption between our web platform and the storage repository.

A very limited number of staff have access to documentation containing personal information, based on their role in the organization as well as a need-to know. Essentially, this means

typically fewer than 20 individuals out of the roughly 1.1 million account holders (0.002%) on VATSIM could possibly ever access those documents, yet VATSIM's elevated data access rules regarding operational necessity also typically limits that to one trained, vetted staff member that conducts the verification and then deletes the submitted identity document. VATSIM uses QUIC where supported by the user, for web page delivery as it is more performant and secure by design. VATSIM also implements additional change-audit scripts and monitors to provide visibility into server and network activity.

IP address and key-based security settings are used to only allow server access to authorized users.

Passwords are stored as hashed encrypted data wherever possible. As a general principle passwords are not stored as plain text.

7.4 System continuity

In order to ensure system continuity, VATSIM retains data backups of relevant systems to ensure a speedy recovery of impacted systems while maintaining data integrity and security.

Access to these backups is granted only to authorized individuals.

7.5 Specific risks

The main specific risks to the security of data are:

- Phishing attacks to gain network or data access,
- Access by means of trojan or keylogging programs on user's systems, and
- Insider threats

Mitigation of the first two risks is by encouraging users who have elevated data access to ensure they adhere to good security practices on their personal systems. The last risk is mitigated by access logging and the ability to revert changes made by those who misuse access.

8 Data recording and storage

8.1 Accuracy

VATSIM data is deemed to be accurate across all systems. However due to the nature of network operations, some human-led mistakes may occur.

8.2 Updating

A VATSIM user may request an update of his/her retained information by making a request in writing to the Vice President of Membership.

The final authority to update such information shall be at the sole discretion of the VATSIM Board of Governors.

8.3 Storage

Data is stored in standard relational databases. Access is via a custom-built web-based interface with a focus on data security.

8.4 Retention periods

VATSIM network data, including but not limited to connection history, authentication events, support tickets etc., are retained indefinitely unless the user exercises the Right of Erasure, as outlined in this policy.

Documents provided to verify real-word aviation certifications, name and/or age are deleted upon verification.

8.5 Archiving

VATSIM does not archive any data at this point in time, as network data (other than data provided to verify real-word aviation certifications, name and/or age) is currently retained indefinitely.

9 Transparency

9.1 Commitment

VATSIM is committed to ensuring all users are aware of what data is collected and why we do so.

- As outlined in the statement of legitimate interests, data is collected for the purpose of ensuring the provision of, and smooth operation of the VATSIM network so that users can jointly enjoy the simulated aviation environment it provides.
- Data may be transferred to other organizations affiliated with, or associated with, the network to provide services to enhance and extend the simulated aviation environment.

9.2 Procedures

Details on how to exercise rights in relation to the data held is detailed in the relevant sections of this policy.

9.3 Responsibility

All staff within VATSIM are responsible for protection of user data at all times. The various departments most closely associated with user data are the VATSIM Supervisors and Administrators, the Conflict Resolution staff, the Membership staff, and the staff of Regions and Divisions.

Where staff require to use data for statistical and management purposes aggregated pseudonymised data should be used where possible.

9.4 Contact

For further information or clarification, users may contact the Vice President of Membership

10 Lawful Basis

10.1 Underlying principles

VATSIM asserts that it has a legitimate interest in collecting and storing the personal data outlined above. The reasons for this claim are:

- VATSIM is a voluntary community promoting flight simulations and virtual air traffic control, and all users seeking to join have an obvious interest in such activities.
- The data collected is the minimum required to allow for the smooth and optimal running of the network, including the protection of the network and community, solely for the enjoyment of its users.
- That the data is necessary to allow for the organization to operate as a like-minded hobby organization, providing a community-minded environment for simulated pilots and controllers to interact in a singular virtual sky.
- That the data is necessary to allow for VATSIM staff to properly manage the network, both in day to day operations, and in circumstances where a user may act in a manner contrary to the VATSIM User Agreement, Code of Regulations, Code of Conduct, and/or other policies.
- That as all users have a shared interest in these aims that the collection of such data should be reasonably expected by all users.

10.2 Opting out

Notwithstanding VATSIM's claim of legitimate interest, users may at their discretion object to this claim and/or request that VATSIM cease processing of a user's personal data. These two rights are known as the Right to Object, and the Right to Restrict Processing.

Users must be aware that if they choose to exercise either of these rights VATSIM is obliged to permanently and irreversibly lock their accounts in order to comply with their wishes and they will be unable to connect to the network or to any service that relies on the VATSIM Single Sign On (SSO) system.

10.3 Timing of opting out

While notification of an objection to VATSIM's claim of legitimate interest, or a request to suspend processing may be made at any time, such claims may not be made retroactively.

11 Right of Access

11.1 Responsibility

Requests for personal data under the Right of Access are the responsibility of VP Membership and their team. Such requests are normally required to be complied with within one month of the request being received. If circumstances prevent this from occurring, an extension of an additional two months may be instituted by VATSIM, and the user making the request should be informed of this fact before the expiration of the original one-month target.

11.2 Procedure for making request

Requests must be in writing. Users shall make their written request via membership support ticket at support.vatsim.net.

If staff at a lower level receive anything that might reasonably be construed to be such a request, they have a responsibility to refer the request to the VATSIM Membership Department.

11.3 Provision for verifying identity

Where the person managing the request does not know the individual personally, there will be a provision for checking their identity before releasing any information.

11.4 Charging

VATSIM will generally not charge a fee for providing data for first/initial requests under the Right of Access. VATSIM may charge a reasonable administrative fee for any requests that are deemed especially excessive or repetitive, such as if an individual requests multiple copies of their personal data.

11.5 Sensitive Information

Because of the sensitive nature of who makes a comment on a user's record, as well as ensuring there is no retaliation or harassment against VATSIM staff, and to protect the privacy of staff members, names of those staff who have made entries in user's records, along with any security measures adopted by VATSIM, are redacted before sending records to the user.

12 Right of Rectification

12.1 Responsibility

Accurate data is in the best interests of both the network and the membership. Requests for rectification are the responsibility of VP Membership and their team. Such requests are normally required to be complied with within one month of the request being received. If circumstances prevent this from occurring, an extension of an additional two months may be instituted by VATSIM, and the user making the request should be informed of this fact before the expiration of the original one-month target.

12.2 Procedure for making request

Requests must be in writing. Users shall make their written request via membership support ticket at support.vatsim.net.

If staff at a lower level receive anything that might reasonably be construed to be such a request, they have a responsibility to refer the request to the VATSIM Membership Department.

12.3 Provision for verifying identity

Where the person managing the request does not know the individual personally, there will be a provision for checking their identity before releasing any information.

12.4 Disputes

Where there is a dispute between a user and VATSIM over the accuracy of data, the VP Membership shall be empowered to make any final decision on whether to alter data or not. This decision should normally be communicated to the user making the request within one calendar month of the request having been made.

12.5 Charging

VATSIM will not charge a fee for normal requests under the Right of Rectification. VATSIM may charge a reasonable administrative fee for any requests that are deemed especially excessive or repetitive.

13 Right of Erasure

13.1 Responsibility

Requests for deletion of personal data under the Right of Erasure are the responsibility of VP Membership and their team. Such requests are normally required to be complied with within one month of the request being received. If circumstances prevent this from occurring, an extension of an additional two months may be instituted by VATSIM, and the user making the request should be informed of this fact before the expiration of the original one-month target.

13.2 Procedure for making request

Requests must be in writing. Users shall make their written request via membership support ticket at support.vatsim.net.

If staff at a lower level receive anything that might reasonably be construed to be such a request, they have a responsibility to refer the request to the VATSIM Membership Department.

13.3 Provision for verifying identity

Where the person managing the request does not know the individual personally, there will be a provision for checking their identity before deleting any information.

13.4 Charging

VATSIM will not charge any fee for deleting data under the Right of Erasure.

13.5 Procedure for granting erasure

VATSIM shall evaluate all requests for erasure. VATSIM reserves the right to retain any data that it believes is in its legitimate interest to do so, or that is required to establish, exercise, or defend any potential legal claims.

14 Staff training and acceptance of responsibilities

14.1 Initial training, acknowledgement and acceptance of policy

All staff requiring elevated data access receive training on elevated data access procedures and safeguards, including personal information, shall acknowledge they have received this training and that they understand and shall be bound by the requirements. Confirmation of this acknowledgement is recorded.

14.2 Continuing training

Recurrent training is conducted, and acknowledgement of training and responsibilities will be provided, annually.