Data Protection and Handling Policy

v1.0 Effective 25MAY18

1 Introduction

1.1 Purpose of policy

This policy has been put in place to achieve the following aims:

- to comply with the law, particularly the EU General Data Protection Regulation
- to ensure good data protection practice
- to protect members, staff, and other individuals
- to protect the organisation

1.2 Types of data

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

- The member's full name
- Their country of residence
- Their age (but not their birthdate)
- Their history of connections to the network, including their IP address and additional security information to protect the integrity of the network
- The simulated Air Traffic Control and/or Pilot Rating they have obtained via training 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 Code of Conduct, to which all members agree to be bound by upon joining

This information is stored in a system known as CERT which is the main central data repository of VATSIM (and is anticipated to migrate to a similar system known as CERT2). In addition to CERT, regions, divisions, and their subsidiary components may also hold their own individual data collections.

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 organisations to facilitate greater situational awareness within the simulation. The only personal information that is transmitted in this manner is the member's name, membership number and network rating. Members are 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 member.

Various subsidiary parts of VATSIM may collect and store additional data relating to the administration of their respective subsection of VATSIM. As a rule, this data is not to be retrieved from CERT. All such data shall be collected, stored, managed, and secured in line with the principles outlined in this document.

1.3 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 protest
  - 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 if this is not required

1.4 Key Risks

Key risks are detailed in Section 3.5 of this document in the Specific Risks paragraph.

2 Responsibilities

2.1 The Board / Company Directors

Overall responsibility for ensuring data protection and overall compliance with the relevant standards and legislation rests collectively with the VATSIM Board of Governors.

2.2 Data Protection Officer

There is no appointed Data Protection Officer within VATSIM as the organisation 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.

2.3 Specific Department Heads

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

- VP Regions – Regional and Divisional Staff
- VP Membership – Membership Staff
- VP Conflict Resolution – Conflict Resolution Staff
- VP Supervisors – The VATSIM Supervisory teams
- VP Network Systems – Control of stored data
- VP Web Services – Remote access to, and control of 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.

2.4 Staff & 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 expect the highest standard of probity of all staff at all levels. No access to data is to take place unless there is a valid network related reason for such access.

2.5 Enforcement

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

3 Security

3.1 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.

3.2 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.

3.3 Security measures

VATSIM employs standard SSL encryption to safeguard data. 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 servers.

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

3.4 Business continuity

In order to ensure business 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 are granted only to authorized individuals.

3.5 Specific risks

The main specific risks to the security of data are:

- Phishing attacks to gain network access or CERT access,
- Access by means of trojan or keylogging programmes on member's systems, and
- Access by upset staff members who have been granted access is also a risk

Mitigation of the first two risks is by encouraging members who have a higher level of access to ensure they adhere to good security practices on their personal systems. The last risk is mitigated by access logging and reverting changes made by those who misuse access.

4 Data recording and storage

4.1 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.

4.2 Updating

A VATSIM Member 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.

4.3 Storage

Data is stored in standard relational databases. Access is via a custom-built web based interface.

4.4 Retention periods

VATSIM data is retained indefinitely unless removal is requested from a VATSIM member, as outlined in this policy.

4.5 Archiving

VATSIM does not archive any data at this point in time, as data is currently retained indefinitely.

5 Transparency

5.1 Commitment

VATSIM is committed to ensuring all members 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 members can jointly enjoy the simulated aviation environment it provides.
- Data may be transferred to other organisations affiliated with, or associated with, the network to provide services to enhance and extend the simulated aviation environment.

5.2 Procedures

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

5.3 Responsibility

All staff within VATSIM are responsible for members data at all times. The various departments most closely associated with members 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 psuedomysed data should be used where possible.

6 Right of Access

6.1 Responsibility

Requests for personal data under the Right of Access are the responsibility of VP Membership and their team. Such requests are required to be complied with within one month of the request being received. If circumstances prevent this from occurring, an extension of a further two months may be instituted by VATSIM, providing that the member making the request is informed of this fact before the expiration of the original one month deadline.

6.2 Procedure for making request

Right of access requests must be in writing (this includes via electronic mail to the address specified on the VATSIM.net website).

If staff at a lower level receive anything that might reasonably be construed to be a request for access they have a responsibility to pass this to the Membership Manager responsible for their Region, Division, or lower subunit without delay, or refer this to the VATSIM Membership Department.

6.3 Provision for verifying identity

Where the person managing the access procedure does not know the individual personally there should be provision for checking their identity before handing over any information.

6.4 Charging

VATSIM will not charge any fee for providing data for requests under the Right of Access.

6.5 Procedure for granting access

The VP Membership is responsible for handling requests under the Right of Access provisions.

Requests will be made via the Membership Department Ticket system, who will then proof read the data and send it to the member making the request.

Because of the sensitive nature of who makes a comment on a CERT 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 CERT records, along with any security measures adopted by VATSIM, are redacted before sending it to the member.

7 Right of Rectification

7.1 Responsibility

Accurate data is in the best interests of both the network and the membership. The VP Membership is responsible for the management of such requests.

7.2 Procedure for making request

Right of rectification requests should in the first instance be made via the self-help system on the membership dashboard section of the VATSIM.net website by the member. If a member is unable to rectify their data via this system, they should raise a ticket using the same system.

If staff at a lower level receive anything that might reasonably be construed to be a request for rectification they have a responsibility to direct the member to the membership dashboard.

7.3 Disputes

Where there is a dispute between a member 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 be communicated to the member making the request within one calendar month of the request having been made.

7.4 Charging

VATSIM will not charge any fee for requests under the Right of Rectification.

8 Lawful Basis

8.1 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 members 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, solely for the enjoyment of its members.
- That the data is necessary to allow for the expected interactions between simulated pilots and air traffic controllers on the network to take place.
- 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 member(s) may act in a manner contrary to the VATSIM User Agreement, Code of Regulations and/or Code of Conduct.
- That as all members have a shared interest in these aims that the collection of such data should be reasonably expected by all members.

8.2 Members under 16 years

VATSIM accepts membership from any individual over the age of 13 years. Members under the age of 16 years require the consent of a parent or guardian in order for their personal data to be stored. Members under the age of 16 will be asked to provide such written permission. Members found to have falsified such permission will have their account suspended until they can prove to the membership department they have attained the age of 16 years.

No person under the age of 13 years shall be permitted to join the network. Any member found to have joined under the age of 13 years shall have their membership suspended until they have attained the age of 13 years and provided parental or guardian consent or have attained the age of 16 years.

8.3 Opting out

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

Members must be aware that if they choose to exercise either of these rights VATSIM is obliged to 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.

8.4 Timing of opting out

While a 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 retrospectively.

9 Right of Erasure

9.1 Responsibility

Requests for deletion of personal data under the Right of Erasure are the responsibility of VP Membership and their team. Such requests are required to be complied with within one calendar month of the request being received.

If circumstances prevent this from occurring, an extension of a further two months may be instituted by VATSIM, providing that the member making the request is informed of this fact before the expiration of the original one-month deadline.

9.2 Procedure for making request

Right of erasure requests should be in writing (this includes via electronic mail to the address specified on the VATSIM.net website).

On receipt of a verbal request for erasure staff concerned should immediately ask the member making the request to confirm the request in writing.

If staff at a lower level receive anything that might reasonably be construed to be a request for erasure they have a responsibility to pass this to the Membership Manager responsible for their Region, Division, or lower subunit without delay.

9.3 Provision for verifying identity

Where the person managing the erasure procedure does not know the individual personally there should be provision for checking their identity before deleting any information.

9.4 Charging

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

9.5 Procedure for granting erasure

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

10 Staff training & Acceptance of Responsibilities

10.1 Induction

All staff who have access to any kind of personal data should have their responsibilities outlined during their induction procedures. Formal guidance on data access and use of CERT is detailed in the relevant department handbooks.

10.2 Continuing training

If there are opportunities to raise Data Protection issues during staff training, team meetings, supervisions, etc these shall be undertaken.

10.3 Procedure for staff signifying acceptance of policy

All staff given CERT access above baseline (CERT level 1 and above) shall receive training on data access procedures via the documents outlined above. All such members are required to provide written acknowledgement they have received this training, that they understand the requirements of them, and their acknowledgement to be bound by them. Electronic mail is an acceptable (and the preferred) method for this acknowledgement.

Confirmation of this acknowledgement is to be recorded in the member's CERT record.

11 Policy review

11.1 Responsibility

The responsibility for review of this policy rests with VP Regions.

11.2 Procedure

At a minimum this review shall require:

- Consultation with the full Board of Governors
- Specific consultation with all Vice Presidents with responsibilities under this policy
- Consultation with the members of the Executive Committee
- Analysis of all audits of data access during the period of validity of the current policy
- Analysis of any data breaches during the period of validity of the current policy
- A new Data Protection Impact Assessment
- A new Legitimate Interest Assessment

11.3 Timing

In order for the required review to be completed by the required date (24 May 2021) such consultation shall commence no later than 24 Nov 2020.