

VATJPN

Data Protection & Handling Policy

VERSION 1

1st August 2021

Contents

Contents.....	2
Section 1 Summary	4
1.1 Definitions	4
Section 2 Introduction.....	4
2.1 Purpose of policy	4
2.2 Types of data	4
2.3 Policy Statement	5
2.4 Key Risks	6
Section 3 Responsibilities.....	6
3.1 Division Staff Group	6
3.2 Data Protection Officer	6
3.3 Specific Department Heads	6
3.4 Staff & Volunteers	6
3.5 Enforcement	6
Section 4 Security.....	7
4.1 Scope	7
4.2 Setting security levels	7
4.3 Security measures	7
4.4 Business continuity	7
4.5 Specific risks	7
Section 5 Data recording and storage.....	8
5.1 Accuracy	8
5.2 Updating	8
5.3 Storage	8
5.4 Retention periods	8
5.5 Archiving	8
Section 6 Transparency	8
6.1 Commitment	8
6.2 Procedures	9
6.3 Responsibility	9
Section 7 Right of Access.....	9

7.1 Responsibility	9
7.2 Procedure for making request	9
7.3 Provision for verifying identity	9
7.4 Charging	10
7.5 Procedure for granting access	10
Section 8 Right of Rectification	10
8.1 Responsibility	10
8.2 Procedure for making request	10
8.3 Charging	10
Section 9 Lawful Basis	10
9.1 Underlying principles	10
9.2 Members under 16 years	11
9.3 Opting out	11
9.4 Timing of opting out	11
Section 10 Right of Erasure	11
10.1 Responsibility	11
10.2 Procedure for making request	12
10.3 Provision for verifying identity	12
10.4 Charging	12
10.5 Procedure for granting erasure	12
Section 11 Staff training & Acceptance of Responsibilities	12
11.1 Induction	12
11.2 Continuing training	12
11.3 Procedure for staff signifying acceptance of policy	12
Section 12 Changes to This Policy	13
12.1 Responsibility	13
12.2 Procedure	13
12.3 Timing	13

Section 1 | Summary

1.1 Definitions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in RFC 2119.

VATSIM refers to the organization at <https://www.vatsim.net/>.

VATJPN refers to the organization at <https://vatjpn.org/>.

Section 2 | Introduction

2.1 Purpose of policy

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

- to comply with the law, particularly Japanese “Act on the Protection of Personal Information”, and the EU General Data Protection Regulation
- to ensure good data protection practice which when followed aims to protect members, staff, the organization and other individuals using our services.

2.2 Types of data

VATJPN collects a range of personal data on members, both provided by the members directly and from third parties.

2.2.1 Data provided to us by a third party

While a member is using VATJPN services, or when they request to join the VATJPN, data is

transmitted from VATSIM centrally to VATJPN for the purpose of ensuring the efficient functioning of our services and to provide the requested user experience. This data includes:

- The member’s full name
- Their email address
- Their country of residence
- Their age band
- The simulated Air Traffic Control and/or Pilot Rating they have obtained with the VATSIM network

- Positions of responsibility they hold with the network, including level of access

2.2.2 Data we collect from you

Whilst using our services, additional data is collected from and about you. This allows us to provide the efficient functioning of our services and to provide the requested user experience. This data includes:

- IP address and connection info
- Records of webpages visited and services utilized
- Individual training records
- Your requests for support
- Disciplinary history
- Communications with other members
- Any data you submit to our systems through forms or actions taken while using any of our services.

Communication platforms, such as our forum, have the functionality to receive any data, in the form of freetext, or media files. Any personal data willingly submitted here by individuals (e.g. personal data such as telephone numbers or addresses) will be retained and stored, even if removed from public view. This data is then only available to a limited number of authorized individuals.

2.3 Policy Statement

VATJPN 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 guidance for staff who handle personal data, so that they can act confidently and consistently
- Report any beliefs that a compromise of user data has occurred to the relevant data protection authorities voluntarily, even if not legally required to do so.

2.4 Key Risks

Key risks are detailed in Section 4.5 of this document.

Section 3 | Responsibilities

3.1 Division Staff Group

Overall responsibility for ensuring data protection and overall compliance with the relevant standards and legislation rests collectively with the VATJPN Staff Group.

3.2 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.

3.3 Specific Department Heads

Several members of the VATJPN Staff Group have specific responsibilities to oversee others accessing personal data collected by VATJPN:

- ATC Training Director – ATC Training Records
- Pilot Training Director – Pilot Training Records
- Web Services Director – Remote access to, and control of stored data

Other members of the VATJPN Staff Group may from time to time be tasked with specific responsibilities pertaining to the control and storage of data.

3.4 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 VATJPN as detailed in this policy. VATJPN expects the highest standard of probity of all staff at all levels. No access to data can take place unless there is a valid network related reason for such access.

3.5 Enforcement

VATJPN has a zero-tolerance policy towards inappropriate access to data stored within our systems. Any such access will result in the individual concerned being prohibited from having further access until such a time that the risk to personal data has been suitably mitigated.

Section 4 | Security

4.1 Scope

This section applies to all VATJPN's servers belonging to or donated to the VATJPN, including, but not limited to Data Servers, Statistic Servers, or Web Servers.

4.2 Setting security levels

VATJPN operates on a segmented security approach, where only the access required (with approval members holding the status of "Privileged Access") to complete a required job is granted.

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

4.3 Security measures

VATJPN employs standard methods of encryption to safeguard data, such as TLS encryption for accessing data via a web browser. VATJPN also implements additional change-audit scripts and monitors to provide visibility into server activity.

IP Address and asymmetric based security settings are used to only allow server access to authorized users or servers.

Any forms of passwords (excluding your network password which is never passed to VATJPN) are stored as salted hashes, preventing them from being viewed in plain text.

4.4 Business continuity

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

These backups are encrypted, and access is granted only to authorized individuals.

4.5 Specific risks

The main specific risks to the security of data are:

- Phishing attacks to gain server level access,
- Access by means of trojan or keylogging programs on members systems, and
- Access by unauthorized staff members who have been granted access

Mitigation of the first two risks is firstly by screening all individuals before granting access and secondary, 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.

Section 5 | Data recording and storage

5.1 Accuracy

The majority of membership data is passed to VATJPN by VATSIM. As such, we assume that this data is accurate. Where it is not, we facilitate the rectification of this, as set out in section 8 of this policy.

5.2 Updating

A VATSIM member may request an update of his/her information retained in VATJPN by making a request in writing to webmaster@vatjpn.org.

5.3 Storage

Data is stored in standard file systems and databases. Access to these systems is controlled by secure direct access to the controlling machine or application, or via a secure web interface. Access is further controlled and protected against unauthorized access using standard measures, such as role-based access control.

5.4 Retention periods

VATJPN is bound by the retention periods of VATSIM, set out in their Data Protection and Handling Policy.

Requests for erasure can be processed by VATJPN but may need escalating to VATSIM in order to fulfill the entirety of the request.

5.5 Archiving

VATJPN does not archive any data to other servers at this point in time for long term storage.

Data is either maintained within the production environment and backed up as per section 4.4, or deleted entirely.

Section 6 | Transparency

6.1 Commitment

VATJPN 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 within the VATJPN Privacy Policy, data is collected for the purpose of ensuring the provision of, and smooth operation of the VATJPN so that members can jointly enjoy the simulated aviation environment it provides.

Data may be transferred to other organizations affiliated with, or associated with, the division to provide services to enhance and extend the simulated aviation environment. Who we transfer data to is covered within the VATJPN Privacy Policy. Where it is not covered, we will seek your permission to pass on personally identifiable data before doing so.

6.2 Procedures

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

6.3 Responsibility

All staff within VATJPN are responsible for the data they access at all times. The various departments most closely associated with members' data are the Web Services Department and Division Staff Group.

Where staff are required to use data for statistical and management purposes, anonymous aggregated or pseudonymized data will be used where possible.

Section 7 | Right of Access

7.1 Responsibility

Accurate data is in the best interests of both the network and the membership. Division Director and Web Services Director is responsible for the management of such requests.

7.2 Procedure for making request

Right of access requests must be sent via email to webmaster@vatjpn.org.

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 Division Director and Web Services Director.

7.3 Provision for verifying identity

Where the person managing the access procedure does not know the individual personally, the individual's identity will be verified before handing over any information.

7.4 Charging

VATJPN will not charge any fee for processing or providing data for requests under the Right of Access.

7.5 Procedure for granting access

Division Director and Web Services Director is responsible for handling requests under the Right of Access provisions.

Requests will be made via email to webmaster@vatjpn.org.

Only personal data will be shared with the member. Other individuals' personal data will be redacted.

Section 8 | Right of Rectification

8.1 Responsibility

Accurate data is in the best interests of both the network and the membership. Division Director and Web Services Director is responsible for the management of such requests.

8.2 Procedure for making request

Right of rectification must be sent via email to webmaster@vatjpn.org.

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 Division Director and Web Services Director.

8.3 Charging

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

Section 9 | Lawful Basis

9.1 Underlying principles

VATJPN asserts that it has a legitimate interest in collecting and storing the personal data outlined above.

The reasons for this claim are:

- VATJPN 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 division, solely for the enjoyment of its members.
- That the data is necessary to allow for VATJPN staff to properly manage the division, both in day to day operations, and in circumstances where a member(s) may act in a manner contrary to the rules and regulations that govern the division.

9.2 Members under 16 years

VATJPN relies on VATSIM to ensure that parental consent is collected from users unable to provide their own consent (because they fall below the minimum age to do so, as defined under the GDPR or other local regulations).

VATJPN acknowledges its responsibility to inform VATSIM of any members that may be below this age and that are actively participating on the network without suitable consent.

9.3 Opting out

Notwithstanding VATJPN's claim of legitimate interest, members may object to this claim and/or request that VATJPN 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 VATJPN is obliged to lock their accounts in order to comply with their wishes and their request may be referred to VATSIM to take the appropriate action for their network account too.

9.4 Timing of opting out

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

Section 10 | Right of Erasure

10.1 Responsibility

Requests for deletion of personal data under the Right of Erasure are the responsibility of Division Director and Web Services Director. 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 VATJPN, providing that the member making the request is informed of this fact before the expiration of the original one-month deadline.

10.2 Procedure for making request

Right of erasure requests must be in writing. Members are requested to make their written request via email to webmaster@vatjpn.org.

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 Division Director and Web Services Director without delay.

10.3 Provision for verifying identity

Where the person managing the erasure procedure does not know the individual personally, the individual's identity will be verified before handing over any information.

10.4 Charging

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

10.5 Procedure for granting erasure

VATJPN shall evaluate all requests for erasure. VATJPN 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 legal claims.

Section 11 | Staff training & Acceptance of Responsibilities

11.1 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 this data is explained within their induction.

11.2 Continuing training

Opportunities to raise Data Protection issues shall be undertaken, including, but not limited to, during staff training, team meetings, and supervisions.

11.3 Procedure for staff signifying acceptance of policy

All staff within the division are required to agree to the relevant policies, as outlined within the VATJPN Privacy Policy.

Section 12 | Changes to This Policy

12.1 Responsibility

The responsibility for review of this policy rests with Division Director.

12.2 Procedure

At a minimum this review shall require:

- Consultation with the full Division Staff Group.
- Specific consultation with the Web Services Director(s)
- 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

12.3 Timing

In order for the required review to be completed by the required date (1 Aug 2023) such consultation shall commence no later than 1 Apr 2023.