DATA PROTECTION POLICY

EFFECTIVE 10 DEC 2023

Table of Contents

1. Control Pages 4
1.1. Document Identification 4
1.2. Revision Records 4
2. Summary 5
2.1. Definitions 5
3. Introduction 5
3.1. Purpose of Policy 5
3.2. Types of Data 5
3.2.1. Data Provided by a Third Party 5
3.2.2. Data we collect from you 6
3.3. Policy Statement 6
3.4. Key Risks 6
4. Responsibilities 7
4.1. Divisional Staff 7
4.2. Data Protection Officer 7
4.3. Specific Department Heads 7
4.4. Staff & Volunteers 7
4.5. Enforcement 7
5. Security 8
5.1. Scope 8
5.2. Setting Security Levels 8
5.3. Security Measures 8
5.4. Business Continuity 8
5.5. Specific Risks 8
6. Data Recording and Storage 9
6.1. Accuracy 9
6.2. Updating 9
6.3. Storage 9
6.4. Retention Periods 9
6.5. Archiving 9
7. Transparency 9

7.1. Commitment 9
7.2. Procedures 10
7.3. Responsibility 10
8. Right of Access 10
8.1. Responsibility 10
8.2. Procedure for Making Request 10
8.3. Provision for Verifying Identity 10
8.4. Charging 10
8.5. Procedure for Granting Access 10
9. Right of Rectification 11
9.1. Responsibility 11
9.2. Procedure for Making Request 11
9.3. Charging 11
10. Lawful Basis 11
10.1. Underlying Principles 11
10.2. Members under 16 Years 11
10.3. Opting Out 12
10.4. Time of Opting Out 12
11. Right of Erasure 12
11.1. Responsibility 12
11.2. Procedure for Making Request 12
11.3. Provision for Verifying Identity 12
11.4. Charging 12
11.5. Procedure for Granting Erasure 12
12. Staff Training & Acceptance of Responsibilities 13
12.1. Induction 13
12.2. Continuing Training 13
12.3. Procedure for Saff Signifying Acceptance of Policy 13
13. Government of this Policy 13
13.1. Responsibility 13
13.2. Changes and Amendments 13

1. Control Pages

1.1. Document Identification

Document Identification	
Type	Policy
Revision	Initial Document
Issue Date	01 FEB 2021
Effective Date	01 FEB 2021
Prepared By	John K – VATMENA1
Approved By	John K – VATMENA1
Next Review Due	10 DEC 2024
Identification	VATMENA_POL _DPP_V1-2023.pdf

1.2. Revision Records

Revision Number	Date	Summary of Changes	Authors
01/2021	01/02/2021	Initial issue	John K

2. Summary

2.1. Definitions

In this document, key terms such as "MUST," "MUST NOT," "REQUIRED," "SHALL," "SHALL NOT," "SHOULD," "SHOULD NOT," "RECOMMENDED," "MAY," and "OPTIONAL" are interpreted as described in RFC 2119.

VATSIM Middle East & Northern Africa, abbreviated as VATMENA. Our website is accessible at https://www.vatsim.me

Virtual Air Traffic Simulation Network, abbreviated as VATSIM. The website is accessible at https://vatsim.net

3. Introduction

3.1. Purpose of Policy

This policy is established with the following objectives in mind:

- To ensure compliance with applicable laws, particularly the EU General Data Protection Regulation (GDPR).
- To uphold best practices in data protection, aiming to safeguard the interests of members, staff, the organization, and other individuals utilizing our services.

3.2. Types of Data

VATMENA collects a variety of personal data from its members, obtained both directly from the members and from third-party sources.

3.2.1. Data Provided by a Third Party

During a member's use of VATMENA services or when requesting membership in the VATMENA division, data is transmitted from VATSIM centrally to VATMENA. This ensures the efficient functioning of our services and delivers the desired user experience. The transmitted data includes:

- Full name of the member
- Email address
- Country of residence
- Age band
- Simulated Air Traffic Control and/or Pilot Rating obtained within the VATSIM network.
- Positions of responsibility held within the network, including level of access.

3.2.2. Data we collect from you

While using our services, additional data is collected from and about you to facilitate efficient service functioning and provide the requested user experience. This data encompasses:

- IP address and connection information
- Records of visited webpages and utilized services.
- Individual training records
- Support requests
- Disciplinary history
- Communications with other members
- Any data submitted through forms or actions taken while using our services.

As we operate primarily through a Discord server, please note that Discord functions as our primary communication platform. Any personal data shared willingly within Discord, including text-based information, will be subject to our data protection practices. Access to this data is restricted to a limited number of authorized individuals within VATMENA.

3.3. Policy Statement

VATMENA is firmly committed to the following principles:

- Compliance: We are dedicated to complying with both legal requirements and best practices in data protection.
- Respect for Individual Rights: We recognize and uphold individuals' rights, including:
- The right of access
- The right of rectification
- The right to object
- The right to suspend protest
- The right of erasure
- Transparency: We are committed to openness and honesty in our dealings with individuals whose data we hold.
- Guidance for Staff: We provide clear guidance for staff members who handle personal data. This ensures they can act confidently and consistently in accordance with data protection principles.
- Reporting Compromises: Any belief or suspicion of a compromise of user data will be reported voluntarily to the relevant data protection authorities. This commitment extends even if not legally required to do so, demonstrating our dedication to maintaining the highest standards of data security and user privacy within VATMENA.

3.4. Key Risks

Key risks are detailed in Section 5.5 of this document.

4. Responsibilities

4.1. Divisional Staff

Overall responsibility for ensuring data protection and overall compliance with the relevant standards and legislation rests collectively with the VATMENA Divisional Staff (Div Staff).

4.2. Data Protection Officer

The appointed Data Protection Officer is listed on the VATMENA staff page here: https://www.vatsim.me/division/staff.

4.3. Specific Department Heads

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

- ATC Training Director – ATC Training Records
- Membership Director – Member related Records
- Technical Director – Remote access to, and control of stored data

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

4.4. Staff & Volunteers

All staff and volunteers within VATMENA are mandated to thoroughly read, comprehend, and accept any policies and procedures pertaining to the personal data they may handle during their engagement with VATMENA, as delineated in this policy. VATMENA expects the utmost standard of integrity from all staff members across all levels. Access to data is strictly conditional upon a valid network-related reason, ensuring that data access is always justified and in accordance with established protocols.

4.5. Enforcement

VATMENA upholds a zero-tolerance policy concerning inappropriate access to data stored within our systems. Unauthorized access will result in the individual in question being prohibited from further access until such time that the risk to personal data has been appropriately mitigated. This stringent approach underscores our commitment to maintaining the highest standards of data security and protecting the privacy of individuals within VATMENA.

5. Security

5.1. Scope

This section is applicable to all servers owned or contributed to the VATMENA division, encompassing Data Servers, Statistic Servers, and Web Servers, among others.

5.2. Setting Security Levels

VATMENA adopts a segmented security approach, granting access only to individuals with "Privileged Access" status, ensuring access is limited to what is necessary to fulfill specific roles. Access monitoring systems are implemented to prevent abuse and trace access back to specific individuals.

5.3. Security Measures

VATMENA employs standard encryption methods, including TLS encryption for web browser access, to secure data. Additional change-audit scripts and monitoring mechanisms provide visibility into server activity. IP address and asymmetric-based security settings are implemented to restrict server access to authorized users or servers. Passwords (excluding network passwords, which are never passed to VATMENA) are stored as salted hashes, preventing plaintext viewing.

5.4. Business Continuity

To ensure business continuity, VATMENA maintains encrypted backups of relevant systems. These backups are accessible only to authorized individuals, ensuring a prompt recovery of impacted systems while preserving data integrity and security.

5.5. Specific Risks

The primary specific risks to data security include:

- Phishing attacks to gain server-level access.
- Access through trojan or keylogging programs on members' systems.
- Unauthorized access by staff members who have been granted access.

Mitigation strategies include thorough screening of individuals before granting access, encouraging members with higher access levels to adhere to good security practices on personal systems, and addressing unauthorized access through access logging and reverting changes made by those who misuse access.

6. Data Recording and Storage

6.1. Accuracy

Most membership data is received by VATMENA from VATSIM, and we operate on the assumption that this data is accurate. If inaccuracies are identified, we facilitate the rectification process, as outlined in section 9 of this policy.

6.2. Updating

VATSIM members in VATMENA may request updates to their retained information by submitting a written request to privacy@vatsim.me.

6.3. Storage

Data is stored using standard file systems and databases. Access to these systems is controlled through secure direct access to the controlling machine or application, or via a secure web interface. Further access control and protection against unauthorized access are ensured through standard measures, including role-based access control.

6.4. Retention Periods

VATMENA adheres to the retention periods outlined by VATSIM in their Data Protection and Handling Policy. Requests for erasure can be initiated by VATMENA and may be escalated to VATSIM to fulfill the entirety of the request.

6.5. Archiving

As of now, VATMENA does not archive data to other servers for long-term storage. Data is either maintained within the production environment and backed up as described in section 5.4 or is completely deleted.

7. Transparency

7.1. Commitment

VATMENA is steadfast in ensuring that all members are informed about the data collected and the reasons for doing so. Aligned with the statement of legitimate interests in the VATMENA Privacy Policy, data is collected to guarantee the provision and seamless operation of the VATMENA division. This facilitates a collective enjoyment of the simulated aviation environment it offers to members. Data may be shared with other organizations affiliated with or associated with the division to enhance and extend the simulated aviation environment. The specifics of data transfers are covered within the VATMENA Privacy Policy. When not explicitly addressed, we will seek your permission before passing on personally identifiable data.

7.2. Procedures

Detailed procedures on how to exercise rights concerning the data held are provided in the relevant sections of this policy.

7.3. Responsibility

All staff within VATMENA bear responsibility for the data they access at all times. The Web Services Department and Division Staff Group are the departments most closely associated with members' data. In instances where staff need to utilize data for statistical and management purposes, anonymous aggregated or pseudonymized data will be prioritized whenever feasible.

8. Right of Access

8.1. Responsibility

Requests for personal data under the Right of Access fall under the purview of the appointed Data Protection Officer and their team. These requests must be fulfilled within one month of receipt. In circumstances where this is not possible, VATMENA may institute an extension of up to two months, provided the member making the request is informed before the original one-month deadline expires.

8.2. Procedure for Making Request

Requests under the Right of Access should be submitted via email to sar@vatsim.me. If lower-level staff come across anything that could reasonably be interpreted as a request for access, they are obligated to forward it to the appointed Data Protection Officer, as defined in section 4.2.

8.3. Provision for Verifying Identity

When the individual managing the access procedure is not personally acquainted with the requester, the identity of the individual will be verified before providing any information.

8.4. Charging

VATMENA does not impose any fees for processing or providing data for requests under the Right of Access.

8.5. Procedure for Granting Access

The appointed Data Protection Officer is responsible for handling requests under the Right of Access provisions. Requests should be submitted via sar@vatsim.me. Only personal data pertinent to the member will be shared, with redaction of personal data belonging to other individuals.

9. Right of Rectification

9.1. Responsibility

Ensuring accurate data is in the best interests of both the network and the membership. The appointed Data Protection Officer holds the responsibility for managing requests related to the Right of Rectification.

9.2. Procedure for Making Request

Requests for rectification should be submitted to privacy@vatsim.me. If lower-level staff encounter anything that could reasonably be seen as a request for rectification, they are obligated to direct the member to the above email address.

9.3. Charging

VATMENA does not impose any fees for requests under the Right of Rectification.

10. Lawful Basis

10.1. Underlying Principles

VATMENA asserts a legitimate interest in collecting and storing the outlined personal data based on the following principles:

- VATMENA is a voluntary community promoting flight simulations and virtual air traffic control, and all members seeking to join have an evident interest in such activities.
- The collected data represents the minimum required for the smooth and optimal operation of the division, solely for the enjoyment of its members.
- The data is necessary to enable VATMENA staff to effectively manage the division, both in day-to-day operations and in circumstances where a member(s) may act contrary to the division's rules and regulations.

10.2. Members under 16 Years

VATMENA relies on VATSIM to ensure that parental consent is obtained from users below the age of 16, as required by the GDPR or other applicable local regulations. VATMENA acknowledges its responsibility to inform VATSIM of any members below this age actively participating on the network without suitable consent.

10.3. Opting Out

Despite VATMENA's claim of legitimate interest, members have the right to object to this claim and/or request that VATMENA cease processing their personal data. These rights are known as the Right to Object and the Right to Restrict Processing. Members should be aware that exercising these rights may lead to the locking of their accounts to comply with their wishes, and such requests may be referred to VATSIM to take appropriate action for their network account.

10.4. Time of Opting Out

While notifications of objections to VATMENA's claim of legitimate interest or requests to suspend processing may be made at any time, such claims may not be made retrospectively.

11. Right of Erasure

11.1. Responsibility

Requests for the deletion of personal data under the Right of Erasure are the responsibility of the appointed Data Protection Officer and their team. Compliance with such requests is mandatory within one calendar month of the request being received. If circumstances prevent this, an extension of up to two months may be instituted by VATMENA, provided that the member making the request is informed of this fact before the expiration of the original one-month deadline.

11.2. Procedure for Making Request

The appointed Data Protection Officer is responsible for handling requests under the Right of Erasure provisions. Requests should be submitted via privacy@vatsim.me. If staff at a lower level receive anything that might reasonably be construed as a request for erasure, they have a responsibility to promptly forward this to the appointed Data Protection Officer.

11.3. Provision for Verifying Identity

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

11.4. Charging

VATMENA will not impose any fees for deleting data under the Right of Erasure.

11.5. Procedure for Granting Erasure

VATMENA shall thoroughly assess all requests for erasure. While VATMENA respects the Right of Erasure, it reserves the right to retain any data that it believes is in its legitimate interest to do so. Additionally, data may be retained if it is required to establish, exercise, or defend any legal claims. This evaluation ensures a balanced approach, considering both the individual's rights and the organization's legitimate interests.

12. Staff Training & Acceptance of Responsibilities

12.1. Induction

All staff within VATMENA with access to any form of personal data will have their responsibilities clearly outlined during their induction procedures. The details of data access and its proper use will be comprehensively explained as part of the induction process.

12.2. Continuing Training

Ongoing opportunities to address Data Protection issues will be provided, encompassing various avenues such as staff training sessions, team meetings, and supervisions. These platforms aim to ensure that staff members remain informed and updated on data protection practices.

12.3. Procedure for Saff Signifying Acceptance of Policy

Every staff member within VATMENA is mandated to acknowledge and accept the relevant policies, as explicitly outlined in the VATMENA Privacy Policy. This acknowledgment ensures a collective commitment to upholding data protection principles and complying with established policies.

13. Government of this Policy

13.1. Responsibility

The responsibility for review of this policy rests with the nominated Data Protection Officer, as defined in section 4.2 of this policy.

13.2. Changes and Amendments

We retain the right to amend this Policy at our discretion, with any modifications being effective immediately upon the posting of the revised Policy unless otherwise specified. The updated date in the policy document will reflect such changes. In the event of materially significant alterations to how we handle Personal Information, impacting your rights, or when required by law, we will seek your renewed consent for the processing of your Personal Information. This consent will be requested during your next login to our Website and Services. Additionally, we may opt to notify you through other means at our discretion, including the contact information you provided.

Your ongoing use of the Website and Services following the effective date of the revised Policy will be deemed as your consent to these changes, except as explicitly specified in the concluding paragraph.