SAN JUAN CERAP | DATA PROTECTION & HANDLING POLICY

Effective Date: 01-06-2022 (June 1st, 2022)

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 organisation at https://www.vatsim.net/.
- San Juan CERAP refers to the organisation at https://www.sanjuancerap.net/.

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 the EU General Data Protection Regulation
- to ensure good data protection practice which when followed aims to protect members, staff, the organisation and other individuals using our services.

2.2 Types of data

San Juan CERAP 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 San Juan CERAP services, or when they request to join San Juan CERAP, data is transmitted from VATSIM centrally to San Juan CERAP 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 utilised
- 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, including our discord server, have the functionality to receive any data, in the form of free-text. 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 authorised individuals.

2.3 Policy Statement
San Juan CERAP 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 San Juan CERAP Staff
Overall responsibility for ensuring data protection and overall compliance with the relevant standards and legislation rests collectively with the San Juan CERAP Staff.

3.2 Data Protection Officer
The appointed Data Protection Officer is listed on the San Juan CERAP staff page here: https://sanjuancerap.net/staff.

3.3 Specific Department Heads
Several members of the San Juan CERAP Staff have specific responsibilities to oversee others accessing personal data collected by VATSIM:

- ATC Training Director – ATC Training Records
- Web Master(s) – Remote access to, and control of stored data

Other members of the San Juan CERAP Staff 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 San Juan CERAP as detailed in this policy. San Juan CERAP 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
San Juan CERAP 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 San Juan CERAP servers belonging to or donated to San Juan CERAP, including, but not limited to Data Servers, Statistic Servers, or Web Servers.

4.2 Setting security levels
San Juan CERAP 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. San Juan CERAP 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
San Juan CERAP employs standard methods of encryption to safeguard data, such as TLS encryption for accessing data via a web browser. San Juan CERAP 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 authorised users or servers.

Passwords (excluding your network password which is never passed to San Juan CERAP) are stored as salted hashes, preventing them from being viewed in plain text.

4.4 Business continuity
In order to ensure business continuity, San Juan CERAP 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 authorised 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 unauthorised 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 San Juan CERAP 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 retained information by making a request in writing to atm@sanjuan.vatcar.net.

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 unauthorised access using standard measures, such as role-based access control.

5.4 Retention periods
San Juan CERAP is bound by the retention periods of VATSIM, set out in their Data Protection and Handling Policy. Requests for erasure can be processed by San Juan CERAP but may need escalating to VATSIM in order to fulfil the entirety of the request.

5.5 Archiving
San Juan CERAP 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
San Juan CERAP is committed to ensuring all members are aware of what data is collected and why we do so. As outlined in the San Juan CERAP Privacy Policy, data is collected for the purpose of ensuring the provision of, and smooth operation of the San Juan CERAP 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 division to provide services to enhance and extend the simulated aviation environment. Who we transfer data to is covered within the San Juan CERAP 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 San Juan CERAP are responsible for the data they access at all times. Where staff are required to use data for statistical and management purposes, anonymous aggregated or pseudonymised data will be used where possible.

Section 7 | Right of Access

7.1 Responsibility
Requests for personal data under the Right of Access are the responsibility of the appointed Data Protection Officer 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 San Juan CERAP, providing that the member making the request is informed of this fact before the expiration of the original one month deadline.

7.2 Procedure for making request
Right of access requests must be sent via email to atm@sanjuan.vatcar.net.

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 appointed Data Protection Officer, as defined in section 3.2.

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

7.5 Procedure for granting access
The appointed Data Protection Officer is responsible for handling requests under the Right of Access Provisions.

Requests will be made via atm@sanjuan.vatcar.net

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. The appointed Data Protection Officer is responsible for the management of such requests.

8.2 Procedure for making request
Right of rectification requests should be made to atm@sanjuan.vatcar.net.

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 above email address.

8.3 Charging

San Juan CERAP will not charge any fee for requests under the Right of Rectification.

Section 9 | Lawful Basis

9.1 Underlying principles
San Juan CERAP asserts that it has a legitimate interest in collecting and storing the personal data outlined above. The reasons for this claim are:

San Juan CERAP 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 San Juan CERAP 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 facility.

9.2 Members under 16 years
San Juan CERAP 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).

San Juan CERAPacknowledges 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 San Juan CERAP's claim of legitimate interest, members may object to this claim and/or request that San Juan CERAP 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 San Juan CERAP 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 San Juan CERAP'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 the appointed Data Protection Officer 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 San Juan CERAP, 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
The appointed Data Protection Officer is responsible for handling requests under the Right of Erasure Provisions.

Requests will be made via atm@sanjuan.vatcar.net

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 appointed Data Protection Officer 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
San Juan CERAP will not charge any fee for deleting data under the Right of Erasure.

10.5 Procedure for granting erasure
San Juan CERAP shall evaluate all requests for erasure. San Juan CERAP 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 facility are required to agree to the relevant policies, as outlined within the San Juan CERAP Privacy Policy.