Data Protection and Handling Policy

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 organization

Data and information

VATSUR 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

The information we collect is maintained with confidentiality to the extent possible. The following information is shared with VATSUR associated facilities:

- VATSIM CERT Identification Number (CID)

- Your name

- Your VATSIM achievements and ratings

- Your VATSIM associated email address

- VATSIM region and division associations

- VATSUR staff associations and VATSUR staff email addresses

The following information may be shared publicly:

- VATSIM CERT Identification Number (CID)

- Your name

- VATSUR staff associations and VATSUR staff email addresses

- VATSIM region and division associations

- VATSIM achievements and ratings

The following information is collected and may be used to protect our services, up to and including cooperation with legal requests for information from Law Enforcement agencies:

- The above listed public information,

- All IP addresses used and associated with your account

- Geolocation against aforementioned IP addresses

- Activities performed with the VATSUR web services

- Hours connected to the network and connected call sing.

The information we collect may be shared, in limited capacities, with the following:

- Virtual Air Traffic Simulation Network (www.vatsim.net)

- Law Enforcement agencies

- Google Analytics

We may store identification tokens and other limited information on your electronic device through web storage or cookie usage.

Cookie Usage

We use various technologies to collect and store information when you visit and use a VATSUR service. This may include a cookie or other similar technologies to identify your browser or device. We also use Google Analytics to help analyze the traffic to our websites and the information may be linked, by Google Analytics, with customers for information across multiple websites.

Our cookies are mainly used as a means of tracking virtual users across the VATSUR

domain. This allows us to know who is requesting and using our services, provide authentication and authorization checks to restricted areas.

You may choose to disable cookie usage via your browser, but know that doing so will prevent access and use across restricted areas of the website and severely degrade your experience.

Opt Out

Given the nature of our services, it is not possible to opt out of data collection and use our services. But if you desire to opt out and no longer desire to use our services, we will purge all information we have collected upon written request.

The first step is to deactivate and request VATSIM to purge your data. Please head to https://membership.vatsim.net/ to do so.

VATSIM, after processing your opt out, will forward the request to VATSUR for processing.

Note VATSUR cannot guarantee that information collected by parties outside of VATSUR will be purged in the process.

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 VATSUR as detailed in this policy. VATSUR 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.

Enforcement

VATSUR has a zero-tolerance policy towards inappropriate access to data stored within the VATSUR SERVER. Any such access will result in the individual concerned being prohibited from having further server. This may also preclude the member concerned from holding positions of responsibility within the network.

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 and VATSUR 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 and VATSUR 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.

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.

Procedure for staff signifying acceptance of policy

All staff given CERT access above baseline (CERT level 1 and above) and server access 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.