Data Handling Policy

Contents

1. Scope and Purpose

This Policy applies to VATAdria and its members.

The Policy details the requirements under the Data Protection Policy. In case of discrepancy or conflicts with local requirements, the latter shall prevail.

This Policy is binding and mandatory for all members of VATAdria as well as consultants.

The aim of this Policy is to find balance between the Data Subject's right to be forgotten and VATAdria legitimate interests to preform and support its activities in a sound manner.

1.1. Roles and responsibilities

Each member and visiting member of VATAdria has responsibility to ensure that they do not store Personal Data longer than what is required for the fulfillment of the purpose for which the Personal Data was collected.

Each Director and Assistant has responsibility to determine which categories of personal data are necessary for their processes and how long the data is needed for that purpose.

Web department has responsibility specifically, to ensure that Personal Data is Deleted in accordance with the instructions in this document in applicable systems, applications, databases etc. and that the methods used for Anonymization or Pseudonymization are adequate and sufficient to ensure compliance with applicable data protection regulations, hereunder the EU General Data Protection Regulations ("GDPR") in terms of the choice of technical measures and techniques.

1.2. Legal Background

As set in the GDPR:

- Personal Data shall be kept accurate and where necessary, up to date
- Data Processing shall be limited to what is strictly necessary to fulfill the purpose
- Personal Data shall not be hold longer than necessary for the purposes for which it was collected
- The Controller (and the Data Processor) shall ensure satisfactory, data security with regard to confidentiality, integrity and availability in connection with the Processing of Personal Data
- Data Subject shall have the right of access to, deletion of rectification of own Personal Data

GDPR Art. 17 states that a Controller, i.e. VATAdria, shall not store Personal Data longer than what is necessary to carry out the purpose of the Processing. This means that when VATAdria no longer has a legitimate purpose for using the Personal Data, such Data shall be Deleted. It will thus depend on the purpose for which the Personal Data is collected as well as the category or type of Personal Data how long it can be stored.

Where other laws or regulations contain provisions that deviate from the GDPR, those provisions shall apply and have precedence. There are other statutory requirements pursuant to which VATAdria is required to keep Personal Data for a longer period than actually needed by VATAdria, such as VATSIM's Data Protection and Handling Policy.

In addition to the above, it is a strong and fundamental human right for the Data Subject to be forgotten and to have their Personal Data Deleted as soon as possible. Furthermore, there is also a requirement upon all Controllers to ensure data minimization. This means that VATAdria must always have "need-to-have" approach when Processing Personal Data.

The Controller may in some instances store Personal Data for historical, statistical or scientific purposes, if the interest in the data being stored clearly exceeds the disadvantages. In such cases, the Controller shall ensure that the Personal Data are not stored in ways which make it possible to identify the Data Subject longer than necessary, which is typically relevant for the Web and Training Departments.

2. Methodologies

2.1. Main principles for deletion

Personal Data shall be deleted when it is no longer necessary for the purposes for which it was collected.

General Timelines for Deletion of user data have been set:

- Users that have never used any VATAdria's service: 6 months after population in VATAdria databases.
- User administration: 2 years after VATAdria membership termination.
- Training administration: 5 years after membership termination
- Upon receiving a GDPR "right to be forgotten"-request: Immediate deletion of all user data, except where data is used for statistical, historical or scientific purposes, or data retention is required by any of VATAdria parent organizations, where data should immediately be pseudonymized.

After these timelines, the Personal Data shall be Deleted. If one document includes several categories of Personal Data with different timelines for Deletion, for example if a document includes both user administration and training data, the longest timeline for Deletion shall be applied to such document.

Personal Data for Active Members are as a main rule not Deleted before the user has terminated their membership with VATAdria. This is because it is important for VATAdria to be able to track all the history with the member during the active engagement, for example if the member has questions pertaining to their historic training data or if there is a legal dispute or complaint pertaining to the membership. For example, it is required for VATAdria to keep all training data in order to be able to demonstrate that VATAdria has complied with VATSIM's Global Rating Policy when recommending a rating upgrade to a member, such as Training Reports evidencing student progression, or a Checkout Report evidencing sufficient controlling behaviour. The exception is that Personal Data that is incorrect or outdated, such as old email addresses that it is not necessary to keep anymore, in most cases shall be Deleted immediately, for example if requested by the member or when the purpose for keeping the data has expired.

Passive or unused member accounts and training requests will remain open until the member or VATAdria actively terminates the member account. However, it is important to observe the principle of data minimization also for active members, so when data is no longer needed for any purpose, the data should be Deleted for active members as well. Moreover, it can be argued that the

member's right to be forgotten is not fully applicable so long as the member has an active engagement with VATAdria. This typically applies to information about the member that was collected when applying to training or other activities during the lifetime of the membership that are vital for VATAdria to document its practices. Such information could be training or exam reports. There is also a need to keep all other activity history on the member as long as the member has an active relationship with VATAdria.

For terminated activities, the following data pertaining to such terminated activity shall not be Anonymized or Pseudonymized as long as the member has other active activities or engagements with VATAdria:

- Name, VASIM CID, or other equivalent identifier that enables the Web Department to verify that the activities belong to the same member,
- Type of activity and duration
- Training requests, training reports and exam reports
- Information regarding disputes in VATAdria with respect to the member in relation to such terminated activity
- Reason for the termination of the activity
- Application data from the member across activity lines, including applications closed or rejected before training completion
- Event Participation or Roster

In any case, data pertaining to the suspension or termination of memberships performed by VATAdria shall not be deleted. Such data shall be kept for as long as the Directors deems necessary, but shall be kept in accordance with the principles of data minimization.

2.2. Test Data

Test Data is used to preform critical maintenance and development activities inn applicable systems, in order to secure safe and reliable services and applications. Testing shall as a main rule always is performed on synthetic, Anonymized or at least Pseudonymized data if possible. In order to perform its task, the Web Department is dependent on the usage of Personal Data in some restricted parts of the test environment. All test data or other data used for statistical analysis shall be Anonymized and randomized.

2.3. Physical Archive

Physical Archives where Personal Data is stored shall not be kept and as such should be destroyed.

2.4. Backups

Preforming system backups is important in order to ensure sustainability of systems, application and data.

It is responsibility of Web Department to ensure that backups are handled in accordance with the requirements of this Policy

Backups shall be stored for a period of maximum 12 months, and thereafter be permanently deleted. Backups shall not be used as an archive or for other similar archival purposes; only legitimate purpose is to be able to restore data, ref GDPR art. 32.

If there is a need to restore data from a backup, this shall be approved by the Web Department and documented. The access to backups shall be strictly limited to a minimal number of people. Backups shall not be commonly available to the staff of VATAdria and it shall not be searchable in the general operating systems, databases and applications.

Backups shall be stored in such a manner that they are secured, protected and that confidentiality is maintained through the retention period, ref. GDPR art. 32.

As long as the backups are not generally searchable or available to the organization, the data subjects' right of access, right of restriction of Processing, right to rectification or deletion, right to portability and right to objections to Processing do not apply to backups. This is conditional upon the backups being scheduled for automatic deletion within a reasonable period of time, the access to backups being strictly limited and the use

The Web Department is responsible for ensuring that in the event deleted or incorrect data is restored, there shall be technical procedures in place to ensure that such data is re-deleted and corrected. Restoring in not permitted if it cannot be secured that deleted or rectified data are safeguarded in a manner compliant with the requirements of this document and the GDPR.

2.5. Unstructured Data

The GDPR generally and the requirements of this document specifically also applies to unstructured data, which is defined as Personal Data which is not part of:

- a core systems or application (e.g. Moodle)
- a satellite system (e.g. VATBOOK)
- a database or a data warehouse

This means that all information in physical archives and documents stored in formats such as e-mail, Word, Excel, PowerPoint etc. classifies as Unstructured Data.

The use of Unstructured Data shall be limited to minimum Unstructured Data pertaining to VATAdria's members is as a general prohibited. For such information, the Unstructured Data must be put in a structured format and thereafter deleted. If there is a legitimate reason why Personal Data must be processed as unstructured data, this must be documented in writing.

It is the responsibility of each Director or Assistant to ensure compliance with these requirements within their departments. All Directors and assistants must prepare routines for sustainable solutions in respect of handling Unstructured Data going forward within their departments and ensure communications of such rules and routines.

Documentation pertaining to member data which needs to be stored shall be archived in a structured data.

The Web Department is responsible for enabling size limitation on *@vatadria.net inboxes and on VATAdria's cloud services in order to limit the amount of data possible to store in an unstructured manner. The Web Department is also responsible for implementing a technical solution to enable identification of Personal Data amongst the Unstructured Data in the services under his control.