DATA HANDLING POLICY

Version 1.0
Last reviewed 25.03.2021

VATSIM SCANDINAVIA

Table of contents

1. Scope and Purpose

This Data Handling Policy (the “Policy”) applies to VATSIM Scandinavia and its members (“vACCSCA”).

The Policy details the requirements under the Data Protection Policy (the “DPP”). In the case of discrepancies between local requirements and this Policy, the latter shall prevail. If anything in this document conflicts with relevant local mandatory laws or regulations, the latter shall prevail.

This Policy is binding and mandatory for all members of vACCSCA as well as visiting members and consultants. Furthermore, the principles set out in this document shall apply similarly to all external Data Processors who process Personal Data on behalf of vACCSCA.

The aim of this Policy is to find the optimum balance between the Data Subject’s right to be forgotten and vACCSCA’s legitimate interests to process Personal Data in order to perform and support its activities in a sound manner. The purpose of this Policy is thus to ensure that Personal Data is Deleted in accordance with applicable laws and regulations in all applicable systems, applications and locations. The scope of this Policy is both member data, non-member data, and staff data, both structured and unstructured data.

Roles and Responsibilities

It is the responsibility of each member and visiting member of vACCSCA to ensure that they do not store Personal Data longer than what is required for the fulfilment of the purpose for which the Personal Data was collected, for example on their Personal Computers, in their email inboxes, in paper copies etc.

It is the responsibility of each Director and Assistant (as defined in vACCSCA's Constitution) to determine which categories of personal data is necessary for their processes and how long the data is needed for that purpose. This shall be specified and available to the Data Protection Officer (the "DPO"), Web Department and Director upon request. The DPO shall assist in identifying statutory retention obligations, such as training reports etc. The Wep department shall decide the requirements for data maintenance and data administration for the relevant IT application.

It is the responsibility of the Web department and the IT asset owner (i.e. the person designated as such by the Web department) specifically, to ensure that Personal Data is Deleted in accordance with the instructions in this document in applicable systems, applications, databases, production- and pre-production environments etc. (including unstructured data) 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 Regulation (the "GDPR") in terms of the choice of technical measures and techniques. Furthermore, it is the responsibility of the IT asset owner to implement the requirements set by the Web Department in terms of data maintenance and data administration in the relevant IT asset.

Each Director and Assistant is responsible for performing first line controls for their processes in compliance with the requirements of this document within their respective departments. In addition, the DPO may perform second line controls monitoring the adherence to these requirements.

Legal Background

As set out 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 fulfil the purpose,

- Personal Data shall not be held longer than necessary for the purposes for which it was collected, i.e. when the data is no longer required it shall be Deleted,
- The Controller (and any external Data Processor) shall ensure satisfactory, data security with regard to confidentiality, integrity and availability in connection with the Processing of Personal Data, and
- Data Subject shall have the right of access to, deletion of and rectification of own Personal Data.

GDPR Art. 17 states that a Controller, i.e. vACCSCA, shall not store Personal Data longer than what is necessary to carry out the purpose of the Processing. This means that when vACCSCA 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 vACCSCA is required to keep Personal Data for a longer period than actually needed by vACCSCA, such as VATSIM's Data Protection and Handling Policy. This may lead to an obligation to store Personal Data in particular and separate archives but to Delete the same data in the front- and core-end applications.

In addition to the above, it is a strong and fundamental human right for the Data Subjects 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, i.e. that a Controller does not request, gather or process more Personal Data than what is strictly required. This means that vACCSCA must always have a "need-to-have" rather than a "nice-to-have" approach when Processing Personal Data.

The Controller may in some instances store Personal Data for historical, statistical or scientific purposes, if the public interest in the data being stored clearly exceeds the disadvantages this may entail for the Data Subject. 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. Such prolonged storage must be approved by the relevant Director, based on a recommendation from the DPO.

2. Methodologies

Main Principles for Deletion

As set out above, Personal Data shall be Deleted when it is no longer necessary for the purpose(s) for which it was collected. Each Director and Assistant shall specify the retention requirements for their respective processing activities to the Web Department. In addition, each Department shall specify the retention requirements pursuant to local legislation in separate documentation as needed. Any additions, changes to or deviations from the retention requirements must be pre-approved by the respective Director, with a recommendation from the DPO.

As set out above; when there is no longer a legitimate need for use of the Personal Data; the data must be Deleted. For this reason, the following set of general timelines for Deletion of user data have been set:

- Users that have never used any of vACCSCA's services: 6 months after population in vACCSCA databases.
- User administration: 2 years after vACCSCA 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 vACCSCA's 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.

As can be seen from the table above, Personal Data for Active Members are as a main rule not Deleted before the user has terminated their membership with vACCSCA. This is because it is important for vACCSCA 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 vACCSCA to keep all training data in order to be able to demonstrate that vACCSCA 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. Reference is made to the DPP for more information on how to handle rectification or deletion requests from the members.

Passive or unused member accounts and training requests will remain open until the member or vACCSCA actively terminates the member account. However, it is important to observe the principle of data minimization also for active members, so when the 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 still has an active engagement with vACCSCA. 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 vACCSCA 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 vACCSCA.

For terminated activities, the following data pertaining to such terminated activity (i.e. training request, CPT etc.) shall not be Anonymized or Pseudonymized as long as the member has other active activities or engagements with vACCSCA:

- Name, VATSIM CID, or other equivalent identifier that enables the Web department to verify that the activities belong to the same member,
- Type of activity, duration of engagement,
- Training requests, training reports and exam reports,
- Information regarding disputes in vACCSCA 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 vACCSCA shall not be deleted. Such data shall be kept for as long as the Director deems necessary, but shall be kept in accordance with the principles of data minimization (i.e. only store CID).

Test Data (Analysis/Maintenance)

Test Data is used to perform critical maintenance and development activities in applicable systems, in order to secure safe and reliable services and applications. Testing shall as a main rule always be 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. Any and all test data (live data exported for testing purposes) or other data used for statistical purposes shall be suitably Anonymized and randomized in order to protect the anonymity of the relevant Data Subjects and general protection of the Personal Data prior to being used for testing. Test data shall be regularly audited for compliance by the DPO.

When limited test data is required where Anonymizing or Pseudonymizing might not be practical, an expiry date of 90 days shall be set.

Physical Archive

Physical Archives (i.e. printed out data) shall not be kept. All physical records of Personal Data existing at the time of the creation of this Policy shall be Deleted immediately.

Backups

Performing system backups is important in order to ensure sustainability and availability of systems, applications and data. Sound backup policies are also an explicit requirement of GDPR art 32.1 (b) and (c) where it is stated that vACCSCA must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including the ability to ensure the "*ongoing confidentiality, integrity, availability and resilience of processing systems and services,*" and the ability to "*restore the availability and access to personal data in a timely manner*" in the event of a physical or technical incident.

However, the legitimate need to keep backups in order to ensure sound IT management must be weighed against other principles regarding Processing of Personal Data. Data subjects have several fundamental rights, such as the right to be forgotten, right to restriction of processing and right of access to their own Personal Data, which must be taken into account when determining the scope and retention period of backups in vACCSCA.

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

Backups shall be stored for a period of maximum 14 months, and thereafter be permanently deleted. Backups shall be put beyond use and shall not be used as an archive or for other similar archival purposes; the only legitimate purpose of backups is to be able to restore data as set out in GDPR art. 32.

If there is a need to restore data from a backup, this shall be approved by the Web Services Director and documented in writing. The access to backups shall be strictly limited to a minimal number of people, and only those who need access to

backups in order to perform their regular tasks and have a legitimate need for such access. Backups shall not be commonly available to the staff of vACCSCA and it shall not be searchable in the general operating systems, databases or applications.

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

As long as the backups are not generally searchable or available to the organization, the Norwegian Data Protection Authority has accepted that the data subjects' right of access, right to restriction of Processing, right to rectification or deletion, right to data 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 of backups being limited to restoring only (as per GDPR art. 32).

The Web Services Director 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 is 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.

Unstructured Data

The GDPR generally and the requirements of this document specifically also applies to unstructured data. Unstructured Data is defined as Personal Data which is not integrated in either:

- a core system or application (for example Control Center and Handover);
- a satellite system (for example VATBOOK); or
- a database or a data warehouse.

This means that all information in physical archives and documents stored in formats such as e-mails, Word, Excel, PowerPoint etc., pictures, videos etc. constitutes Unstructured Data. This also applies to shared folders (such as on

Google Disk or Dropbox), personal folders and online tools (for example Discord, the Forums, Trello, Slack, Jira etc.).

The use of Unstructured Data shall be limited to a strict minimum. Unstructured Data pertaining to vACCSCA's members is as a general rule 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 (i.e. stored) in an unstructured manner, this must be documented in writing and sent to the DPO.

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 respective departments and ensure communications of such rules and routines within their departments. This will also help avoid time-consuming clean-up reviews on an irregular basis.

Documentation (including e-mails) pertaining to member data which needs to be stored shall be archived in a structured format.

The Web Services Director is responsible for enabling size limitations on *@vatsim-scandinavia.org inboxes and on vACCSCA's cloud services in order to limit the amount of data possible to store in an unstructured manner. The Web Services Director is also responsible for implementing a technical solution to enable identification of Personal Data amongst the Unstructured Data in the services under his control.

3. Governance

This Policy shall be reviewed and updated once a year by the DPO. Next review shall be performed by 24th of March, 2022.

4. APPENDIX A - SPECIFIC REQUIREMENTS REGARDING UNSTRUCTURED DATA

A. All staff and *@vatsim-scandinavia.org e-mail inboxes:
    a. Obsolete e-mails with member Personal Data shall be deleted immediately
    b. If a team (such as the Web department) has a joint e-mail account, e-mails with member Personal Data shall not be sent from the staff member's own email account
    c. To the extent technically possible, Deleted items in the relevant email application must be permanently deleted upon membership termination
    d. E-mails pertaining to Sensitive Personal Data (such as health data or data about legal minors) shall be archived in a structured manner where required and thereafter deleted immediately.
B. All staff, examiner, and mentor personal computers:
    a. Member Personal Data shall not be kept in personal files.
    b. Unstructured Data stored on personal computers (if any exceptions are approved by the DPO) must be structured in a way that makes deletion and accessibility possible. Staff, examiners and mentors must periodically (at least every 2 months) ensure that no Personal Data is stored as Unstructured Data in non-compliance with the rules of this Policy description or the GDPR
    c. Documents/files moved to a structured format shall be deleted thereafter from the personal folders in order to avoid duplicates and data maximization
C. Joint mailboxes:
    a. Member correspondence and internal e-mails shall be deleted after 12 months
    b. The e-mails that are subject to statutory retention requirements shall be stored in a structured manner in the relevant IT application and thereafter deleted within 12 months (at the latest).
    c. Obsolete emails shall be deleted immediately

D. Shared folders and collaboration platforms (for example Google Disk, Dropbox, Trello etc.)
    a. Unstructured Data stored in shared folders must be structured in a way that makes deletion and accessibility possible. Folder owners must on a regular basis (at least every 2 months) ensure that no Personal Data is stored as Unstructured Data in non-compliance with the rules of this Policy or the GDPR
    b. Documents/files moved to a structured format shall be deleted thereafter in the shared folders in order to avoid duplicates and data maximization

E. Physical Archives:
    a. Physical archiving shall not take place
    b. Current physical archives shall be digitalized or shredded

F. Questionnaire:
    a. Each Director of a Department is responsible for completing the below questionnaire. An overview must be prepared of which files and documents the department keeps in an unstructured format, as well as location. This only applies to files and documents containing Personal Data.

Scope	Question	Answer
Files to be moved into structured format	Which folders/documents shall be moved into a structured format?	
Files to be moved into structured format	Who is responsible for the moving?	
Files to be moved into structured format	What is the future sustainable solution for deletion and retention?	
Files to be moved into structured format	Are appropriate access controls implemented?	

Files to be deleted	How is adequate deletion ensured?	
Files to be deleted	Who is responsible for the deletion?	
Files to be deleted	Are appropriate access controls implemented?	
General cleaning	When do you expect the above cleaning activities to be completed?	

Each Director is responsible for performing first line controls of compliance with the requirements of this procedure within their respective departments. The questionnaire in Appendix A shall be completed by each Director by 31st of May each year and delivered to the DPO by sending an email to dpo@vatsim-scandinavia.org.