DATA PROTECTION IMPACT ASSESSMENT: CONTROL CENTER & HANDOVER

Version 1.0
Last reviewed 18.02.2021

VATSIM SCANDINAVIA

Table of contents

1. Introduction

1.1. Background and Aims

This Data Protection Impact Assessment (DPIA) is used to investigate, recognize and mitigate potential risks to the personal data processed by Control Center (CC) and Handover. Hereafter, "*the UMS*" will refer to CC and Handover in combination.

With this DPIA, VATSIM Scandinavia aims to, in the long or short term:

- Better understand the data protection risks that will be faced in the development and usage of the UMS,
- Calculate methods to decrease or eliminate those risks,
- Weigh the benefits of the UMS against the data protection risks,
- Document data protection measures to demonstrate GDPR compliance to supervisory authorities, and
- Identify opportunities to incorporate *data protection by design*-principles into the UMS.

EU's GPDR requires that a DPIA is carried out *where a type of processing […] is likely to result in a high risk to the rights and freedoms of natural persons*. CC and Handover are deemed to require a DPIA, according to law.

1.2. Approach

The methodology used to conduct this DPIA is based on the guidance in Article 35, Recital 75 and Recital 90 of the EU's GDPR; the WP29 guidelines on DPIA; the UK Information Commissioner's Office; and the Norwegian Supervisory Authority (Datatilsynet).

This DPIA is conducted and documented by VATSIM Scandinavia's DPO, who will reassess this DPIA regularly.

2. Assessment

2.1. Purpose and Description of Processing Activities

2.1.1. The Nature of Processing

CC does automatic decision-making to facilitate correct and expeditious handling of training requests following any relevant policies or procedures.

Large-scale data processing may find place on the UMS. Its purpose is to process the data of all VATSIM Scandinavia members and visiting members (VATSIM members from outside of VATSIM Scandinavia).

The data processed in the UMS is **matched** with data from third-party datasets. VATSIM Scandinavia is a subsidiary of VATSIM Europe Division, VATSIM Europe Region, and VATSIM. Therefore, VATSIM Scandinavia relies on data controlled and processed by the parent organizations mentioned above.

Vulnerable data subjects such as children, mentally ill, persons that for some reason cannot provide legal consent, and elderly persons may be subject to the processing of their data by the UMS. VATSIM Scandinavia has a minimum age limit of 13 years and does not discriminate against people for any other reason. Furthermore, VATSIM Scandinavia's ability to confirm the age of its members is limited as such data is controlled and processed solely by VATSIM.

Data processed by the UMS can be used to **prevent** data subjects from using VATSIM Scandinavia's and its parent organizations' services to some or a full extent. Such an example may be because VATSIM Scandinavia or any parent organizations flag a member as inactive or suspended. Such a determination may be automatic.

The highest-risk processing activity done by CC is the processing of data related to a data subject's **performance and development** of individual skillsets, which is done due to CC's nature of being a training tracker and administration system.

The paragraphs listed above discuss types of processing that are identified as likely to *result in a high risk to the rights and freedoms of natural persons*.

The personal data the UMS processes originate from *VATSIM Connect*, which is VATSIM's single sign-on, and the *VATSIM Data API*. Such data is stored in VATSIM Scandinavia's database. Data is deleted from the UMS via a static script in CC. Please refer to the data flow diagram in Annex A.

2.1.2. The Scope of Processing

The amount of data processed in the UMS depends directly on the number of users logged in via Handover. A VATSIM member flagged as a VATSIM Scandinavia member is not necessarily subject to the processing of their data in the UMS. Handover processes personal data of a member only when they log into a system supported by Handover. Similarly, the UMS may process data of data subjects that are not a VATSIM Scandinavia member, so long as they are a VATSIM member.

Personal data is processed following the principles of storage limitation, ref. Art. 5 and Recital 39 of the GDPR. Moreover, VATSIM Scandinavia is bound by its *Data Protection Policy* and VATSIM's *Data Protection and Handling Policy*. For these reasons, data that does not explicitly require erasure according to the GDPR is anonymized or pseudonymized when a *Right of Erasure*-request has been made to VATSIM Scandinavia. Such data is de-pseudonymized when the data subject logs in to Handover again, in which case the data subject will need to accept the *Data Protection Policy* again. Whenever a *Right of Erasure*-request has been made to VATSIM, VATSIM Scandinavia will ensure the deletion of all personal data on that data subject and cease processing their data.

2.1.3. The Context of Processing

All of the data subjects are members of VATSIM that want to use VATSIM Scandinavia's systems. There may be several reasons for this, but persons wishing to get an ATC rating in VATSIM Scandinavia make up most of the data subjects.

A data subject's rights protected under Chapter 3 of the GDPR are respected and enforced by VATSIM Scandinavia. This means that the data subjects have full control of their data should they want to exercise any of these rights.

Furthermore, the GDPR defines valid consent as "*freely given, specific, informed and […] indicated by […] clear, affirmative action*." VATSIM Scandinavia has made every effort to ensure that its consent processes meet the standards set forward by the GDPR. The *Data Protection Policy* is readily available on VATSIM Scandinavia's websites. Consent must be given before the first-time login to Handover and when the policy has been updated. There are some children under the age of 18 having their data processed by the UMS. As VATSIM has set a minimum age limit of 13 years, efforts are made to ensure that children under the age of 13 are not data subjects to the UMS. It is important to note that VATSIM Scandinavia does "bundle" specific terms of consent, which may call into question the *freely given* aspect of consent. For example, consent for e-mail notifications is assumed unless actively unselected. Other than that, VATSIM Scandinavia takes extraordinary measures to ensure that consent is freely given and to ensure transparency in how personal data is processed.

Personal data is stored in standard filesystems and databases. Standard authentication is required before authorization per information security principles. The technology used in the UMS is not considered novel. Primary concerns to security flaws in this type of processing are that backups and pre-production environments are not physically separated from the production environments, which is not according to reasonable information security principles. The reasoning for this is finances: VATSIM Scandinavia is a non-profit organization living on the finances that donators can provide.

2.1.4. The Purposes of Processing

CC exists primarily to manage and handle all VATSIM members who want to be trained as a virtual ATC in VATSIM Scandinavia – from the point a training request is made until the examination and checkout are complete. Secondary purposes include member management and support of VATSIM Scandinavia's members, staff, and board's daily operations.

Handover exists to centralize VATSIM Scandinavia's processing of the personal data that VATSIM controls and acts as a single sign-on for VATSIM Scandinavia's services. Handover's secondary purposes include the management of VATSIM Scandinavia's member roster, with additional attributes such as local bans or the flagging of activity, as per VATSIM Scandinavia's constitution.

The intended effect the UMS has on individuals is expeditious and correct handling of their training requests and that it would support their daily operations.

VATSIM Scandinavia benefits from this processing because it enables the organization to fulfil the requirements and responsibilities set forth by its parent organizations. Namely, this is the handling of training requests and the daily management of its members. In a broader sense, the data processing will help ensure that VATSIM Scandinavia's members' rights are upheld and would likely be a contributing factor to the increase in active membership.

2.2. Consultation

VATSIM Scandinavia values transparency and democracy. Therefore, all stakeholders are presented with significant changes to systems or processes and encouraged to contribute their opinions. VATSIM Scandinavia has a hierarchical consultation process. Any major operations are overseen and approved by direct managers of the process owners before any other stakeholders are consulted.

VATSIM Scandinavia does not have a micromanaging culture; therefore, minor processes are seldom consulted with stakeholders.

External information security consultants are not expected to be used by VATSIM Scandinavia. IT departments and other personnel of other organizations within the VATSIM umbrella may be consulted during the development and usage of the UMS.

2.3. Necessity and Proportionality Assessment

The GDPR, being the highest-standard legal framework for data protection in the world, puts forth a set of principles to adhere to as a data controller and processor.

Art. 5 of the GDPR requires that personal data shall be:

- Processed lawfully, fairly and in a transparent manner,
    - VATSIM Scandinavia adheres to Art. 6 of the GDPR with regards to the lawfulness,
    - No data is being processed unfairly, and
    - VATSIM Scandinavia always aims to be as transparent as possible in all of its processes, especially with regards to personal data.
- Collected for specified, explicit and legitimate purposes,
    - VATSIM Scandinavia does not collect data without a purpose, and those purposes are legitimate.
- Adequate, relevant, and limited to what is necessary,
    - VATSIM Scandinavia does not collect more data than necessary.
- Kept […] for no longer than [what] is necessary, and
    - VATSIM Scandinavia is bound by VATSIM's *Data Protection and Handling Policy* and deletes data upon their request.
- Processed in a manner that ensures […] security.
    - VATSIM Scandinavia values data confidentiality and integrity, and thus, data is processed per acceptable information security practices.

Furthermore, the GDPR requires that a data controller shall be able to demonstrate compliance with the principles mentioned above. VATSIM Scandinavia's DPO regularly performs audits on the organizations internal controls to ensure these principles are upheld.

It is deemed that the purposes of the UMS are achieved by the actual processing that is done. It has been discussed that Handover could have been removed completely, and instead, an API of sorts could be used in each service. However, this was deemed to create too many links in the chain, thus decreasing overall security and data processing control. CC's purposes cannot be fulfilled by other means.

Data quality is ensured by a daily pull from VATSIM Connect to Handover. CC logs are stripped of IP addresses after 14 days and are deleted after 3 months.

International transfers of data cannot be guaranteed to be secure, as VATBOOK transfers are done by the unsecured HTTP protocol.

2.4. Inherent Risk Identification and Assessment

Risk	Likelihood	Impact	Overall Risk
Internal data leakage	High	Medium	Medium
External data leakage	Medium	Medium	Medium
Data obsolescence	Medium	Low	Low
Loss of data availability	Low	High	Low
Misuse of data	High	Medium	Medium
Failure to adhere to DPP	High	High	High

2.5. Mitigating Actions to Reduce Risk

Risk	Mitigating Action	Effect	Residual Risk
Internal data leakage	Data monitoring, low turnover of managerial positions, effective IAM	Reduced likelihood	Medium
External data leakage	Data monitoring, healthy internal controls	Reduced likelihood	Low
Data obsolescence	Accepted risk	N/A	Low
Loss of data availability	Monitoring of system availability, good SLAs with service providers	Reduced likelihood	Low

Misuse of data	Data monitoring, healthy internal controls	Reduced likelihood	Low
Failure to adhere to the DPP	Healthy internal controls	Reduced likelihood	Medium

3. Sign-Off

This DPIA has been conducted and approved by VATSIM Scandinavia's DPO, Henrik Sønstebø. He has also signed off on the inherent and residual risks. The DPIA will be kept under review by the DPO.

4. Annex A. Data Flow Diagram