

# PERSONAL DATA BREACH AND DEVIATION HANDLING ROUTINE

---

Version 1.0

Last reviewed 25.03.2021



## Table of contents

Scope and Purpose	4
<b>Methodologies</b>	<b>6</b>
Internal Deviation Handling	6
Containing the Incident	7
Classification of the Personal Data Breach	7
Data Breach reporting to Competent Authorities	8
Deviation reporting to Parent Organizations	9
Cross-Border Processing	9
Information to the affected Data Subjects	10
Subsequent Evaluation and Documentation	11
<b>Governance</b>	<b>12</b>
<b>APPENDIX A. Summary of Actions</b>	<b>12</b>



# 1. Scope and Purpose

This Personal Data Breach and Deviation Handling Routine (the “Routine”) applies to VATSIM Scandinavia and its members (“vACCSCA”).

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

This Routine 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. Each Director is responsible for the implementation of this Routine within their department.

The aim of this Routine is to ensure swift, correct and proper handling of deviations and reportable incidents under the GDPR as set out in article 33 and 34 of the GDPR.

A Personal Data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed. This means that both loss of confidentiality, integrity and availability of Personal Data may constitute a Personal Data breach. As a starting point, all Personal Data breaches must be reported to the Data Protection Officer (the “DPO”), unless the Personal Data Breach is unlikely to result in a risk to the rights and freedoms of a Data Subject. When the Personal Data breach is likely to result in a high risk to the rights and freedoms of a Data Subject, the Controller (i.e. vACCSCA) shall also notify the concerned Data Subject of the breach without undue delay.

It might be necessary for staff members to report the same incident across multiple channels. The purpose of this Routine is to ensure that deviations from the

set of governing documents of vACCSCA in terms of data protection and privacy as well as any and all Personal Data breaches are properly and adequately addressed in a sound manner and without undue delay, in accordance with the GDPR. The main purpose of the deviation handling is to close the deviation as fast as possible, secure relevant personal data and prevent reoccurrence. Furthermore, this Routine shall help identify improvements to vACCSCA's internal control regimes in order to ensure that adequate measures are put in place to avoid that future similar non-conformances take place. The Web Department and DPO in conjunction shall maintain a log with overviews of data breaches within vACCSCA. The log shall be made available to the Board upon request.

## 2. Methodologies

### Internal Deviation Handling

Incidents covered by this Routine can arise from, but are not limited to, these different situations or non-conformances:

- Non-compliance with vACCSCA's internal policies or routines, including, but not limited to the Data Handling Policy
- Actions performed by staff, mentors or examiners, such as breaches of the Data Handling Policy, or non-intentioned/accidental actions stemming from inadequate training or awareness
- Actions performed by external parties, such as cyber compromises
- Actions performed by staff, mentors, examiners, or consultants as a result of social engineering

A Personal Data breach can be categorised according to the following three principles:

- "Confidentiality breach" - Where there is an unauthorised or accidental disclosure of, or access to, Personal Data
- "Integrity breach" - Where there is an unauthorised or accidental alteration of Personal Data, compromising the confidence in the correctness of the data

- “Availability breach” - Where there is an accidental or unauthorised loss of access to, or destruction of, Personal Data

A Personal Data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to Data Subjects such as loss of control over their Personal Data or limitation of their rights, discrimination, identity theft and fraud, financial loss, unauthorized reversal of pseudonymisation, damage to reputation, loss of confidentiality of Personal Data protected by professional secrecy or any other significant economic or social disadvantage to the Data Subject concerned. The main priority in case of a Personal Data breach is thus to contain and control the breach or deviation as soon as possible.

Personal Data breaches often require a rapid reaction and must be reported immediately. All staff are responsible for reporting any known or suspected Personal Data breach to the DPO.

The DPO is responsible for ensuring timely and appropriate notification to the Board and Director, as well as to the Competent Authority if necessary.

### **Containing the Incident**

Upon identifying an incident, the first priority is to contain the incident and prevent further Personal Data breaches if possible. This is the responsibility of the person detecting the data breach as well as the Director in question. Once the issue is contained and under control, focus should be returning to the ordinary course of business and prevent reoccurrence of the same form of incidents. Follow-up and handling of deviations and Personal Data breaches, including mitigating actions and controls to ensure that similar events do not occur again is the responsibility of the relevant Director and the DPO.

### **Classification of the Personal Data Breach**

In evaluating whether reporting to the Competent Authority and the Data Subject is required, due consideration should be given to the circumstances of the breach, including whether or not Personal Data had been protected by appropriate technical

protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse. Breaches that are classified as unlikely to result in a risk to the rights and freedoms of natural persons do not require notification to the Competent Authority or the Data Subject. The DPO shall assess whether a breach is reportable to the Competent Authority or not.

## Data Breach reporting to Competent Authorities

If a Personal Data breach has resulted in unauthorised exchange, loss, alteration etc. of Personal Data where confidentiality is required, and the exceptions under “Classification of the Personal Data Breach” does not apply, the Competent Authority shall be informed immediately and without undue delay and not later than 72 hours after vACCSCA becomes aware that a Personal Data breach has occurred. This awareness is stated to apply after an initial time of investigation; a rule of thumb is that:

*“...a controller should be regarded as having become “aware” when the controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised. This will depend on the circumstances of the specific breach, whereas in others, it may take some time to establish if personal data have been compromised. However, the emphasis should be on prompt action to investigate an incident to determine whether personal data have indeed been breached, and if so, to take remedial action and notify if required.”*

As soon as an incident is detected, the DPO must be informed by the person detecting the breach, or alternatively by the respective Director if the person detecting the breach has reported it to their respective Director.

The report to the Competent Authority shall be prepared in accordance with local processes and submitted by the DPO or its delegates to the Competent Authority, acting on behalf of vACCSCA. If the DPO is in doubt, external guidance shall be sought to determine whether the requirements for notification pursuant to GDPR art. 33 and 34 are met or not. This assessment will vary from country to country based on the guidance and practice from local Competent Authorities. Where a notification to the Competent Authority cannot be achieved without undue delay,



the reasons for the delay shall accompany the notification and information may be provided in phases. Depending on the situation, the most convenient means of contact should be used. In the case of urgency, it might be advisable to contact the Competent Authority by phone. Please note that failure to report incidents to the Competent Authority may lead to fines and administrative sanctions for the organizations, thus it is important that all staff inform their respective Director and the DPO immediately upon becoming aware of a relevant incident. Failure to comply with this duty of notification may result in disciplinary actions for the staff in question.

### **Deviation reporting to Parent Organizations**

The DPO shall complete a report to VATEUD, VATEMEA or VATSIM BoG (as applicable) without undue delay and if possible within 12 hours after becoming aware of the incident. This report must include a description of the incident with all the information required to determine the impact.

When informing a parent organisation, the DPO will state if the breach complies with the necessary requirements in order to be notified to the local Competent Authority. In case there is no need to report the breach to the local Competent Authority, the notification to the parent organisation can be withheld if not already notified.

In any case, the DPO must report to the local Competent Authority before 72 hours after becoming aware of a Personal Data breach.

### **Cross-Border Processing**

If a Personal Data breach affects two or more countries, the DPO shall coordinate in terms of identifying the lead supervisory authority and reporting such data breach to the relevant supervisory authority as per GDPR Article 56.

## Information to the affected Data Subjects

The relevant Director (or whomever he delegates to) shall communicate the Personal Data breach to the Data Subject(s) affected by a Personal Data breach without undue delay, where that Personal Data breach is likely to result in a high risk to the rights and freedoms of the Data Subject(s), in order to allow them to take the necessary precautions. This mandatory information requirement is typically relevant when the incident may lead to the Data Subject potentially being exposed to discrimination, unequal treatment, ID-theft, fraud, loss of reputation or loss of life and health. As a rule of thumb, Data Subjects should be notified when practically possible and deemed suitable even when not strictly required by applicable law. Such notification necessitates that vACCSCA is able, with reasonable efforts, to determine the identity of the Data Subject for correct notification.

The communication shall describe the nature of the Personal Data breach as well as recommendations for the affected Data Subject(s) to mitigate potential adverse effects. The need to mitigate an immediate risk of damage would call for prompt communication with Data Subject(s), whereas the need to implement appropriate measures against continuing or similar Personal Data breaches may justify more time prior to information to the affected Data Subject(s). The communication to the Data Subject shall describe in clear and plain language the nature of the Personal Data breach and contain at least the following items:

1. a description of the nature of the breach;
2. the name and contact details of the DPO or other contact person;
3. a description of the likely consequences of the breach; and
4. a description of the measures taken or proposed to be taken by the Controller to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.

When contacting the Data Subject, consideration must be made to the method of contact. Whereas advantages of fast contact might be established, the possibilities and administrative workload must be considered. A best-effort approach where the following methods are to be used, should be considered:

1. Verbal notification (such as on Discord),
2. Instant Messaging (such as Discord DM),

3. E-mail,
4. Public Announcements (such as announcements on vACCSCA's website).

Verbal notifications might be used in cases where the volumes are considerably small (~10 people), however, it is not a preferred method as it may be difficult to evidence that the Data Subject has been informed. If verbal communication is used, it shall be noted a memo of this, and preferably also reiterated in an e-mail to the Data Subject. Emails are the preferred option as they allow for swift communication with the Data Subject in case time is of the essence. Public announcement is a valid source of communication when volumes are large and a vast majority of vACCSCA's members might be affected, or where it is difficult or impossible to conclusively determine the identity of the Data Subject. For general announcements to the public, notification will be performed either by the Director, the DPO or by the Event Department.

If there is uncertainty as to whether information to the affected Data Subject is required or not, the DPO should be consulted.

## Subsequent Evaluation and Documentation

The results of all Personal Data breach reporting shall be documented in writing. The comprehensiveness and scope of such written reports shall be adapted to the degree of seriousness of the breach in question. It is the responsibility of the DPO to ensure that the results are documented in writing.

Subsequent to material Personal Data breaches with a large impact and risk exposure potential, the relevant Director shall prepare (or ensure that the relevant Data Processor or subcontractor in question prepares) a report evaluating the root cause of the incident, the deviation handling process and the follow-up measures needed to avoid similar incidents occurring in the future. What is considered a large impact must be decided on a case-by-case basis, taking into consideration the nature of the breach, the impact on the affected Data Subject(s), the availability of mitigating measures and number of affected Data Subject(s). As a starting point, Personal Data breaches involving Special Categories of Personal Data (as per

GDPR art. 4) will as a general rule be considered to have a large impact. The DPO shall assist the relevant Directors with the above responsibilities.

### 3. Governance

This Personal Data Breach and Deviation Handling Routine shall be reviewed and updated once a year by the DPO. Next review should be conducted by 24th of March 2022.

## 4. APPENDIX A. Summary of Actions

**All vACCSCA staff:**

- Upon suspecting an incident, immediately contain it and report it to your department's Director and the DPO.

**All Directors of a vACCSCA Department:**

- Ensure that all subordinate staff and relevant members have read and adhere to this Routine.
- Upon identifying an incident, inform the affected Data Subject(s) without undue delay, pursuant to the *Information to the affected Data Subjects* section of this Routine.
- Upon identifying an incident, prepare a report, pursuant to the *Subsequent Evaluation and Documentation* section of this Routine.