# Data Handling Policy

[Portfolio: Division Director]

## Part 1—Preliminary

### 1 Objects

The objectives of this policy are to establish a framework within VATPAC for—

(a) achieving compliance with the **Data Protection and Handling Policy** of VATSIM;

(b) receiving and processing requests in relation to personal data;

(c) ensuring that this policy is implemented effectively.

### 1A Responsibility of the Board

The Board is collectively responsible for data protection, preventing loss of or unauthorised access to data and compliance with applicable laws.

### 2 Definitions

The following terms are defined as given—

| **Term** | **Definition** |
|---|---|
| Collected data | Defined in section 3 |
| Data breach | Defined in section 6 |
| Data request | Defined in section 4 |
| Data risk register | The register referred to in section 8 |
| Personal data | Has the meaning provided in the **General Data Protection Regulation** of the European Union |

| Term | Definition |
|---|---|
| Register of Collected Data | The register referred to in section 3 |

## 3 Collected Data

(1) **Collected data** is the personal data collected by VATPAC.

(2) The division director shall maintain and publish a **Register of Collected Data** which shall contain the types of personal data collected by VATPAC.

## 3A Collection of data

(1) VATPAC shall only collect personal data of the types listed in the Register of Collected Data.

(2) Collected data shall be linked to its subject by VATSIM CID as far as is practical.

# Part 2—Data Requests

## 4 Data requests

(1) A data request includes—

(a) right of access requests;

(b) right of rectification requests; and

(c) right of erasure requests.

(2) A person may make a data request in writing to it@vatpac.org.

(3) If a staff member receives, via an official means of communications, anything that could be construed as a data request, that staff member shall refer the data request to the Director IT.

(4) When VATSIM receives a data request under the Data Protection and Handling Policy (VATSIM), it may refer that request to VATPAC for processing.

(5) Requests received by VATPAC under subsections (2) to (4) shall be processed in accordance with this part.

(6) If a staff member receives from a person a verbal communication that could be a data request, the staff member shall advise that person to confirm the data request by submitting it in accordance with subsection (2).

VATPAC shall not take any further action until written confirmation is received.

## 4A Authentication

Prior to processing any data request, VATPAC shall verify the identity of the applicant as far as is practicable.

## 5 Processing right of access requests

(1) If a right of access request does not specify the scope of the request, then VATPAC shall provide to the applicant all of the collected data for the applicant.

(2) If a person making a right of access request does not specify the scope of the request or requests data that may be held by VATSIM or VATOCE, the request shall be referred to VATSIM and/or VATOCE as the situation dictates.

(3) In processing a right of access request, information shall not be released if the release of that information would—

(a) breach the privacy of another person;

(b) be illegal under the laws of any jurisdiction in Australia; or

(c) breach the General Data Protection Regulation (EU).

(4) A right of access request should not be refused only because of subsection (3) if the collected data could be released by removal of the information referred to in subsection (3).

## 5A Processing right of rectification requests

(1) If a right of rectification request is in relation to data that may be held by VATSIM or VATOCE, the request shall be referred to VATSIM and/or VATOCE as the situation dictates.

(2) Prior to processing a right of rectification request, VATPAC shall verify the supplied information as far as is practicable.

## 5B Processing right of erasure requests

(1) Unless a right of erasure request is clear that the only data collected by VATPAC is to be erased, the request shall be referred to VATSIM and VATOCE.

(2) In processing a right of erasure request, information shall not be erased if:

(a) erasure of that information would be illegal under the laws of any jurisdiction in Australia;

(b) the information may be required to establish, exercise or defend any legal claims;

(c) the information is required to prevent circumvention of a disciplinary process or sanction; or

(d) the information is required for operational or statistical purposes, in which case the information shall be anonymised.

# Part 3—Data Protection

## 6 Data breaches

(1) A **data breach** is an event in which loss or unauthorised access occurs to collected data held by VATPAC.

(2) In the event of an actual or suspected data breach, the Director IT shall—

(a) notify the Board within 24 hours of becoming aware of the data breach;

(b) present to the Board, within 14 days of becoming aware of the data breach, a data incident report including—

(i) the factual events;

(ii) the immediate actions taken to mitigate or stop the data breach;

(iii) the cause of the data breach as determined by an investigation by the Director IT; and

(iv) the actions taken to prevent a re-occurrence of the data breach.

(3) The Board may approve an extension of time to the presentation of a data incident report.

(4) In the event of a suspected or actual data breach, VATPAC shall, at the earliest opportunity and where practicable, notify affected persons of the data breach.

## 7 Access to Data

(1) Each portfolio director shall establish a system for controlling access to data collected by that portfolio and ensure that staff members are only granted a level of access appropriate to their duties.

(2) Each portfolio director shall ensure that before a staff member is granted access to data collected by that portfolio, that staff member receives training on and provides acknowledgement of their responsibilities under this policy.

## 8 Protection of Data

(1) The Director IT shall mitigate risks to collected data.

(2) The Director IT shall maintain a **Data Risk Register** which includes—

(a) the risks to collected data;

(b) the controls implemented to mitigate those risks.

(3) At each ordinary Board meeting, the Director IT shall table the Data Risk Register.

## 9 Reporting

The Director IT shall issue a report after each June including the following information for the period 1 July of the previous year to 30 June of that year:

(a) the numbers of: data requests received by VATPAC directly; data requests received via VATSIM; requests processed with no action required; requests processed with action; requests rejected; and requests referred to VATSIM; and

(b) a summary of actual and suspected data breaches.

# Revision History

| Date enacted | Change |
|---|---|
| 2 February 2019 | First issue |