



Data Privacy Vulnerabilities and Exposures (DPVE)

Preliminary Specification - DRAFT 0.1.0

Drafted by

Data Foundation Lab

DFLab FHO Pty Ltd – Proprietary Limited Company
(13 676 090 289)

Table of Contents

Abstract	3
1. Introduction.....	4
1.1 Background	4
1.2 Purpose.....	4
1.3 Intended Applications.....	4
2. Terminology and Scope	5
2.1 Privacy Occurrence	5
2.2 Data Privacy Vulnerability	5
2.3 Data Privacy Exposure	5
2.4 Primary Classification	6
2.5 Privacy Beyond Cybersecurity	6
2.6 Exclusions	6
3. Core Principles	7
3.1 Persistence.....	7
3.2 Evidence Before Allegations	7
3.3 Factual and Legal Neutrality.....	7
3.4 Reproducibility	7
3.5 Right of Response.....	7
3.6 Revision Without Erasure.....	7
3.7 Protection of Individuals.....	7
3.8 Interoperability	8
3.9 Remediation Recognition.....	8
4. DPVE Identification Model.....	8
4.1 Identifier Format	8
4.2 Unit of Identification	8
4.3 Occurrence Types	9
5. DPVE Records.....	9
5.1 Record Structure	9
5.2 Illustrative Record	10
6. Evidence and Verification	11
6.1 Evidence Requirements	11
6.2 Evidence Provenance	11
6.3 Sensitive Evidence	11
6.4 Verification and Record Status	12

7. Governance, Disclosure and Accountability.....	12
7.1 Initial Governance	12
7.2 Entity Notification and Response	13
7.3 Coordinated Disclosure	13
7.4 Disputes and Corrections	13
7.5 Independence	13
8. Interoperability and Public Registry.....	13
8.1 Relationship with Existing Frameworks	13
8.2 Data Privacy Weakness Enumeration	14
8.3 Public Registry	14
9. Experimental Development and Consultation	14
9.1 Experimental Validation.....	14
9.2 Matters Requiring Further Development	15
9.3 Development Outlook	15
10. Conclusion	15
Appendix A: Illustrative DPVE Record	17
A.1 Purpose	17
A.2 Example Scenario.....	17
A.3 Illustrative JSON Record	17
A.4 Interpretation	19
A.5 Limitations.....	19

Abstract

Data Privacy Vulnerabilities and Exposures (DPVE) is a proposed open standard for the persistent identification, classification, documentation and referencing of identifiable data privacy vulnerabilities and exposures.

DPVE seeks to establish a common identification mechanism through which privacy-relevant technical weaknesses, system designs, data processing practices, incidents and exposures can be independently referenced.

A DPVE identifier follows the proposed format:

DPVE-YYYY-NNNNNN

Example: DPVE-2026-000001

DPVE is intended to address a gap between existing cybersecurity vulnerability identification systems, privacy threat-modelling frameworks, breach registers, regulatory databases and privacy-risk assessment methodologies.

The proposed framework introduces:

1. Persistent identifiers for identifiable privacy occurrences.
2. Common classifications and structured records.
3. Evidence-based documentation and verification.
4. Mechanisms for recording remediation, disputes and entity responses.
5. Interoperability with existing privacy and cybersecurity frameworks.
6. A publicly accessible, machine-readable registry

DPVE does not determine legal liability, establish regulatory violations or replace existing privacy and cybersecurity standards.

This preliminary specification presents the foundational concepts of DPVE for public consultation. It is non-exhaustive and subject to revision.

1. Introduction

1.1 Background

Data privacy vulnerabilities and exposures are documented through various mechanisms, including academic research, regulatory investigations, data breach notifications, cybersecurity advisories and independent technical assessments.

However, these mechanisms do not generally provide a common identification system through which individual privacy occurrences can be persistently and independently referenced.

For example, cybersecurity vulnerabilities can be identified through Common Vulnerabilities and Exposures (CVE), allowing researchers, engineers and organisations to refer to the same vulnerability using a consistent identifier.

Comparable identification mechanisms are not widely established for privacy occurrences such as:

- Excessive personal information collection.
- Undisclosed third-party tracking.
- Inadequate or misleading consent mechanisms.
- Inappropriate secondary use of personal information.
- Excessive retention or inadequate deletion.
- Re-identification of individuals.
- Privacy-invasive system designs.
- Inappropriate disclosure or surveillance.

Such occurrences may arise independently of conventional cybersecurity vulnerabilities.

1.2 Purpose

DPVE proposes a common identification and documentation layer for these occurrences.

Its primary objective is to enable researchers, privacy engineers, organisations, regulators and other stakeholders to consistently reference a particular privacy occurrence without relying exclusively on individual reports, publications or regulatory proceedings.

For example: DPVE-2026-000001

The identifier would continue to reference the same occurrence regardless of subsequent investigation, remediation, dispute or changes to its associated record.

1.3 Intended Applications

DPVE is intended to support:

- Privacy research and academic publications.
- Privacy engineering and technical investigations.
- Privacy Impact Assessments (PIAs) and Data Protection Impact Assessments (DPIAs).
- Organisational privacy-risk management.
- Privacy vulnerability and exposure detection tools.

- Regulatory and compliance research.
- Cross-referencing between existing privacy and cybersecurity frameworks.

DPVE is intended to complement these activities rather than replace their existing methodologies or decision-making processes.

2. Terminology and Scope

2.1 Privacy Occurrence

A **privacy occurrence** is an identifiable event, condition, practice, weakness or system behaviour affecting one or more systems, services, datasets, processing activities or entities that has resulted in, or creates a substantiated risk of, adverse privacy consequences for individuals.

A privacy occurrence is the primary object represented by a DPVE record.

2.2 Data Privacy Vulnerability

A **data privacy vulnerability** is a technical, organisational, procedural, architectural or design condition capable of causing or materially contributing to adverse privacy consequences.

Examples include:

- Excessive collection by default.
- Inadequate data separation.
- Insufficient de-identification.
- Unnecessary identity linkage.
- Privacy-invasive default configurations.
- Inadequate deletion mechanisms.

A privacy vulnerability does not necessarily involve a conventional cybersecurity vulnerability.

2.3 Data Privacy Exposure

A **data privacy exposure** is an identifiable event, behaviour, processing activity or practice through which personal information or an individual's privacy interests are adversely affected or placed at material risk.

Examples include:

- Undisclosed third-party tracking.
- Inappropriate disclosure.
- Collection beyond a stated purpose.
- Persistent surveillance.
- Inappropriate secondary use.
- Re-identification.
- Excessive retention.

An exposure may result from an underlying privacy vulnerability. However, an exposure may also occur when a system operates exactly as designed.

2.4 Primary Classification

A DPVE record may represent one of three classifications:

Classification	Description
VULNERABILITY	An identifiable privacy-relevant weakness or condition.
EXPOSURE	An identifiable privacy-affecting event, practice or behaviour.
VULNERABILITY_AND_EXPOSURE	A documented privacy vulnerability accompanied by or resulting in a documented exposure.

These classifications distinguish underlying weaknesses from their resulting or accompanying privacy consequences.

2.5 Privacy Beyond Cybersecurity

DPVE recognises that privacy failures do not necessarily require:

- Unauthorised system access.
- Exploitation of a cybersecurity vulnerability.
- Compromise by a malicious actor.
- Accidental system behaviour.
- A regulatory enforcement action.
- A demonstrated violation of law.

For example, an application may intentionally transmit behavioural information to third parties without meaningful user awareness.

Although the transmission may be technically secure and the application may operate as intended, the processing practice may nevertheless constitute a privacy exposure.

2.6 Exclusions

DPVE identifiers should not ordinarily be assigned to:

- Purely hypothetical privacy risks without an identifiable implementation or practice.
- Unsupported allegations or speculative claims.
- General criticism of an organisation.
- Policy disagreements without a concrete privacy occurrence.
- Cybersecurity vulnerabilities without a material privacy dimension.
- Duplicate reports of an existing DPVE occurrence.

The proposed threshold for identification is **substantiated privacy relevance**, rather than the existence of disagreement concerning privacy.

3. Core Principles

DPVE is proposed around the following foundational principles.

3.1 Persistence

A DPVE identifier should permanently refer to the same underlying privacy occurrence.

Identifiers should not be reassigned, even when records are corrected, disputed, remediated or withdrawn.

3.2 Evidence Before Allegations

Published DPVE records must be supported by identifiable evidence. Unsupported claims should not be presented as verified privacy occurrences.

3.3 Factual and Legal Neutrality

DPVE records should distinguish between:

- Observed facts.
- Technical analysis.
- Registry assessments.
- Allegations.
- Entity statements.
- Regulatory determinations.
- Judicial findings.

Assignment of a DPVE identifier does not establish that an organisation or individual has violated any law.

3.4 Reproducibility

Where reasonably practicable and safe, supporting evidence should permit independent evaluation of the documented occurrence.

Reproducibility must be balanced against privacy, security and legal risks.

3.5 Right of Response

Organisations and other identifiable entities materially associated with a DPVE record should have a reasonable opportunity to provide corrections, contextual information, supporting evidence, remediation details or formal disputes.

3.6 Revision Without Erasure

DPVE records should preserve substantive revision histories. Corrections should not silently remove or rewrite historical information.

3.7 Protection of Individuals

DPVE must not unnecessarily publish personal information, compromised datasets or sensitive evidence.

The publication process should not create additional privacy or security harm.

3.8 Interoperability

DPVE should complement existing privacy and cybersecurity frameworks rather than unnecessarily duplicate their functions.

3.9 Remediation Recognition

DPVE is not intended to operate as an organisational blacklist.

Meaningful remediation should be recognised and recorded, while the historical occurrence remains independently referenceable.

4. DPVE Identification Model

4.1 Identifier Format

The proposed identifier format is:

DPVE-YYYY-NNNNNN

Component	Description
DPVE	Identifier namespace.
YYYY	Four-digit year of identifier assignment.
NNNNNN	Unique numerical sequence within the assignment year.

Example: DPVE-2026-000001

The identifier does not encode severity, jurisdiction, affected entity, classification, verification status or legal status.

These attributes may change without altering the identifier.

4.2 Unit of Identification

A DPVE identifier represents a **specific privacy occurrence**.

It does not identify an organisation, entire product, news article, regulatory investigation or legal contravention.

Multiple reports concerning substantially the same underlying occurrence should ordinarily reference the same identifier.

Separate identifiers may be appropriate where occurrences differ materially in their mechanism, affected system, processing activity, responsible entity, affected population, timeframe or underlying privacy condition.

Detailed rules for determining occurrence boundaries remain subject to further development and validation.

4.3 Occurrence Types

DPVE proposes a set of descriptive occurrence types, including:

Type	Example
Data breach	Unauthorised access, disclosure or loss of personal information.
Design weakness	A system design creating a material privacy vulnerability.
Collection	Excessive or insufficiently disclosed collection.
Use	Inappropriate or unexpected processing.
Disclosure	Inappropriate disclosure to another party.
Tracking	Tracking individuals or devices across contexts.
Linkage	Linking previously separated identities or datasets.
Inference	Deriving information about individuals from other information.
Retention	Retaining personal information beyond an appropriate period.
Consent failure	A consent mechanism failing to provide meaningful choice or understanding.
Surveillance	Monitoring that creates a material privacy exposure.
Re-identification	Associating de-identified information with identifiable individuals.

A single occurrence may have multiple applicable types. The complete taxonomy and classification boundaries remain open to refinement.

5. DPVE Records

5.1 Record Structure

Each published DPVE record is intended to provide a structured description of an identifiable privacy occurrence.

The proposed minimum record includes:

Field	Description
Identifier	Persistent DPVE identifier.
Title	Concise description of the occurrence.
Summary	Factual overview of the occurrence.
Classification	Vulnerability, exposure or both.
Occurrence type	Applicable privacy occurrence categories.
Verification status	Current evidentiary assessment.
Affected entities	Relevant organisations or entities, where identifiable.
Affected systems or services	Systems, services or processing activities involved.
Data categories	Types of personal information concerned.
Evidence	Supporting evidence descriptions and references.
References	Relevant publications, reports or external identifiers.
Timeline	Relevant occurrence and investigation events.
Publication and update dates	Record publication and revision information.

Additional information may include affected populations, privacy impacts, legal references, remediation, entity responses, disputes and related DPVE identifiers.

Where information cannot reasonably be determined, the record may explicitly indicate that it is unknown.

5.2 Illustrative Record

The following example is fictional and demonstrates the intended structure rather than an actual documented occurrence.

Identifier: DPVE-2026-000001

Title: Undisclosed behavioural tracking on Example Service

Classification: EXPOSURE

Occurrence types: TRACKING, DISCLOSURE

Affected entity: Example Pty Ltd

Affected service: Example Service

Affected information: Device, browsing and behavioural information

Evidence: Independent network traffic analysis

Verification status: VERIFIED

Remediation: Not specified

Summary

An independent technical investigation identified behavioural information being transmitted from Example Service to a third party without meaningful user awareness.

The occurrence was classified as a privacy exposure because the documented processing practice may adversely affect individuals' privacy interests, irrespective of whether the transmission resulted from a cybersecurity vulnerability.

This example is illustrative only. It does not represent an actual DPVE assignment or a finding of unlawful conduct.

6. Evidence and Verification

6.1 Evidence Requirements

DPVE is intended to operate as an evidence-based identification framework. A public record should identify the evidence supporting its publication.

Proposed evidence sources include:

- Regulatory determinations and official reports.
- Judicial records.
- Organisational disclosures.
- Reproducible technical investigations.
- Academic research.
- Independent privacy research.
- Authoritative public records.

Evidence should be distinguishable from interpretation, allegations and subsequent conclusions.

6.2 Evidence Provenance

Where practicable, evidence references should identify their source, author or authority, relevant dates, evidence type and access restrictions.

Technical evidence may additionally include persistent references or cryptographic hashes.

6.3 Sensitive Evidence

DPVE records should not publicly reproduce evidence where doing so would unnecessarily expose personal information, facilitate exploitation, endanger individuals, compromise confidential sources or materially increase security risks.

A record may instead reference evidence retained under restricted access or indicate that evidence has undergone independent review.

The appropriate mechanisms for evidence custody, controlled access and independent verification remain subjects for further consultation.

6.4 Verification and Record Status

The internal working specification proposes the following record statuses:

Status	Meaning
RESERVED	Identifier assigned but not publicly disclosed.
REPORTED	A credible report exists; verification remains incomplete.
CORROBORATED	Multiple independent sources support the occurrence.
VERIFIED	Available evidence satisfies applicable verification requirements.
DISPUTED	A material component is subject to a documented dispute.
REMEDIATED	Evidence indicates that the occurrence has been materially addressed.
SUPERSEDED	Record reorganised or incorporated into another record.
REJECTED	Reserved identifier determined to be ineligible.
WITHDRAWN	Publication withdrawn for a documented exceptional reason.

Verification, disputes and remediation may need to be represented independently rather than as mutually exclusive states.

The verification methodology, evidence thresholds and final status model require further technical development.

7. Governance, Disclosure and Accountability

7.1 Initial Governance

During the experimental stage, Data Foundation Lab proposes to coordinate initial DPVE identifier assignment and registry development.

The longer-term governance model may support distributed assignment through accredited DPVE Numbering Authorities (DNAs).

Potential numbering authorities could include universities, research institutions, privacy research organisations, regulators and other appropriately governed entities.

Any distributed model would require mechanisms to maintain globally unique identifiers, consistent assignment practices and independent oversight.

7.2 Entity Notification and Response

Where a verified DPVE record identifies a specific entity, reasonable efforts should ordinarily be made to notify that entity before publication.

Exceptions may be necessary where notification is impracticable, would increase risk or conflicts with justified coordinated disclosure procedures.

Affected entities should be able to submit factual corrections, contextual information, evidence, remediation details and disputes.

A substantiated occurrence should not be removed solely because publication is undesirable to the affected entity.

7.3 Coordinated Disclosure

Where publishing a record could expose an unremediated technical vulnerability or materially increase privacy risk, publication may be delayed to support investigation and remediation.

Protection of affected individuals should take precedence over publication speed.

7.4 Disputes and Corrections

Materially affected parties should be able to dispute factual accuracy, attribution, technical interpretation, classification, severity or other substantive record information.

Material unresolved disputes should be represented transparently. Corrections should preserve an auditable revision history.

7.5 Independence

DPVE is intended to support independent, evidence-based documentation of privacy occurrences without requiring the consent of the entity associated with an occurrence. Publication must nevertheless comply with applicable legal requirements and appropriate safeguards for sensitive information, responsible disclosure and affected individuals.

At the same time, the framework must maintain safeguards against unsupported allegations, inaccurate attribution and reputational misuse.

Detailed governance, appeals and oversight arrangements remain open for consultation.

8. Interoperability and Public Registry

8.1 Relationship with Existing Frameworks

DPVE is intended to complement established frameworks, including:

- Common Vulnerabilities and Exposures (CVE).
- Common Weakness Enumeration (CWE).
- LINDDUN.
- MITRE PANOPTIC.

- NIST Privacy Framework.
- Privacy Impact Assessments and Data Protection Impact Assessments.
- Regulatory and organisational incident-management systems.

Where appropriate, DPVE records may reference related cybersecurity vulnerabilities, privacy threat classifications, regulatory findings or privacy-risk assessments.

DPVE identifies the underlying privacy occurrence; these other frameworks may provide complementary information about weaknesses, threats, impacts, obligations or remediation.

8.2 Data Privacy Weakness Enumeration

The internal working specification also proposes a complementary **Data Privacy Weakness Enumeration (DPWE)**.

DPWE would describe recurring classes of privacy weakness, whereas DPVE would identify particular occurrences.

For example, a general weakness category concerning excessive data collection could be associated with multiple DPVE records documenting separate instances of that weakness.

The need for a distinct DPWE catalogue, and its relationship with existing taxonomies, requires further evaluation.

8.3 Public Registry

DPVE proposes a publicly accessible registry of identified privacy occurrences.

The registry is intended to be:

- Searchable and publicly accessible.
- Machine-readable.
- Version-controlled and historically auditable.
- Exportable and independently mirrorable.
- Accessible through documented interfaces.

A structured format such as JSON is proposed for canonical records. A formal JSON Schema, API specification and related implementation requirements are anticipated as future development work.

9. Experimental Development and Consultation

9.1 Experimental Validation

Before establishing a mature DPVE specification, the proposed model should be evaluated against documented privacy occurrences.

Potential test cases include:

- Notifiable data breaches.
- Regulatory privacy determinations.

- Cybersecurity vulnerabilities with privacy consequences.
- Third-party tracking.
- Consent failures.
- Excessive collection and retention.
- Re-identification.
- Privacy-invasive system design.
- Occurrences involving no cybersecurity breach.

Experimental validation should examine whether occurrences can be consistently identified, classified, evidenced and represented across different contexts and jurisdictions.

9.2 Matters Requiring Further Development

The following areas remain open for consultation and technical refinement:

1. How should distinct occurrences and duplicate reports be identified consistently?
2. Are the proposed vulnerability, exposure and occurrence-type classifications sufficiently clear?
3. What standards of evidence and independent review should be required?
4. How should verification, disputes, remediation and corrections be represented?
5. What assignment, oversight and appeals arrangements would support independence and credibility?
6. Should DPVE introduce a standardised privacy severity methodology?
7. How should DPVE integrate with existing technical, research and regulatory frameworks?
8. What minimum record schema and interfaces are necessary for practical adoption?

These questions are not intended to limit the scope of consultation.

9.3 Development Outlook

DFLab proposes an iterative development process informed by public consultation, technical review and experimental validation.

Subsequent versions may introduce revised terminology, classifications, evidence requirements, governance mechanisms and machine-readable specifications.

The objective is to establish a framework that is technically credible, independently reviewable and practically useful across privacy engineering, research and organisational environments.

10. Conclusion

DPVE proposes a common identification layer for data privacy vulnerabilities and exposures.

Its central proposition is that identifiable privacy occurrences should be independently referenceable, supported by evidence and capable of being connected to existing technical, research and regulatory information.

DPVE recognises that privacy failures cannot be represented solely as cybersecurity vulnerabilities. They may arise from technical weaknesses, organisational practices, system architecture or intentional processing activities, including circumstances in which a system operates exactly as designed.

The purpose of this preliminary specification is to present the proposed foundations of DPVE for scrutiny and further development.

DPVE remains an experimental proposal. Its definitions, technical requirements and governance arrangements are subject to consultation, validation and revision.

Appendix A: Illustrative DPVE Record

A.1 Purpose

This appendix provides a fictional example of a structured DPVE record to demonstrate how an identifiable privacy occurrence may be documented, classified and independently referenced.

The example illustrates the proposed relationship between a persistent identifier, privacy occurrence classification, affected systems, supporting evidence, verification status and associated information.

It is provided for consultation purposes only. The record structure and field names are preliminary and do not constitute a finalised DPVE JSON Schema.

A.2 Example Scenario

An independent privacy researcher examines the network activity of a fictional online service, **Example Service**, operated by **Example Pty Ltd**.

The investigation identifies the transmission of device identifiers, browsing activity and behavioural information to a third-party analytics provider.

The researcher determines that the processing activity is not adequately disclosed to users.

The occurrence is classified as a **data privacy exposure**, as the documented processing practice may adversely affect individuals' privacy interests despite the absence of a conventional cybersecurity vulnerability.

A.3 Illustrative JSON Record

```
1. {
2.   "identifier": "DPVE-2026-000001",
3.   "title": "Undisclosed behavioural tracking on Example Service",
4.   "summary": "Independent network traffic analysis identified the transmission of device
5.   identifiers, browsing activity and behavioural information from Example Service to a third-party
6.   analytics provider without meaningful user awareness.",
7.   "classification": "EXPOSURE",
8.   "occurrence_types": [
9.     "TRACKING",
10.    "DISCLOSURE"
11.  ],
12.  "verification_status": "VERIFIED",
13.  "affected_entities": [
14.    "Example Pty Ltd"
15.  ],
16.  "affected_systems_or_services": [
17.    "Example Service"
18.  ],
19.  "data_categories": [
20.    "DEVICE_INFORMATION",
21.    "BROWSING_INFORMATION",
22.    "BEHAVIOURAL_INFORMATION"
23.  ],
24.  "affected_population": {
25.    "confirmed": null,
26.    "potential": null,
27.    "status": "UNKNOWN"
28.  }
29. }
```

```

26.   },
27.   "jurisdictions": [
28.     "AU"
29.   ],
30.   "evidence": [
31.     {
32.       "type": "TECHNICAL",
33.       "strength": "PRIMARY",
34.       "description": "Independent network traffic analysis demonstrating behavioural
information transmitted to a third-party analytics endpoint.",
35.       "source": "Independent privacy researcher",
36.       "access": "RESTRICTED",
37.       "independently_reviewed": true
38.     },
39.     {
40.       "type": "ENTITY_DISCLOSURE",
41.       "strength": "CONTEXTUAL",
42.       "description": "Publicly available privacy notice reviewed against observed network
activity.",
43.       "source": "Example Pty Ltd",
44.       "access": "PUBLIC"
45.     }
46.   ],
47.   "references": [],
48.   "timeline": [
49.     {
50.       "date": "2026-09-01",
51.       "event": "Initial technical observation"
52.     },
53.     {
54.       "date": "2026-09-05",
55.       "event": "Independent evidence review completed"
56.     },
57.     {
58.       "date": "2026-09-08",
59.       "event": "Affected entity notified"
60.     },
61.     {
62.       "date": "2026-09-15",
63.       "event": "DPVE record published"
64.     }
65.   ],
66.   "remediation": {
67.     "status": "NOT_REPORTED",
68.     "description": null
69.   },
70.   "entity_response": {
71.     "status": "NO_RESPONSE_RECORDED",
72.     "description": null
73.   },
74.   "legal_references": [
75.     {
76.       "jurisdiction": "AU",
77.       "instrument": "Privacy Act 1988",
78.       "reference": "APP 1",
79.       "relationship": "POTENTIALLY_RELEVANT"
80.     },
81.     {
82.       "jurisdiction": "AU",
83.       "instrument": "Privacy Act 1988",
84.       "reference": "APP 5",
85.       "relationship": "POTENTIALLY_RELEVANT"
86.     }
87.   ],
88.   "related_dpve": [],
89.   "date_published": "2026-09-15",
90.   "date_updated": "2026-09-15"
91. }

```

A.4 Interpretation

This example demonstrates several proposed characteristics of DPVE.

1. The identifier DPVE-2026-000001 refers to the documented privacy occurrence rather than the organisation or service as a whole.
2. The occurrence is classified as an exposure because it concerns an identifiable data processing practice. No conventional cybersecurity vulnerability is required.
3. Technical observations provide the primary supporting evidence, while the service's privacy notice provides contextual information.
4. The underlying network captures are not reproduced in the public record. Their restricted status allows the record to describe the evidence without unnecessarily publishing potentially sensitive information.
5. The record indicates that the occurrence has been independently reviewed. The precise requirements for assigning a VERIFIED status remain subject to further specification.
6. References to Australian Privacy Principles indicate potentially relevant regulatory provisions. They do not establish that a legal contravention occurred.
7. The record can be updated to reflect subsequent remediation, organisational responses or disputes without changing its identifier.

A.5 Limitations

This example does not establish mandatory field names, permissible values, validation rules or API requirements.

The structure is illustrative and may change following public consultation, technical review and experimental validation.

The example is entirely fictional. Its identifier, entities, investigation, findings and timeline are provided solely to demonstrate the proposed DPVE record model.