



Data Privacy Vulnerabilities and Exposures (DPVE)

Public Consultation Paper

Drafted by

Data Foundation Lab

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

Table of Contents

<i>Introduction</i>	<i>2</i>
<i>What is DPVE?</i>	<i>3</i>
<i>How would DPVE Work?</i>	<i>4</i>
<i>Matters for Public Consultation</i>	<i>5</i>
<i>Consultation and Next Steps</i>	<i>6</i>

Introduction

Data privacy vulnerabilities and exposures are increasingly documented through academic research, regulatory investigations, organisational disclosures, cybersecurity reports and independent technical assessments.

However, unlike cybersecurity vulnerabilities, which can be consistently identified and referenced through systems such as Common Vulnerabilities and Exposures (CVE), there is no widely adopted equivalent for identifying individual data privacy vulnerabilities and exposures.

Privacy issues such as excessive personal information collection, undisclosed third-party tracking, inappropriate data sharing, inadequate consent and privacy-invasive system design are often documented independently, without a common mechanism for identifying and referencing the same underlying occurrence.

This fragmentation makes it difficult to correlate findings, conduct comparative research, track remediation and integrate privacy-related findings into existing technical and organisational workflows.

Data Foundation Lab (DFLab) proposes **Data Privacy Vulnerabilities and Exposures (DPVE)** as an open standard intended to address this gap, developed with input from privacy researcher **Dr Saad Masood** (Swinburne University of Technology).

This consultation seeks feedback from researchers, privacy professionals, engineers, organisations and other interested stakeholders on the proposed framework and its future development.

What is DPVE?

DPVE is a proposed open standard for identifying, classifying, documenting and referencing concrete data privacy vulnerabilities and exposures.

Its central concept is the assignment of a persistent identifier to an identifiable privacy occurrence.

For example:

DPVE-2026-000001

Each identifier would correspond to a structured record describing the privacy occurrence, including its nature, affected systems or processing activities, supporting evidence, potential impact and remediation status.

DPVE distinguishes between:

- **Privacy Vulnerability:** A technical, organisational or design weakness capable of causing adverse privacy consequences.
- **Privacy Exposure:** An event, behaviour or processing practice that adversely affects, or creates a substantiated risk to, an individual's privacy.
- **Vulnerability and Exposure:** An occurrence involving both an underlying weakness and an associated privacy exposure.

Importantly, a **privacy occurrence does not necessarily require a cybersecurity breach or technical malfunction**.

A system may operate exactly as designed while engaging in processing activities that create significant privacy risks.

DPVE is not intended to replace existing cybersecurity standards, privacy frameworks, regulatory processes or privacy impact assessments. Rather, it proposes a common identification layer through which privacy occurrences can be consistently referenced across these environments.

How would DPVE Work?

Under the proposed framework, privacy occurrences would be documented through standardised, evidence-based records maintained in a publicly accessible DPVE registry.

A typical DPVE record would identify:

- The privacy vulnerability or exposure.
- The affected system, service or processing activity.
- The categories of personal information involved.
- Supporting evidence and references.
- Verification and remediation status.
- Related privacy occurrences and applicable external classifications.

Records would be publicly accessible and machine-readable, enabling integration with research databases, privacy engineering tools, organisational risk assessments and other systems.

DPVE would distinguish between technical findings, allegations, organisational responses and official regulatory or judicial determinations.

The assignment of a DPVE identifier would not constitute a determination of legal wrongdoing.

The framework also proposes safeguards for sensitive evidence, independent verification, responsible disclosure and the right of affected organisations to respond or dispute findings.

During its experimental development, DFLab would initially coordinate identifier assignment, with potential future arrangements for independent or distributed numbering authorities.

Matters for Public Consultation

DPVE remains an experimental proposal. Its technical specification, governance arrangements and operational requirements are subject to further development.

DFLab particularly welcomes feedback on the following questions:

1. Need and Relevance

Is there a meaningful need for a common identification framework for data privacy vulnerabilities and exposures? Would DPVE address limitations in existing privacy and cybersecurity frameworks?

2. Scope and Classification

Are the proposed definitions of privacy vulnerabilities and exposures appropriate? What types of privacy occurrences should qualify for identification?

3. Evidence and Verification

What evidence and verification requirements would be necessary to establish credible and reproducible DPVE records, particularly where supporting evidence cannot be publicly disclosed?

4. Governance and Independence

How should DPVE be governed to maintain transparency, independence, accountability and long-term accessibility?

5. Practical Applications and Adoption

How could DPVE be used within privacy engineering, academic research, risk assessment, regulatory processes and existing cybersecurity systems? What barriers might prevent its adoption?

Respondents are welcome to address any or all of these questions, raise additional concerns or propose alternative approaches.

Consultation and Next Steps

DFLab is inviting public and professional feedback to evaluate the feasibility, relevance and proposed direction of DPVE.

Feedback received will inform subsequent revisions of the DPVE specification, experimental validation and consideration of future governance arrangements.

The DPVE Preliminary Specification v0.1.0 is available alongside this consultation paper as a supporting technical reference, providing further detail on the proposed framework, identification model, evidence requirements and governance arrangements.

Consultation period: Start: 26 October 2026 – End: To be announced

Submission details: via office@dfib.org

DFLab welcomes contributions from privacy and cybersecurity researchers, engineers, academics, organisations, regulators, civil-society groups and interested individuals.

The purpose of this consultation is to encourage open discussion and critical evaluation before progressing towards a more mature DPVE framework.

About Data Foundation Lab

Data Foundation Lab (DFLab) is an Australian for-humanity organisation dedicated to developing foundational data privacy technologies and strengthening and advancing data privacy through education, research, and advocacy to benefit and enrich humanity at large.

DPVE is an initiative proposed by **Data Foundation Lab (DFLab)**, developed with academic input and consultation from privacy researcher **Dr Saad Masood** (Swinburne University of Technology).

This paper is published for consultation purposes. DPVE remains an experimental proposal and does not constitute an established international standard or regulatory framework.