"Verinice is too complex for quick DPO workflows"
"It requires extensive customization for privacy tasks"
"Better suited for ISMS/security management"
"For DPO tasks, a dedicated privacy tool would be more efficient"

"I created 3 DPO documents: DPIA, Data Subject Request Form, and Privacy Policy"

1. DPIA (DOC-58) — Data Protection Impact Assessment

Purpose:

- Assess privacy risks before starting new data processing
- Required by GDPR for high-risk processing
- Document what data you collect, why, risks, and mitigations

When to use:

- Before launching a new product/service that processes personal data
- When using new technology (AI, biometrics, etc.)
- When processing sensitive data (health, financial, etc.)

Example: Before adding facial recognition to your app, create a DPIA to assess privacy risks.

---

2. DSRF (DOC-59) — Data Subject Request Form

Purpose:

- Handle requests from individuals about their personal data
- GDPR gives people rights (access, deletion, correction, etc.)
- This form helps process those requests

When to use:

- Someone asks: "What data do you have about me?"
- Someone asks: "Delete my data"
- Someone asks: "Correct my information"
- Someone asks: "Give me a copy of my data"

Example: A customer emails asking to see all data you have about them → use this form to track and process the request.

---

3. PRIV-POL (DOC-60) — Privacy Policy Template

Purpose:

- Template for your organization's privacy policy
- Explains to users what data you collect and how you use it
- Required by GDPR and many privacy laws

When to use:

- Creating/updating your website privacy policy
- Required for apps/websites that collect user data
- Must be shown to users before they use your service

Example: Your website collects emails → you need a privacy policy explaining this.

Item	Purpose	When to Use
DPIA	Assess privacy risks	Before new data processing
DSRF	Handle user data requests	When someone asks about their data
Privacy Policy	Tell users about data use	Required for any service collecting data
PERSONS	Track who does what	Document roles and responsibilities

"Verinice allows custom document creation but requires manual setup"
"The tool tracks PERSONS, DOCUMENTS, CONTROLS, and RISKS separately"
"You need to link them together to show compliance coverage"

I can build the **API connector** to send data to Verinice, but I cannot define the **Risk Models** or **Compliance Controls** inside Verinice. That is a legal/compliance task, not a developer task.

ISMS (Information Security Management System): The software category Verinice belongs to. It's a central database for tracking security risks and controls (like an ERP for security).
DPO (Data Protection Officer): The compliance manager who will likely be the primary user of this tool.
DPIA (Data Protection Impact Assessment): A specific legal workflow/report the DPO needs to generate to prove a process is safe.
PDPA (Personal Data Protection Act): The data privacy law in Singapore. Verinice needs to be adapted to fit this, as it is originally European (GDPR).
SMB: Small and Medium-sized Business (Verinice's target market, meaning it's lighter than SAP GRC).

- **SAP (Systems, Applications, and Products):** This is the ERP system itself. In your context, **SAP GRC** is a specific module within SAP for managing risk. Your boss might be using **Verinice** as a cheaper, external alternative to the expensive SAP GRC module to audit your SAP data.
- **GRC (Governance, Risk, and Compliance):** The software category Verinice belongs to.
    - **Governance:** Ensuring IT supports business goals.
    - **Risk:** Identifying threats (e.g., "Can a hacker access our ERP database?").
    - **Compliance:** Following laws. Your job as a developer is often to provide the technical *evidence* (logs, user lists) that feeds into this GRC system.
- **GDPR (General Data Protection Regulation):** The EU privacy law that effectively forces companies to use tools like Verinice. It is the reason your DPO is asking for "DPIAs" (Data Protection Impact Assessments) and "Article 35" reports. Even if you are in Singapore, if your ERP holds data on European customers, this law applies to your code.