2025-10-08

CERN IT DPIA process and workflow

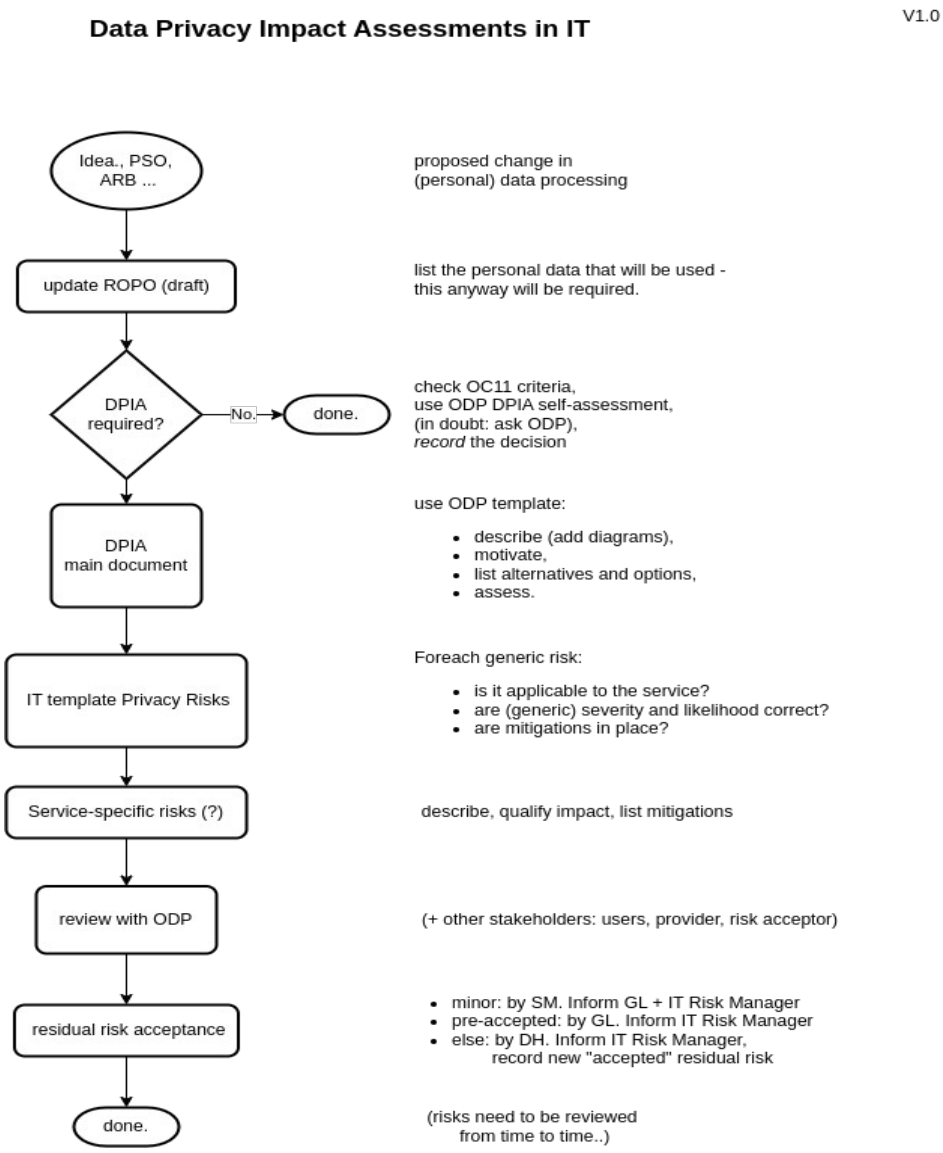
Background

With the increasing use of externally-provisioned cloud services as well as machine-learning/AI technologies, CERN IT department will have to perform frequent Data Privacy Impact Assessments (DPIA) - this document outlines the IT-internal processes.

It complements the CERN-wide DPIA procedure from the CERN Admin E-Guide, (where applicable) the "CERN IT Cloud Services Framework DPIA", and clarifies residual privacy risk acceptance in the IT department.

Ownership of the DPIA process for a given service is with the respective IT Service Owner (Group Leader). The Office of Data Privacy (ODP) defines the procedure to follow and reviews the result (and can provide guidance).

Diagram



Prepare

- Create (or update) the service's Record of Processing Operations (ROPO)
    - This (in tabular form) lists which personal data is concerned, for which purpose, who has access, how long it is kept. The DPIA does not replace this, but will refer to this data.
- Assess whether a DPIA is required
    - The ODP provides a questionnaire, in doubt: ask.
    - If no DPIA has to be done – document.
- Use the ODP-provided "complex case" Word template (from the above Admin E-Guide) for the textual assessment
    - This document will describe and explain the proposed processing, motivates it, discusses the alternatives considered and eventually balances the impact on user privacy with expected benefits for the organisation
    - Avoid duplication: refer to ROPO and Risk Register
- For the Risk Assessment: use the list of generic (template) IT-defined risks from this repository
    - evaluate whether each (generic) risk applies to your service
        - in particular, client-side encrypted application data makes ITA-16 not applicable and much reduces impact on ITA-18, ITA-19
        - if not, justify and move to next risk
    - evaluate whether the (generic) risk impact and likelihood are correct for your service - if not, correct (and justify)
    - evaluate whether all "mandatory" mitigations are met
        - For contractual obligations: go through contract, DPA documents, quote, record. Mark confidential passages as such.
        - Document any technical measures taken to reduce the risk
    - evaluate whether all "recommended" mitigations can be met, record, justify if not.
    - Add any service-specific mitigations that have been implemented
- add any service-specific risks (e.g raised by users)
    - Treat as above: describe, qualify initial risk score (using some example), discuss service-specific mitigations and expected outcome (reduced impact, reduced likelihood), qualify the resulting residual risk
    - If "generic": ask for them to be added to the IT template list.
- Open questions, apparently-unmet mitigations: ask external supplier for clarification (keep IPT and ODP in the loop).
- Consult external experts (user representatives, security team, privacy advocates, ODP, DPC)
- Decide on who is required to sign off on any eventual residual privacy risks, see below.

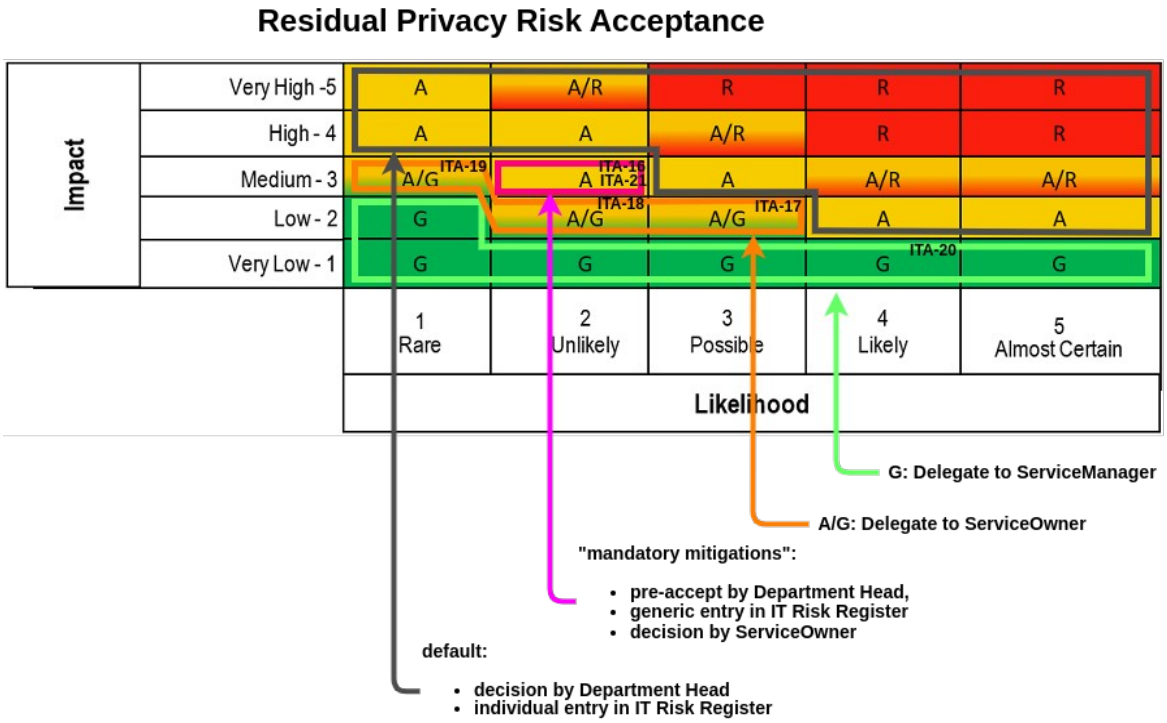
Review

- The DPIA procedure is concluded via a formal review between the service, IT risk acceptor(s) and ODP. ODP will advocate for minimum privacy impact solutions, challenge listed motivations, processing and risk scoring and the service is expected to justify each of these. ODP is expected to bring up any potential OC11 violation. Nevertheless, the final decision (also on residual risk acceptance) is with IT.
    - ODP records the outcome.

    - A non-confidential version of the DPIA is to be kept in a separate (IT) repository.
- Major (level “Amber” and above) new risks need to be accepted by the IT department head and will be added to the IT-wide risk register.
- Note: a DPIA will have to be periodically checked and updated in case of new risk factors emerging.

(Privacy) Risk Acceptance

IT will use the existing risk scoring criteria (Impact and Likelihood scores and “R/A/G” matrix) defined by CERN’s Office of Data Privacy (ODP), in conjunction with the “mandatory mitigations” from the templated “IT privacy risk register”:



With that,

- Service Managers (technical level) can chose to directly accept during a review all “Very Low” impact privacy risks, as well as “Rare” “Low” impact (“Green”), with a trace of the accepted risks being sent to both the IT Risk Manager and Group Leader.
- Service Owners (typically the respective IT Group Leader) can accept
    - “low” impact “unlikely” or “possible” risks, as well as medium-impact “rare” risks (“Amber/Green”)
    - higher-scoring risks that nevertheless satisfy the IT-defined “mandatory mitigations” from the corresponding (generic) risk template. These have been pre-agreed with the IT department head, and are tracked (as generic risks) in the IT risk register.
    - in both cases, a trace of the accepted risks has to be sent to the IT Risk Manager
- IT Department Head: decides on all other risks, with a corresponding specific entry in the IT risk register.

References:

- CERN Admin E-Guide "Data Privacy Impact Assessment"
- “R/A/G” matrix, Likelihood+Severity scores: all from ODP's **DPIA-risks.xlsm**, available via above CERN Admin E-Guide

- Generic (template) IT-defined risks: from the IT Privacy Risk Register Template
- CERN IT Cloud Services Framework DPIA