CERN IT CLOUD SERVICES FRAMEWORK DPIA

Project/Policy/Procedure Title:	CERN IT Cloud Services Framework DPIA
Controlling Service:	IT Department Head (IT-DH)
Service Owner:	E. Porcari
Date:	2024-09-24

Contents

1 Overview

This generic “Data Protection Impact Assessment” (DPIA) assesses privacy-related risks and suitable mitigation measures in order to protect personal data when planning and using Externally-Provisioned Cloud Services to support the Organization’s activities.

This DPIA

- adheres to the provisions for the protection of personal data listed in CERN’s Operational Circular N°11
- lists generic risks of processing and storage when using Externally-provisioned Cloud Services, and establishes IT-mandatory or recommended mitigation measures
- sets a framework for usage that is consistent with the Policy for the Cloud Usage at CERN, as well as the (draft) policies for Data Classification and Handling

This generic DPIA will be complemented by contract- and service-specific DPIAs.

1.1 Why is this DPIA needed?

The outsourcing of any part of the IT service portfolio to externally provisioned services for processing and storage of information poses a potential risk to data privacy and hence requires a DPIA. Individual IT services are bound by IT’s Policy for the Cloud Usage at CERN. This DPIA establishes ownership of the policy and resulting generic risks to privacy by the head of the IT Department.

1.2 Who is responsible for this DPIA?

This DPIA is carried out by the head of the IT Department (E. Porcari) as Controlling Service.

It will be maintained by the IT Departmental Data Privacy Protection Coordinator and approved by the head of IT department.

1.3 Format and Structure

The document structure below (Necessity/Proportionality Tests, “Step X”) follows the ODP guidelines for “Data Privacy Impact Assessments for Policy Making”.

1.4 Terms

The following terms have specific meanings when capitalised:

- Data Subject, Controlling Service, Processing Service, Sensitive Personal Data: used here per their definitions in OC11
- Externally-provisioned Cloud Service: a computing service where data processing and/or data storage happens outside of the CERN campus.
- External Provider: non-CERN entity (commercial or otherwise), itself not subject to OC11, which provides the Externally-provisioned Cloud Service to CERN, via a contract or memorandum of understanding

2 Necessity Test

2.1 Step 1: Factual description of the measure proposed

The IT Department has established a Policy for the Cloud Usage at CERN which applies when the IT Department outsources part of the IT service portfolio to an Externally-provisioned Cloud Service for processing and storage of personal and non-personal data for or on behalf of CERN.

The IT Department Policy for the Cloud Usage at CERN is to use Externally-provisioned Cloud Services where appropriate and cost effective. CERN IT will retain control and responsibility for the use of such an Externally-provisioned Cloud Service.

2.1.1 Description of the data processing involved

The usage of an Externally-provisioned Cloud Service involves the processing of personal data by an External Provider: on one hand information about the cloud users (e.g. to identify, authenticate and grant them access), on the other hand information contained in or linked to the content processed in the cloud (e.g. an Excel file with a list of names and expenditures; the file's metadata containing the name of its author). In the following, the extent of the processing of personal data through an Externally-provisioned Cloud Service is described in general terms.

2.1.1.1 CATEGORIES OF DATA AND PURPOSE OF THEIR PROCESSING

The following personal data would be processed:

- Account data, including roles, of users of the Externally-provisioned Cloud Services

Purpose: To grant and manage access of the user to the Externally-provisioned Cloud Service, and to implement access control within that service.

- Application data:
  - Content associated to an individual
  - Content containing personal data of specific individuals

Purpose: To provide the Externally-provisioned Cloud Service.

(It cannot be excluded a priori that this application data contains Sensitive Personal Data).

- Log data of users of Externally-provisioned Cloud Service

Purpose: To enable technical troubleshooting and support; to ensure security and enforce compliance with applicable rules and regulations; for fraud detection, prevention and follow-up; to establish, exercise or defend possible legal claims.

2.1.1.2 CATEGORIES OF DATA SUBJECTS

The persons concerned by the processing are primarily active members of the personnel of CERN, personnel of CERN's contractors and temporary labour workers. However, access to such Externally-provisioned Cloud Service may also be provided for former CERN members of personnel, associated users and/or the general public, i.e. all "people who interact with CERN" per OC11 §1.

2.1.1.3 Processing Operations

The personal data would be transferred between CERN's devices and infrastructure and those of the External Provider; the latter will store the data, provide back-up services and any other processing operations as agreed in the specific case.

These processing operations require the usage of the personal data on a regular basis. They will be retained for as long as they are necessary for their respective purposes.

The duration of the processing is linked to the specific contract CERN concludes with the External Provider.

2.1.1.4 Access to Personal Data

The personal data will be accessed by the External Provider to provide the agreed service, by the user concerned, and if necessary and agreed, by the relevant services of the IT Department.

2.1.1.5 Legal Base for the Processing

For the processing of personal data caused by the use of these Externally-provisioned Cloud Services, the IT Department would normally rely on the legitimate interest of the Organization to benefit from state-of-the-art IT services. This interest will have to be balanced against the privacy rights of the Data Subject.

Specific Externally-provisioned Cloud Services might have additional legal bases, and will refer to these in the service-specific DPIA:

- In case of "maintaining the Organization's archives, for scientific or historical research or for the preparation of statistics, always subject to the relevant internal legislation and policies;" the relevant rules (typically OC3) and policies will be identified.
- For "application of its internal legislation and compliance with its legal obligations", the relevant rules will be identified and explained.

2.2 Step 2: Define objectives of the measure

The objective of the Measure above is to provide IT services with one or more of the following characteristics (this list is not exhaustive):

- of a new type (that is not part of the existing IT portfolio) and/or,
- requiring a higher level of functionality,
- requiring a higher level of reliability,
- requiring a higher level of scalability,
- at lower cost,
- with a lower environmental impact

than what can be provided internally from within CERN-IT via on-premise services, through an External Provider. The service-specific DPIA (that will be done as part of each concrete proposal) will explain the concrete objective and link to CERN's mission.

2.3 Step 3: Identification of limitations to the rights of data subjects

By exposing the aforementioned Categories of personal data to an External Provider, data subjects could be impacted by a possible

- Loss of control over their data
- Missing transparency of the processing carried out by the external processor

Furthermore, data subjects could suffer more or less significant consequences due to a possible

- Usage of the data by the external processor for its own purposes that could violate the data subject's privacy, incl. transfer to third parties;
- Further collection of personal data by the External Provider, for example via tracing and tracking of the users' interactions with the Externally-provisioned Cloud Service, and their subsequent processing for own purposes;
- Lack of security of the data in the Cloud, leading to a data breach;
- Inadequate level of data protection due to the domestic law the external processor is subject to.

As neither profiling nor automated decision making are envisaged, a potential difference of future treatment of data subjects is rather unlikely.

However, the concrete limitation of freedoms and rights and their level of impact on the data subjects depend on the relevant Externally-provisioned Cloud Service concerned, and must be determined for each specific application separately. To aid in this, an "IT privacy risk register" (see below) will collect possible generic limitations on these rights (as well as specify agreed mitigation measures).

Nevertheless, the exercise of data subject rights (as defined in OC 11 VII) is guaranteed by CERN, even for data processed in an Externally-provisioned Cloud Service. Effective remedies, such as access to the Report and Complaint Mechanisms as set out in OC 11 IX will be available to all data subjects subject to the relevant conditions. It is up to each respective CERN Controlling Service to ensure that these rights can be still exercised on an Externally-provisioned Cloud Service.

2.4 Step 4: Choose option that is effective and least intrusive

The following generic options are available to deliver some unspecified IT service for CERN, in order of increasing exposure of personal data:

- Via standalone applications directly installed on the users' devices,
    - User interactions and data stay within the machine (unless deliberately exported from there)
- Through some service owned and operated by CERN, within the CERN network,
    - User interactions and data are visible to the CERN service managers, but only within CERN
- Cloud-based: through a service operated by CERN, but hosted on some External Provider's infrastructure resources outside of CERN ("Infrastructure as a Service"),

    - User interactions and application data technically must leave CERN, but can often be shielded from the infrastructure operator, e.g via encryption (on the network and on storage)

- Cloud-based: through a service operated by some commercial provider outside of CERN ("Software as a Service")
    - User interactions and application data by technical necessity become visible to the External Provider
    - Contractual agreements (including on technical measures) are the only means to ensure that this data will not be misused

A concrete proposal for any Cloud-based solution (i.e. the two latter options) will –in a separate DPIA - show why other privacy-preserving options are either inexistent, insufficient or ineffective in meeting the demand for that particular IT service.

Once the need for a Cloud-based solution has been established, for each contract of such an Externally-provisioned Cloud Service there will be further options that impact data privacy:

- The physical location of the service and applicable jurisdiction:
    - CERN member states have recognized CERN's privileges and immunities. In the case of legally mandated data transfers to state authorities, External Providers from these countries are expected to successfully challenge orders.
    - External Providers from countries that apply the EU GDPR or Swiss FRDP are expected to already comply with the corresponding OC11 obligations
- Contractual terms:
    - In particular, a contract under the General Conditions of CERN Contracts (chapter 15 "Data Protection") ensures CERN rules are contractually agreed to

It is recognized that these privacy-preserving options cannot always be successfully negotiated, in particular where CERN is a "small" customer. Nevertheless, the attempt and outcome will be documented.

3 Proportionality Test

3.1 Step 5: Assess the importance ('legitimacy') of the objective and whether and to what extent the proposed measure would meet this objective (effectiveness and efficiency)

The usage of Externally-provisioned Cloud Services will strongly contribute to the achievement of the IT mandate: these services create greater agility and flexibility and reduce or eliminate the need to maintain and support on-site hardware and software. The objectives listed in "Step 2" are hence legitimate.

In many IT application domains, Externally-provisioned Cloud Service have become the industry norm, and are the only way to deliver state-of-the-art functionality, including in areas that are critical for the functioning of CERN, such as e-mail communication and office software.

Alternative non-cloud solutions usually are only available on a very limited scale, for older or unsupported versions. Even currently-existing standalone solutions are rapidly becoming unsupported and no longer receiving updates, and hence cannot be continued due to the IT security risks they present. For cases where the functionality delivered is critical for CERN, cloud-based services will have to be provided.

Self-hosted services ("private Cloud" inside CERN) are in many cases not available (however, each concrete cloud proposal and DPIA will assess whether this is an option), or may have reduced functionality.

A concrete example is the Microsoft suite of productivity software, which since 2010 moved from the previous pure standalone desktop-based application first to a hybrid model (subscription-based with a locally-installed client accessing remote services), then to a browser-based Software-as-a-Service delivered by the Microsoft cloud. The original desktop-based productivity suite "Office 2021" will be unsupported as of 2026, and (as a major potential vector of computer malware) will then have to be removed. Alternatives to Microsoft's productivity tools do exist (both as standalone applications and hosted at CERN), but as the MALT project has shown in 2021, their reduced functionality was not sufficient for CERN.

Hence, we conclude that Externally-provisioned Cloud Services can in general be effective in meeting the Organization's computing needs. Depending on the actual licence terms and contract, their cost can typically be linked to actual dynamic usage (with reduced CERN-side fixed costs, compared to an in-house service), and hence these Externally-provisioned Cloud Services can also be efficient in delivering functionality.

3.2 Step 6: Assess the impact of the measure on the rights of data subjects

The actual impact of Externally-provisioned Cloud Services' processing on data subjects' rights depends on the actual service under consideration and will be documented in a service-specific DPIA. However, for the general case of processing work-related application data (and excluding Sensitive Personal Data), certain generic privacy-related risks for using Externally-provisioned Cloud Services have emerged. These have been collected in the "IT privacy risk register", together with an assessment of their respective impact on both the individual and on the Organization, for credible data misuse scenarios. These impacts have then been graded (based on likelihood of a misprocessing and severity of outcome).

For the case of high impact on the rights of data subjects, CERN IT has agreed on a set of mandatory mitigations for each risk that either reduce likelihood of a misprocessing, or the severity of the impact of a potential misprocessing. Typically, these mitigations consist in required contractual assurances from the External Provider.

3.3 Step 7: Proceed to the fair balance evaluation of the measure

The objectives of the Externally-provisioned Cloud Service processing are legitimate and can be both effective and efficient, with potentially significant benefits for CERN in terms of cost and functionality. Conversely, categorically rejecting any use of Externally-provisioned Cloud Services can have a significant negative impact on CERN's ability to deliver IT services.

Nevertheless, the risk of limitations to data subjects' rights are equally clearly present.

Whether benefits from using a particular Externally-provisioned Cloud Service outweigh the privacy impact will have to be evaluated in a dedicated DPIA for that service.

However, the risks and mitigations from the "IT privacy risk register" define an envelope in which CERN IT can make use of Externally-provisioned Cloud Services to deliver functionality, while maintaining adequate data privacy: while personal data will be exposed to the Externally-provisioned Cloud Service, contractual terms ensure it will not be misused by the External Provider. Exposure of Sensitive Personal Data is excluded and will be limited to cases where this data is provided by mistake. Even in those cases contractual confidentiality ensures it will not be exploited in a way that causes harm to the individual. Overall, these mitigation measures will ensure that impact of Externally-provisioned Cloud Service processing on data subjects' rights will be limited.

3.4 Step 8: analyse conclusions on the proportionality of the proposed measure. If the conclusion is 'not proportionate', identify and introduce safeguards which could make the measure proportionate.

The above analysis shows that while the objectives of using Externally-provisioned Cloud Services overall are legitimate, the risks to user privacy remain, and, in the general case, cannot simply be accepted. The proportionality of the "benefit" vs "privacy impact" also depends very much on the actual service under consideration, and hence, again in the general, cannot be decided on upfront.

As such, the IT department will use the OC11-mandated DPIA process to assess these risks for each concrete service, and as safeguard will impose mandatory mitigation measures on the IT services for the use of such Externally-provisioned Cloud Services. These safeguards will ensure that the overall proportionality between Externally-provisioned Cloud Services' benefits and impact on data subjects' rights is kept.

After a service-specific DPIA has been done in collaboration with the ODP, with processing within the boundaries set by the "IT privacy risk register", and when implementing the mandatory mitigations listed there, IT services can make use of Externally-provisioned Cloud Service without further approval by IT DH.

IT DH will in such cases nevertheless assume the residual privacy-related risks of such processing.

4 IT Privacy Risk Register

Established in collaboration with the ODP, the “CERN IT Services Privacy Risk Register” template, in a separate document, collects the identified generic privacy-related risks and their respective impact assessments. As part of a DPIA, each potential Externally-provisioned Cloud Services will systematically be assessed against these risks (beyond any other service-specific risks):

- Is the risk applicable?
- Are the (generic) severity and likelihood correct?
- Are the listed mitigations applied to the service?

The Risk Register specifies mandatory mitigations that will apply to all Externally-provisioned Cloud Services provided by the IT department. Any exception to these mitigation measures will have to be separately agreed to by IT DH (and discussed as part of a specific DPIA with ODP).

This register also clarifies which residual generic risks from Externally-provisioned Cloud Service processing (i.e. remaining risks after the mitigations have been applied) have been accepted by the IT DH, for services within the IT department portfolio.

References

OC11: Operational Circular N°11, https://cds.cern.ch/record/2651311/files/Circ_Op_Angl_No11_Rev0.pdf

ITCloudPolicy: Policy for the Cloud Usage at CERN, https://cds.cern.ch/record/2799153/files/CERN%20IT%20department%20strategy%202022-2025.pdf#page=14

DHP: CERN Data Handling Policy, https://security.web.cern.ch/rules/en/dhp.shtml

ODPPolicyDPIA: Data Privacy Impact Assessment for Policy Making, https://admin-eguide.web.cern.ch/en/content/data-privacy-impact-assessment-guidelines-policymaking

ITPRR: CERN IT Privacy Risk Register template, https://gitlab.cern.ch/it-privacy/dpia/it-template

GenConCERNcontract: General Conditions of CERN Contracts, https://procurement.web.cern.ch/document-category/key-reference-documents?page=0

Gartner: Cloud, AI and Software Are Top Investment Areas for Data & Analytics, 2021, https://www.gartner.com/en/articles/cloud-ai-and-software-are-top-investment-areas-for-data-analytics

McKinsey: Securing software as a service, 2019, https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/securing-software-as-a-service

MS365: Wikipedia:Microsoft365, https://en.wikipedia.org/wiki/Microsoft_365

MALT: Final MALT report (public), https://computing-blog.web.cern.ch/2022/01/three-year-malt-project-comes-to-a-close/#more-1039