Audit Requirement Guide

SURF Framework of Legal Standards for (Cloud) Services – Annex D

Utrecht, October 2016
Version number: 1.0

Credits

Audit Requirement Guide
SURF Framework of Legal Standards for (Cloud) Services – Annex D

SURF
P.O. Box 19035
NL-3501 DA Utrecht
T +31 88 787 30 00

info@surf.nl
www.surf.nl

SURF is the collaborative ICT organisation for higher education and research in the Netherlands.
This publication is available in digital format on the SURF website: www.surf.nl/publicaties

Table of Contents

1. Introduction

1.1. Background

In 2013, SURF published the SURF Framework of Legal Standards for (Cloud) Services (hereinafter referred to as "the Framework of Standards"). Best practice contract clauses on confidentiality, data property, availability and privacy are at the heart of the Framework of Standards.

The main focus is on privacy. The Framework of Standards sees the institution as the Controller of Personal Data Processing, even if a Processor (supplier) is used. This means that the institution must be able to demonstrate that it is and shall remain in control through adequate agreements and adequate compliance supervision.

The duty to report data breaches (in force since 1 January 2016), the ruling of the European Court regarding Safe Harbor (6 October 2015) and the recently adopted European Privacy regulation have led to an update of the privacy clauses. To make the Framework of Standards a more practical tool, it was decided to include the updated privacy clauses in a so-called Processor Agreement. Once the Legal Committee had adopted this Processor Agreement in January 2016, it was published on https://www.surf.nl/kennisbank/2013/surf-juridisch-normenkader-cloudservices.html. An updated version of the Processor Agreement was made available in October 2016. An English version is also available.

One important provision in the Processor Agreement concerns security and requires the Processor to have an audit performed. The Processor is requested to assign an independent IT auditor or expert to assess the Processor's organisation either periodically or on request to ensure the Processor meets the provisions on protection of confidentiality, integrity, availability and security of Personal Data and confidential data as described in the Service Agreement and Processor Agreement. The frequency of the assessment is once every two years, except in case of high-risk Data Processing, which requires annual assessments of the processor. The risk is always high when processing sensitive Personal Data as referred to in the Personal Data Protection Act. If only public Personal Data are processed, the risk is considered low and there is no obligation to perform a periodic investigation.

SURF-affiliated institutions use a variety of suppliers. There is great diversity among the suppliers. Their size, type and organisation history are all very different. Suppliers provide a wide range of services to affiliated institutions and the sensitivity of the processed data varies also.

This diversity means that a different application of the audit requirement is sometimes necessary. A one-size-fits-all solution is not always feasible, particularly at first.

1.2. Objective

The objective of this document is to offer a guide on how to approach the audit requirement in practice at the time when the institutions and suppliers are concluding the process agreements.

1.3. Reading guide

Chapter 2 describes the audit requirement in more detail. Chapter 3 then offers a guide for variations of this requirement and lists the relevant considerations and exclusions in this regard. If this leads to a different interpretation of the audit requirement, a number of options are described at the end of the chapter.

The annex outlines the relevant laws and regulations.

2. Audit requirement

The Framework of Standards considers the institution responsible for process control, even when a Processor (supplier) is used. This means that the institution must be able to demonstrate that it is and shall remain in control by means of adequate agreements and adequate compliance supervision.

The Framework of Standards provides security rules in terms of:
- suitable measures for logical and physical security;
- duty to report and provide information on security incidents (for example loss of data);
- duty to respond: secure and prevent further unauthorised actions;
- duty to cooperate: inform the authorities and data subjects;
- duty to provide information on the organisation processing the data and the security of Personal Data (when asked).

The Framework of Standards has converted the requirement for compliance supervision into an independent audit requirement. This independent investigation aims to establish that the supplier meets the agreement's provisions in terms of:
- Personal Data security;
- confidentiality, integrity, availability of the services provided by the supplier.

The Framework of Standards includes the following provision:

> ARTICLE 6. AUDIT
>
> 6.1 The Processor is obliged to assign an independent IT auditor or expert to assess the Processor's organisation either periodically or on request to ensure the Processor meets the provisions on protection of confidentiality, integrity, availability and security of Personal Data and confidential data as described in the Agreement and the Processor Agreement. The frequency of the assessment is once every two years, except in case of high-risk Data Processing, which requires annual assessments of the processor. The risk is always high when processing sensitive Personal Data as referred to in the Personal Data Protection Act. If only public Personal Data are processed, the risk is considered low and there is no obligation to perform a periodic investigation. Annex A describes the risks.

6.2 The Processor shall make available the findings of the IT auditor or expert to the Controller in a Third Party Memorandum upon request.

6.4 The Processor shall bear the costs of the periodic audit. The Controller shall bear the costs of a requested audit, unless the audit findings show that the Processor has not met the Processor Agreement provisions. In that case, the Processor shall bear the costs. This provision shall be without prejudice to any of the Controller's other rights, including its rights to compensation.

6.5 When it is established during an audit that the Processor does not meet the provisions of the Agreement and the Processor Agreement, the Processor shall take all steps that are reasonably required to ensure these are still met.

The audit requirement included in the Processor Agreement consists of the following elements:

1. The Processor shall instigate an investigation of the Processor's organisation to ensure the Processor meets the provisions on protection of confidentiality, integrity, availability and security of Personal Data and confidential data.

2. An independent ICT auditor or expert to be assigned by the supplier shall perform the investigation.

3. The supplier provides the investigation's results in a Third Party Memorandum (TPM). A TPM is a statement by an independent external expert who assesses the measures taken by a Processor.

4. The frequency of the investigation also depends on the risk classification. The risk classes refer to the sensitivity of processed Personal Data (see Framework of Standards, Chapter 4, Classification of Personal Data).

The following table outlines the risk classification of Personal Data and shows which TPM obligations apply.

Class	Personal Data	Frequency
Low (public level)	Public Personal Data (for example business e-mail address online).	No obligation
Medium	Non-public, but non-sensitive Personal Data (for example enrolment of a student).	At least twice a year
High	This includes Sensitive Personal Data, for example reports on psychological health or medical details as part of an examination.	At least once a year

An audit is always required, unless the Personal Data is public.

5. The Processor shall bear the costs of the periodic audit.

6. The institution can also submit a request for an additional audit. The institution shall bear the costs of the audit, unless the audit findings show that the Processor has not met the provisions of the Processor Agreement. In that case, the Processor shall bear the costs.

The above audit requirement is the starting point for negotiations with suppliers. If the specific circumstances require a deviation from the audit requirement, the following chapter offers guidance.

3. Guide for audit requirement variations

3.1. Introduction

This chapter describes when and under which conditions temporary deviations can be made from the standard audit requirement if a supplier is (currently) unable to meet the audit requirement.

3.2. Stage 1: Start an investigation into Personal Data Processing

The first step is to document the necessary information to determine the risk class, the operation of the service, the location of the data and the associated risks.

The possibility of a variation can be assessed based on a set of criteria. These criteria concern the supplier as well as the service to be provided. They allow a quality assessment.

There is no audit requirement if adequate end-to-end encryption is used to provide a service, provided that the supplier and/or Subprocessors do not have access to the Personal Data and the institution holds the keys. Due to the complexity and rapid developments in encryption technology, an investigation by subject-matter experts is advisable if the supplier indicates that there is end-to-end encryption.

3.2.1. Assessment criteria

An overview of the relevant assessment criteria is provided below. This also includes an exhaustive set of response categories for each criterion and a general explanation.

The following criteria can be distinguished for the supplier and the service:

1. **Subprocessors' level of commitment.**
   Explanation: the Subprocessors' level of commitment and the importance of the role the Subprocessors fulfil for the institution has a potential impact on the reliability level in terms of the protection of Personal Data.

   Many Subprocessors: more than two Subprocessors are used for the service.
   Few Subprocessors/important role: one or two Subprocessors are used for the service and at least one Subprocessor fulfils an important role in the processing of Personal Data (for example a significant portion or all of the Personal Data is temporarily or permanently stored at the Subprocessor's site or is transported across its network unencrypted).
   Few Subprocessors/subordinate role: one or two Subprocessors are used for the service and neither of them fulfils an important role in the processing of Personal Data.
   No Subprocessors: no Subprocessors are used for the service.

2. **The number of Data Subjects whose data is being processed.**
   Categories: high, medium, low.
   Explanation: the number of Data Subjects whose data is being processed has a potential impact on the level of risk involved in processing the Personal Data. **High:** the Personal Data of

at least 50,000 natural persons is expected to be processed within a reasonable term (one year) after the service is made available.

Medium: the Personal Data of at least 5,000 and at most 50,000 natural persons is expected to be processed within a reasonable term (one year) after the service is made available.

Low: the Personal Data of at most 5,000 natural persons is expected to be processed within a reasonable term (one year) after the service is made available.

3. **The quantity of processed data per Data Subject.**
   Categories: high, medium, low.
   Explanation: the quantity of processed data per Data Subject has a potential impact on the level of the risk involved in processing the Personal Data. The answer must be provided based on the maximum number of processed data a Data Subject could possibly have. The average quantity of processed data is not what matters here. Processed data must be classed as a data type. For example, the exam result data type is one data type, even though 20 exam results have been recorded.

   High: more than 25 different data types are expected to be processed for natural persons within a reasonable term (one year) after the service is made available.

   Medium: more than 10 but less than 25 different data types are expected to be processed for natural persons within a reasonable term (one year) after the service is made available.

   Low: less than 10 different data types are expected to be processed for natural persons within a reasonable term (one year) after the service is made available.

4. **Data sensitivity.**
   Categories: Sensitive Personal Data, non-sensitive Personal Data.
   Explanation: the sensitivity of processed data has a potential impact on the level of the risk involved in processing the Personal Data. This is about the processed data that is qualified as most sensitive, rather than average sensitivity.

The Personal Data Protection Act describes Sensitive Data as special Personal Data:

5. **Impact on the Data Subject.**
   Categories: high, medium, low.
   Explanation: the possible impact of Personal Data Processing on the Data Subject may affect the level of the risk involved in processing the Personal Data. This is about the maximum possible impact of Personal Data Processing, rather than the average impact.

   High: the possible impact of Personal Data Processing on the Data Subject can be qualified as high. This involves measures that have legal consequences for the Data Subject or a significant effect on the Data Subject's interests, rights or liberties,
   for example the Data Subject's acquisition of a diploma, loan or healthcare treatment.

   Medium: the possible impact of Personal Data Processing on the Data Subject can be qualified as medium. This involves measures that have no legal consequences for the Data Subject or do not significantly affect the Data Subject's interests, rights or liberties, but are important to the Data Subject all the same,
   for example the Data Subject's access to study materials.

   Low: the possible impact of Personal Data Processing on the Data Subject can be qualified as low.
   One example is the possibility to acquire software at low prices.

6. **Location of the Personal Data.**
   Categories: outside the EEA / with appropriate protection level, within the EEA, within NL.
   Explanation: the location of the Personal Data has a potential impact on the level of the risk

involved in processing the Personal Data. If the location is dynamic, i.e. if the exact location cannot be determined, the first possible category must be chosen. The same principle applies if the location of the Personal Data changes depending on the type of Personal Data.

Outside the EEA / with appropriate protection level: the location of the Personal Data is outside the European Economic Area (EU member states and Norway, Liechtenstein and Iceland) in a country that is on the list of countries with an appropriate level of protection (see link).
The Safe Harbor agreements with the US are no longer applicable. A new framework is being prepared as a replacement: the EU-US Privacy Shield.
For the time being, US service providers processing Personal Data need to sign the EU standard clauses.
Within the EEA: the location of the Personal Data is within the European Economic Area (EU member states and Norway, Liechtenstein and Iceland).
Within NL: the location of the Personal Data is in the Netherlands.

If desired, additional criteria can be used such as the supplier's track record, innovative service, etc.

3.2.2. Stage: Establish knockouts

The first substage in an assessment is to establish whether there are any so-called "knockouts" when audit requirement variation is never desirable. The following overview lists the knockouts.

Criterion	Knockout
Data sensitivity	Sensitive Personal Data
Impact on the Data Subject	High

If one knockout applies, deviation from the audit requirement is not desirable.

3.2.3. Stage: Assessment based on the criteria

If no knockout applies, the next step is a quality valuation based on the mentioned criteria. It is important to assess the criteria according to the situation. The variation can be considered further based on the quality assessment.

3.3. Stage 2: Possible variation of audit requirement

An outline of the variation options for the audit requirement is provided below.

1. A temporary deferred requirement, including compensatory measures. It is recommended to use a term of 6 and certainly no more than 12 months and to include this in the Processor Agreement. An institution-approved description of the security set-up can be a compensatory measure.

2. Another party performing the investigation (instead of the external ICT auditor on behalf of the supplier):

   - an external ICT auditor or expert from or on behalf of the institution;
   - one or more institutions on behalf of the supplier;
   - one or more institutions on behalf of one or several other institutions (peer audit);
   - self-assessment by an institution based on SURF audit.

3. Another Framework of Standards for the investigation:

- specifically named frameworks of standards (such as Healthcare Service Provider and SURFaudit);
- specifically named Best Practice provisions;

4. Investigation of the set-up and existence of the measures under consideration, rather than their operation.

It is important to specifically support the suggested variation of the audit requirement and to ensure it is accompanied by the compensatory measures to be taken.

4. Annex providing an overview of the relevant laws and regulations

Several laws and regulations set standards for processing Personal Data in the cloud. These are mainly:

- the Personal Data Protection Act;
- Personal Data Security Guidelines, Personal Data Protection Board;
- View on the implementation of the Personal Data Protection Act for an agreement for cloud computing services from a US supplier, Personal Data Protection Board; and
  Opinion 05/2012 on Cloud Computing, Article 29 Data Protection Working Party;
- the General Data Protection Regulation.

These sources are discussed below insofar as they are relevant for the guidelines.

Personal Data Protection Act

The Dutch Personal Data Protection Act is an important source of standards for supplier outsourcing, particularly Articles 12, 13 and 14. The supplier acts under the authority of the institution and processes Personal Data only at the institution's request (Article 12, paragraph 1 of the Personal Data Protection Act). The parties processing Personal Data under the supplier's responsibility shall maintain confidentiality (Article 12, paragraph 2 of the Personal Data Protection Act). The institution is responsible for ensuring a suitable security level for the Personal Data to be processed (Article 13 of the Personal Data Protection Act). This obligation means that the institution makes sure that the supplier meets the institution's obligations and that the requirements are met (Article 14, paragraphs 1 and 3 of the Personal Data Protection Act). The supplier's Personal Data Processing is governed by an agreement (Article 14, paragraph 2 of the Personal Data Protection Act).

Personal Data security guidelines

The Personal Data Protection Board prepared some guidelines on Personal Data security. The Personal Data Protection Board has used the guidelines to offer additional requirements and instructions for security measures to be taken in terms of Personal Data protection. The Personal Data Protection Board indicates when a risk analysis of the Processor's processing activities is required, for example. To list these risks, we must consider the guarantees the Processor put in place for technical and organisational measures (as referred to in Article 13 of the Personal Data Protection Act). It shall also be established to what extent the institution (the Controller) is capable of supervising compliance with the measures. The most common threats and vulnerabilities must always be included in this risk analysis. They can be identified by considering issues such as Personal Data security, the level of security transparency the (Sub)processor aims to achieve and the type of action taken in case of any incidents. The Processor's ability to continue the service in the event of an incident shall also be considered. If the agreement is to be dissolved or terminated, it must be established to what extent the data can be moved to another IT provider (data portability). All this information shall be included in a Processor

Agreement. The Controller shall perform regular checks to ensure the Processor complies with the existing arrangements. The process to handle security incidents and data breaches shall also be assessed.

View on cloud computing with a US supplier and Opinion 05/2012 on Cloud Computing

The Personal Data Protection Board provided a formal view on the implementation of the Personal Data Protection Act in an agreement on cloud computing services provided by a US supplier in 2012 at the request of SURFmarket. The Personal Data Protection Board's view emphasises the Controller's specific responsibility to perform a risk analysis and its obligation to ensure compliance with the law and the agreement. The view is relevant to the audit requirement as included in the Framework of Standards for the implementation of standards for TPMs as a possibility to fulfil that responsibility.

The view focuses on standards ISAE 3402 and SSAE 16. These TPM standards are based on the Processor's description of the measures that are relevant to the TPM target group. One aspect is whether technical security measures for cloud processing and measures for Subprocessors are adequately covered, or dealt with in separate supplementary reports. This ultimately determines whether the TPM and its supplementary reports are considered to cover the specific situation. The external expert reviews different aspects of how the measures are described, such as completeness. The external expert then establishes whether the Processor has actually implemented the described measures. Depending on the type of TPM, the external expert makes a statement on the presence of the described measures on a certain date (type 1) or during a certain period (type 2).

The Article 29 Working Party, which is the independent advisory and consultative body of European privacy regulators, issued an opinion on cloud computing and privacy protection on a European level in 2012. The issues discussed in this opinion that are relevant to the audit requirement are in line with the Personal Data Protection Board's view. The Personal Data Protection Board's view also refers to the opinion several times.
The opinion specifically indicates that the Controller must ensure that:

- they are capable of showing that the information security principles mentioned by the opinion have actually been implemented (accountability);
- the Processor always cooperates in order to comply with the Controller's right to monitor the Data Processing (right to audit);
- this monitoring is performed by the Controller or a reputable third party;
- this monitoring is based on a recognised, relevant audit standard.

General Data Protection Regulation

The General Data Protection Regulation (hereinafter referred to as "GDPR") is a European legal data protection act offering standards for outsourcing to a supplier ("Processor"). Only the standards that deviate (significantly) from the Personal Data Protection Act are mentioned below.
NB: The GDPR officially came into force on 25 May 2016. After this date, member states have two years to transpose the regulation in their legislation. On 25 May 2018, the regulation shall actually be applied to replace the current Personal Data Protection Act.

In a general sense, the Processor is directly co-responsible for putting in place technical and organisational measures and procedures to ensure the Data Processing meets the regulation's conditions. This includes the application of the principles of privacy by design (Articles 24 and 25 of the GDPR). The Processor is also directly responsible for putting in place the appropriate technical and organisational measures to guarantee the appropriate security level (Article 32 of the GDPR).

The GDPR obliges the Controller to perform a privacy impact assessment (PIA) in a number of situations (Article 35 of the GDPR). This assessment investigates the risks involved in the Data Processing and the changes to be made to cover these risks.

Like the processing Controller, the Processor shall cooperate with the supervisory authority in the performance of its tasks (Article 31 of the GDPR). The Processor shall make available to the processing Controller all information necessary to demonstrate compliance with the obligations and shall allow on-site inspections (Article 28, paragraph 2(h) of the GDPR).

The Processor shall assist the Controller to ensure compliance with the obligations pursuant to Articles 32 to 36 of the GDPR (Article 28, paragraph 2(f) of the GDPR). These obligations include the security of the Data Processing, the reporting of any security breaches to the supervisory authority and to the Data Subjects, risk detection, the implementation of privacy impact assessments (PIAs) and previous consultation of the supervisory authority.
The Processor's obligations mentioned above must be reflected in the agreement between the institution(s) and the supplier and must ensure that the Processor's relevant management measures are included in the scope of the independent investigation (Article 28 of the GDPR).