SURF Framework of Legal Standards for (Cloud) Services

Utrecht, October 2016
Version number: Version 2.0, 2016

Credits

SURF Framework of Legal Standards for (Cloud) Services

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

info@surf.nl
www.surf.nl

October 2016

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. History 4
2. Subjects of the Legal Standards Framework 5
3. Legal Committee 11
4. Practical Tools and Other Guidelines 13

1. History

The former SURF ICT and Business Platform Management established the SURF Framework of Legal Standards for (Cloud) Services in April 2014. The Framework is an industry tool to include adequate guarantees for the consumption of cloud services with regard to the handling of Personal Data, the confidentiality of information, service availability and data ownership. The Framework's main focus is on the provisions regarding the handling of Personal Data. These provisions offer privacy guarantees to the User based on national and European legislation.

Framework Update

The Framework for privacy provisions has been updated in connection with developments in international flows of Personal Data (Safe Harbor declared invalid by the European Court of Justice) and the obligation to report data breaches that is coming into force.

It was decided to include the updated privacy provisions in a so-called processing agreement. The institution is legally obliged to conclude such a processing agreement when Services are purchased for which Personal Data is processed on behalf of the institution. The SURF Model Agreement is a practical tool in this regard. The Model Processing Agreement is determined by the Legal Committee (see Chapter 3) with the support of law firm Project Moore.

The Model Processing Agreement and the other Framework provisions apply to all Services on behalf of the institution where privacy, availability, confidentiality and property are relevant. The document therefore refers to the 'supplier'.

The set-up of the Legal Framework has also changed. This document explains what the Framework entails and how it came about. It also includes the provisions on confidentiality, intellectual property and availability. It has several annexes, such as the abovementioned processing agreement and suggestions on issues such as security and audits for the proper implementation of the Framework.

2. Subjects of the Legal Framework

The Framework offers educational institutions a solid basis for contracts with suppliers. Suppliers of ICT Services for education, research and institution management keep (corporate) client data in their ICT infrastructure for storage and processing. This requires guarantees with regard to the **control, confidentiality, availability and privacy** of this data.

Particularly in the case of Personal Data, (national and European) laws and regulations state that the management of an institution is responsible for respecting the privacy of the persons, even if the data is processed by a third party, such as the supplier.

Control of data and confidentiality also require guarantees to ensure the institutions' interests. The clauses in the Framework offer these guarantees.

The above four subjects are specified further and standard provisions have been worded for each subject. This is followed by an explanation of how to interpret and use these provisions.

NB: The standard provisions in these documents mention certain capitalised concepts. These concepts must be defined in the Agreement. The following definitions can be used:

Definitions to be used:

Service: *the supplier's Service to be provided under the Agreement.*

User: *a (natural) person in any way associated with the institution, such as a member of staff, a teacher and/or a student, authorised by the institution for (a certain part of) the Service.*

Data: *all details, data, information and other materials or content entered, sent, posted or processed in any other way by the institution and/or Users as part of the Agreement using the Service, including Personal Data.*

Agreement: *this Agreement for Services based on which the supplier processes Data on behalf of the institution.*

Personal Data: *all information regarding an identified or identifiable natural person that is or will be processed by the supplier in any way as part of the Agreement.*

1. Property rights and control

Provision to be used:

(INTELLECTUAL) PROPERTY RIGHTS AND CONTROL

1. All (intellectual) property rights – including any copyright and database rights – on the Data (file or files) shall always remain with the institution, the User in question or their respective licenser(s).

2. The supplier does not have independent control of the Data it processes. The Data is controlled by the institution and/or the User in question.

Explanation	
Which parts?	- Intellectual property - Control of Data
Why is this important?	To ensure that control of Data is not transferred to the supplier
Where is this arranged?	Master Agreement
Explanation	Intellectual property: The intellectual property rights to the Data (specifically all Data and not just Personal Data) never transfers to the supplier, but remains in the hands of the institution, User or the licensers of the User or institution. This provision stipulates that the supplier must respect the intellectual property rights. Control: By giving the User and/or institution control over the Data (explicitly all Data and not just Personal Data), it is explicitly determined that the Data can only be processed when requested by the User/institution.
In practice	The intellectual property of Data, such as student projects, belongs to the student and/or institution. This can never be transferred to the supplier. The processed Data remains under the control of the institution and/or User. In Dutch law, the terms property and ownership apply to physical items. As cloud Services do not involve any physical items, terms other than ownership are used to convey the same meaning: (intellectual) property rights and control.

2. Availability

Provision to be used:

DATA AVAILABILITY

1. The supplier shall be responsible for the availability of the Service to the institution according to the provisions of this Agreement <and the Service Level Agreement (SLA), which forms part of the Agreement>.

2. The supplier shall provide adequate back-up and restore facilities to guarantee the availability of the Service (including the static and dynamic Data).

Explanation	
Which parts?	- Availability - Back-up and restore facilities
Why is this important?	To ensure that there is agreement on the Service availability and to guarantee adequate back-up.
Where is this arranged?	Master Agreement and the Service Level Agreement (SLA)
Explanation	Availability: In this provision, the supplier explicitly agrees with the Agreement's provisions. If the institution finds that the Service does not meet the provisions, this article offers an extra opportunity (besides non-compliance with the provision) to address the supplier in a legal sense. Back-up and restore facilities: The supplier shall keep the Data or a copy of the Data in case the Service fails (for whatever reason). The supplier shall also ensure it can use a recent back-up to start up (restore) the Service again after it failed. This ensures the Data remains available to the institution.
In practice	If the supplier fails to comply with the provisions, a formal notice can be prepared with references to this and any other provisions. The text in between brackets < > in paragraph 1 can be omitted if there is no SLA.

3. **Confidentiality**

Provision to be used:

ARTICLE ON CONFIDENTIALITY

1. The parties shall keep secret all Data which they know or reasonably suspect is confidential and which they have become aware of or received as part of the execution of this Agreement. The parties shall not share this Data with any third parties or disclose it internally or externally in any way, except:

a) when it is necessary to announce and/or provide the Data as part of the execution of this Agreement;
b) when any mandatory legal statutory or court ruling forces the parties to announce and/or provide the Data or information, in which case the parties shall inform the other party first;
c) when the Data is announced and/or provided with the other party's prior permission in writing; or
d) when the information was already lawfully considered public not caused by one of the parties' actions or failure to act.

2. The parties shall be charged a €25,000 penalty for every violation of their confidentiality obligation, payable immediately and without prejudice to the other party's other compensation entitlements.

3. The parties shall contractually oblige the people working for them (including employees) involved in the processing of confidential Data to keep said confidential Data secret.

4. One party shall cooperate when the other party requests supervision of the use and storage of confidential Data by or on behalf of the other party.

5. The parties shall make available all the Data they have as part of the execution of the Agreement, including any copies at the other party's request.

6. Each party shall inform the other party immediately as soon as it has detected (i) a possible or actual violation of confidentiality; (ii) loss of confidential Data; or (iii) a violation of security measures. The party in breach shall take all the necessary measures at its own expense to secure the confidential Data, resolve any shortcomings in the security measures to prevent any further access, changes and disclosure, without any prejudice to the noting party's right to damages or other measures. The party in breach shall help to inform the people involved at the request of the other party.

Explanation	
Which parts?	- Confidentiality - Breach of confidentiality - Secrecy - Confidentiality supervision
Why is this important?	To arrange that certain (Personal) Data is treated confidentially, cannot be distributed internally or externally and employees have a duty of confidentiality.
Where is this arranged?	In the Master Agreement and, if necessary, in the Processing Agreement.
Explanation	1. Pursuant to this article, data declared confidential by the institution or User is treated as such. The confidentiality of data means that the supplier must keep this data secret without any internal or external distribution/disclosure. Personal data can be distinguished from confidential data (although Personal Data can also be confidential data). The Dutch Personal Data Protection Act must be respected in terms of Personal Data. Ad a. Confidential data may have to be disclosed or provided in order to execute the Service and/or Agreement. The disclosure and distribution of confidential data are permitted only when this is the case. Ad b. The confidentiality of data must not prevent the supplier to meet the mandatory laws and regulations. Again, the disclosure and provision of the confidential data are permitted only to allow the supplier to meet the mandatory laws and regulations. Ad c. Confidential data can only be disclosed/provided with the written consent of the person responsible. Again, the disclosure and distribution are only permitted in accordance with the written consent and shall not go beyond the specifics of the consent. Ad d. Confidentiality no longer applies if the confidential data are already public (because of the institution's actions or failure to act). 2. A violation of secrecy shall result in an immediately payable penalty, as violations of secrecy cannot be reversed. The level of the penalty takes into account the Dutch General Government Terms and Conditions for IT Contracts, but it does not follow them completely. It was decided to apply a lower amount – €25,000 – for each violation. 3. In order to comply with this article, a confidentiality agreement must be signed by both the supplier and the people working for the supplier. This is to further effectuate the duty of confidentiality and establish liability in terms of violation of the duty of confidentiality. 4. To ensure the supplier's proper execution of the duty of confidentiality, the supplier shall cooperate with the institution if it wishes to supervise this. Under this provision, the supplier shall cooperate in supervision on compliance with this duty of confidentiality. 5. The institution can request (confidential) data. This includes any copies of the data, so that confidential data is no longer processed by the supplier. This

	allows the institution to control and manage the processing of the (confidential) data. 6. The supplier has a duty to provide information on security incidents involving confidential data immediately. This involves both suspected and actual incidents to guarantee the duty of confidentiality as much as possible. The incidents include unauthorised access, loss and security breaches. Besides this duty to provide information, the supplier must respond adequately to any incidents by securing the confidential data, taking measures to stop and/or prevent the incident and cooperating to further handle the incident.
In practice	1. The institution or User can indicate specifically that data is confidential. From then on, the data is subject to the provisions of this article. If confidentiality is not specifically indicated, but the supplier can reasonably suspect that the data is confidential, the data must also be treated as confidential. In practice, it is recommended to specifically indicate the data's confidentiality to avoid any discussion. In that case, the institution and/or User are responsible for judging the data's confidentiality. If the data can reasonably be assumed to be confidential, this is ultimately at the discretion of the judge. The supplier's duty of confidentiality ensures that it shall not distribute the confidential data any further than necessary for the execution of the Service. This data shall not be disclosed or distributed further internally or externally. 2. If the supplier violates the duty of confidentiality, the charged penalty shall be payable immediately. A violation of the duty of confidentiality can often not be reversed and causes immediate damage. 3. The confidentiality agreement must be verified before the Service starts. This can be done by requesting the relevant contractual obligation from the supplier. 4. The institution can supervise compliance with the duty of confidentiality, for example by requesting the confidentiality agreement with the supplier's staff or by checking the procedures to execute the duty of confidentiality.

4. Privacy

The Dutch Data Protection Act holds the institution responsible for guaranteeing the privacy of the persons whose data is being processed. If a supplier is processing data on behalf of an institution, the Dutch Data Protection Act states that arrangements must be made in writing between the party responsible for the Personal Data (the institution in this case) and the processor (the supplier) to guarantee the Personal Data is handled in the best possible way and to agree on what a processor can and cannot do with the Personal Data.

It is important that the institution classifies Personal Data according to the risk level. In accordance with the guidelines of the Personal Data Authority, which supervises the execution of the Dutch Data Protection Act, the Framework's requirements of the supplier increase accordingly in

line with the level of the detected risk. The levels of the Framework go from Low (public Personal Data) to Normal/Medium (Personal Data that are not public or sensitive) and High (in any case sensitive Personal Data). The provisions ensure the institution that legal responsibility has been taken and can be justified towards the regulator. The rights of the persons involved are also guaranteed. The provisions also ensure that the supplier continues to meet the rights and obligations in terms of the institution's responsibility when using subcontractors. This also applies when the supplier or subcontractors are outside the European Economic Area (EEA).

Provisions on privacy and the protection of personal data are included in a Processing Agreement. The Processing Agreement can be concluded as an individual agreement in addition to the Master Agreement, or as an annex to the Master Agreement arranging the Service. A Model Processing Agreement forms part of the Framework.

The Model Processing Agreement has the following subjects:

- Processing on behalf of the customer and according to instructions;
- Using subcontractors;
- Security;
- Duty to report data breaches;
- Audit obligation;
- International movement;
- Handling search requests;
- Informing the parties involved;
- Indemnification;
- Regulator measures;
- Changes to the processing of Personal Data;
- Duration and termination;
- Governing law and dispute resolution;
- Specification of Personal Data and security measures.

The Model Processing Agreement is enclosed with the Framework as Annex A.

A separate annex to the Framework includes an explanation of every provision of the Processing Agreement and an instruction to complete Annex A of the Model Processing Agreement (specification of Personal Data and security measures).

3. Legal Committee

When the Framework was determined, it was decided to establish a Legal Committee with lawyers representing the institutions. The Legal Committee also includes security experts from the security community (previously called SURFibo, now SCIPR).

The Legal Committee monitors the content elements of the Framework and follows relevant developments in the applicable national and international laws and regulations in that regard. The Legal Committee also plays a part in the Framework's practical execution when SURFmarket concludes agreements for the SURF target group. The Legal Committee discusses any substantiated departures from the Framework.

The tasks and procedures of the Legal Committee are as follows:

- The further development of the Framework. This may include modifications and improvements, but also further development of the Standard Framework's subjects and guidelines for practical implementation.
- Discussion of the substantiated departures from the standards when SURFmarket enters into agreements.
- The creation of an annual overview to be shared with the SURF executive board.

Committee Composition

The Legal Committee consists of lawyers, personal data officers, privacy officers or security experts at the institution representing the target group. The aim is to have a representative of each of the following target group segments on the Legal Committee: universities, colleges, colleges of higher education, university medical centres, secondary vocational education (MBO) institutions and the research industry. New members shall be appointed according to an appointment procedure.

The Legal Committee elects one of its members as its chairperson. SURF provides the secretary. SURFmarket is represented by the head of contract management. SURF lawyers shall be involved in the Framework and the SURF Corporate Privacy Officer shall also be part of the Committee.

4. Practical Tools and Other Guidelines

The Legal Framework contains a number of annexes to help with using and applying the Framework.

Annex A: SURF Model Processing Agreement
Annex B: Instructions with the Model Processing Agreement
Annex C: Guidelines for Security Measures
Annex D: Guidelines for Supplier Audit Obligations

The Framework continues to evolve. The objective is to further complete the Framework with guidelines and practical tools for the practical implementation of the Framework. This version of the Framework paid a lot of attention to privacy, but other subjects – such as availability and confidentiality – are also on the agenda for further development.