SURF Framework of Legal Standards for Cloud Services

Utrecht, September 2018
Version number: version 3.0, September 2018

Framework of Legal Standards for Cloud Services

SURF
Postbus 19035
NL-3501 DA Utrecht
T +31 88 787 30 00

info@surf.nl
www.surf.nl

September 2018

SURF is the collaborative ICT organisation for Dutch tertiary education and research institutions.
This publication can be inspected online on SURF's website: www.surf.nl/publicaties

Contents

1. Historical background

SURF's Framework of Legal Standards for Cloud Services was adopted by the then SURF ICT and Management Platform Board in April 2014. The Framework provides the sector with tips that will help its members guarantee an appropriate level of security with regard to the use of personal data, data confidentiality, reliable data availability, and the rights to the data when using cloud services. The most important aspect of the Framework is the provisions governing the use of personal data. These provisions safeguard the user's privacy and are based on both Dutch national legislation and EU law.

Framework update

Due to the latest developments with regard to the international transfer of personal data (the European Court of Justice recently declared the Safe Harbor agreement invalid) and the entry into effect of the data breach notification obligation, SURF has updated the privacy provisions of the Framework.[1]

We have opted to include the updated privacy provisions in a so-called data processing agreement. When a tertiary education or research institution hires a company to provide services that include the processing of personal data at the institution's request, said institution is required by law to have the company sign a data processing agreement. SURF's model data processing agreement may serve as a useful tool in this regard. The model data processing agreement was adopted by the Legal Affairs Committee (see Chapter 3) and drawn up with the support of the Project Moore law firm.

The model data processing agreement and the other provisions of the Framework apply to all services provided at the institution's request which involve privacy, reliable data availability, confidentiality, and rights. Therefore, the document refers to a 'service provider'.

The layout of the Framework of Legal Standards has been revised, as well. This memo provides an explanation of what the Framework entails and how it was drawn up. It also presents the provisions governing confidentiality, intellectual property and data availability. In addition, the memo has several appendices, such as the aforementioned data processing agreement, as well as useful information with regard to security and audits, which will help educational and research institutions apply the provisions of the Framework effectively.

[1] The privacy-related provisions of the Framework were updated in June 2018 due to the entry into force of the General Data Protection Regulation on 25 May 2018 and the implementation by the European Commission of the EU-US Privacy Shield, which has replaced the Safe Harbor agreement.

2. Subjects discussed in the Framework

The Framework provides educational institutions with a solid basis for the contracts to be signed with service providers. When an institution hires an ICT service provider to provide services related to its teaching, research and management duties, personal and organisational data is integrated within the service provider's ICT infrastructure for storage and processing purposes. This requires security measures that safeguard **control over this data**, as well as the **confidentiality, reliable availability and privacy** of this data.

In the particular case of personal data, laws and regulations stipulate that an educational institution's board of governors is liable for ensuring that data subjects' privacy be respected, even if the data is processed by a third party, such as a service provider.

The institutions' boards of governors must also request control of the data and guarantee its confidentiality so as to ensure that the institutions' interests are properly served. The provisions of the Framework safeguard compliance with these requirements.

The Framework includes separate sections for each of the four aforementioned subjects, and standard provisions have been drafted for each subject. It also contains explanations on how to interpret and implement these provisions.

Please note: several words are capitalised in the standard provisions outlined in this memo. Definitions of these words must be included in the agreement. You may wish to consider using the definitions provided below:

Definitions to be used:

Agreement: *the present Agreement, which concerns the provision of Services, and on the basis of which the service provider processes Data on behalf of the institution.*

Data*: any and all data, information and other materials or content (expressly including Personal Data) entered, uploaded, sent, posted or otherwise processed by the institution and/or Users by using the Service as part of the Agreement.*

Personal Data: *every piece of information relating to an identified or identifiable natural person processed in any way whatsoever, now or in the future, by the service provider as part of the Agreement.*

Service: *the service to be provided by the service provider under the terms of the Agreement.*

User: *any natural person affiliated with the institution in any capacity (e.g. support staff, academic staff and/or students) who is authorised to access the Service provided, or parts thereof.*

1. Property rights and control

Provision to be used:

(INTELLECTUAL) PROPERTY RIGHTS AND CONTROL

1. Ownership of and title to the property rights and intellectual property rights – expressly including copyright and database right – pertaining to the Data and the file(s) containing it are and shall remain at all times with the institution, the User concerned or their respective licensor(s).

2. The service provider is not authorised to make any decisions regarding the Data it processes at its own discretion. The institution and/or the User concerned retain(s) the rights to the Data.

Explanation	
What does it cover?	- Intellectual property - Control of the data
Why include it?	To ensure that control of the data is not transferred to the service provider
To be included where?	In the main agreement
Explanation	Intellectual property: The intellectual property rights (which explicitly cover all data, not just personal data) will never be transferred to the service provider, but will remain with the institution, the user or the user's/institution's licensor. This provision is included to ensure that the service provider respects intellectual property rights. Control of data: By stipulating that control of the data (which explicitly covers all data, not just personal data) remains with the user and/or the institution, the institution puts into writing that the data must only be processed if and insofar as the user/institution authorises the service provider to do so.
In actual practice	The intellectual property rights to the data, e.g. students' essays, will remain with the students and/or the institution. They will never be transferred to the service provider. The institution and/or user will remain in charge of the data to be processed. In Dutch law, the terms 'property' and 'ownership' are associated with tangible objects. Since cloud services are not tangible objects, we have chosen not to use the term 'ownership', but rather phrases that jointly express the same idea with regard to data: intellectual property rights and control.

2. Data availability

Provision to be used:

RELIABLE DATA AVAILABILITY

1. The service provider is responsible for ensuring that the services to be provided under the terms of this Agreement <and of the Service Level Agreement (SLA) that is part of this Agreement> are reliably available.

2. The service provider will ensure that proper data back-up and data restore features are in place so as to ensure the constant reliable availability of the Service (and thus the static and dynamic Data).

Explanation	
What does it cover?	- Reliable data availability - Data back-up and data restore features
Why include it?	To ensure that both parties are in agreement with regard to the reliable availability of the service to be provided, and to ensure that the data is backed up properly.
To be included where?	In the main agreement and in the Service Level Agreement (SLA)
Explanation	Reliable data availability: By signing this agreement, the service provider explicitly agrees to the terms of the agreement. If the educational institution finds that the services provided do not meet the requirements laid down in the agreement, this article will give the institution an additional ground (on top of the provision whose obligations were not fulfilled) to hold the service provider legally liable. Data back-up and data restore features: The service provider is required to store the data or a copy of the data in case of a service interruption, howsoever caused. In addition, the service provider is required to make regular backups so as to be able to restore its service following a service interruption. In so doing, the service provider will ensure that the data will remain available to the educational institution.
In actual practice	Educational institutions may refer to this provision (among others) in a notice of failure to perform in the event that the service provider fails to adhere to its obligations under the agreement. The text included between angle brackets < > in sub-section 1 can be removed if no SLA is in place.

3. **Confidentiality**

Provision to be used:

CONFIDENTIALITY CLAUSE

1. The parties will protect the confidentiality of all Data whose confidential nature is known to them or can reasonably be inferred and which is disclosed to them or placed at their disposal for the performance of their obligations arising from the Agreement, and will not disclose said Data to any internal or external parties in any way, nor place it at any third party's disposal, except in cases where:

a) disclosing of the Data in question and/or placing it at another party's disposal is necessary for the performance of this Agreement;
b) the parties are required by a mandatory statutory provision or by a court ruling to disclose the Data or information and/or place it at another party's disposal, in which case the parties must first notify the other party;
c) the other party has given prior written permission to disclose the Data and/or place it at another party's disposal; or
d) the information concerns data which has already been lawfully disclosed in a manner not including negligence or carelessness on either party's part.

2. Every time a party violates its obligation of confidentiality, it will owe the other party an immediately due and payable fine of EUR 25,000 per violation, without prejudice to the other party's other rights to compensation.

3. The parties will contractually obligate all persons who carry out duties on their behalf (including their employees) and who are involved in the processing of confidential Data to respect the confidentiality of said Data.

4. The parties will be cooperative every time the other party or its representative requests permission to inspect the manner in which the confidential Data is stored and used.

5. The parties will place all Data for which they are responsible for the purpose of performing the Agreement, including any copies they may have made, at the other party's disposal at the first request to do so.

6. Either party will notify the other party without delay if it has learned that (i) its duty of confidentiality has or may have been violated; (ii) confidential Data has or may have been lost; or (iii) its security measures have or may have been compromised. The negligent party will, at its own expense, implement any measures necessary to safeguard the confidentiality of the Data and remedy the shortcomings in its security measures so as to prevent further access, alteration or disclosure, without any prejudice to the affected party's right to compensation or other sanctions. At the affected party's request, the negligent party will help notify the data subjects involved.

Explanation	
What does it cover?	- Data confidentiality - Violations of the obligation of confidentiality - Non-disclosure - Monitoring of compliance with the obligation of confidentiality
Why include it?	To ensure that certain data or personal data is treated confidentially and is not disclosed to internal or external parties, and to ensure that employees are sworn to secrecy.
To be included where?	In the main agreement and possibly in the data processing agreement.
Explanation	1. When this clause is included, data that is designated as confidential by the educational institution or the user must be held in strict confidence. Due to the confidentiality of the data, the service provider is obligated to protect the confidentiality of this data and to refrain from disseminating or disclosing it to internal or external parties. Personal data and confidential data are not necessarily the same, but at the same time, personal data may constitute confidential data. If the data concerned is personal data, its processing must comply with the provisions of the General Data Protection Regulation (GDPR). Re: a. In certain cases, the disclosure or provision of the confidential data may be necessary for the provision of the service and/or the performance of the agreement. If and insofar as this is the case, the disclosure and/or provision of confidential data is allowed. Re: b. Data confidentiality must not prevent the service provider from complying with applicable laws and regulations. Again, the disclosure and/or provision of confidential data is allowed if it helps the service provider comply with applicable laws and regulations. Re: c. The disclosure or provision of confidential data is subject to the controller's written consent. Here, too, confidential data must only be disclosed or provided in the manner outlined in the written consent, and only for the purposes outlined in the written consent. Re: d. If the confidential data has already been disclosed (through the educational institution's own negligence or carelessness), the duty of confidentiality no longer applies. 2. Since violations of the obligation of confidentiality are irreversible, they are punishable by an immediately due and payable fine. In determining the amount of the fine, we took into consideration the ARBIT Terms and Conditions, but we chose not to follow its recommendations in this regard. Instead we decided to apply a smaller fine, amounting to €25,000 for each violation. 3. The service provider as well as the persons carrying out their duties on its behalf must sign a confidentiality agreement in order to fulfil the obligations imposed under this article. They must do so to give themselves a greater incentive to observe their duty of confidentiality and to record who is liable in the event of a violation of the duty of confidentiality.

	4. To ensure proper compliance with the duty of confidentiality by the service provider, the service provider is obligated to provide full cooperation in any attempt made by the educational institution to monitor its level of compliance. Pursuant to this provision, the service provider is required to cooperate in any attempt to monitor its adherence to the obligation of confidentiality. 5. The educational institution is entitled to make a request to inspect data (including confidential data, and also including any copies which may have been made of the data, so as to ensure that confidential data is no longer processed by the service provider). This enables educational institutions to check and control the processing of their (possibly confidential) data. 6. The service provider is subject to an obligation to notify the educational institution at once in the event of a security breach involving confidential data. The service provider must notify the educational institution without delay in the event of either a proven or suspected incident, thus allowing data confidentiality to be safeguarded to the maximum extent possible. 'Incidents' here refers to unauthorised data access and security breaches resulting in the unlawful loss, destruction or alteration of data. In addition to the obligation to report data breaches, the service provider has the obligation to respond to incidents by ensuring that the confidential data is secure, implementing measures designed to terminate and/or prevent the incident, and fully cooperating with incident follow-up activities.
In actual practice	1. If the educational institution or data user has explicitly stated that the data to be processed is confidential, said data is subject to the provisions of this clause. If the educational institution or data user has not explicitly designated the data as confidential but the service provider can be reasonably expected to infer that the data is confidential, the data must also be treated confidentially. In actual practice, we explicitly recommend designating confidential data as such, so as to prevent unnecessary discussions. In such cases, the decision on the data's level of confidentiality must be made by the educational institution and/or data user itself. In cases where data can be reasonably deemed to be confidential, the final judgement will be up to the court. For the service provider, the duty of confidentiality means that confidential data must only be shared with others to the extent necessary for the provision of the service. Confidential data must not be disclosed to any internal or external parties, nor disseminated to others. 2. If the service provider violates the obligation of confidentiality, an immediately due and payable fine should be imposed. Violations of the obligation of confidentiality are typically irreversible and often result in immediate damage. 3. The confidentiality agreement must be checked prior to the commencement of the service to be provided. You can do so by requesting the service provider to submit the relevant contractual obligation. 4. The educational institution is entitled to monitor the service provider's compliance with the confidentiality agreement – for instance, by requesting permission to inspect the non-disclosure agreements signed by the service provider's employees, or the service provider's procedures with regard to ensuring compliance with the obligation of confidentiality.

4. Privacy

Pursuant to the GDPR, both the educational institution and the service provider are responsible for ensuring the privacy of the persons whose data is being processed (i.e. the data subjects). If a service provider processes data on behalf of an educational institution, the GDPR stipulates that the arrangements made between the controller (in this case, the educational institution) and the data processor (i.e. the service provider) must be confirmed in writing, so as to ensure proper processing of the personal data and to help the data processor understand what it is and is not allowed to do with the personal data.

It is vital, in this process, that the educational institution classify the level of risk associated with the data. In accordance with the guidelines issued by the Dutch Data Protection Authority (the Dutch supervisory authority tasked with monitoring compliance with the GDPR), the Framework imposes demands on service providers that get more stringent as the level of risk increases. These provisions allow educational institutions to feel safe in the knowledge that they have done everything they are required to do by law and that they can demonstrate as much to the supervisory authority, while at the same time safeguarding the data subjects' rights. In addition, the provisions ensure that the service provider will continue to fulfil its obligations (thus helping the educational institution fulfil its own obligations) even in the event that it hires a sub-contractor. This is also true if the service provider or sub-contractor is located outside the European Economic Area (EEA).

Provisions pertaining to privacy and the protection of personal data are incorporated into a data processing agreement. Data processing agreements can be concluded as separate agreements, to be signed in addition to the main agreement, or alternatively, they can be appended to the main agreement that outlines the services to be provided. The Framework includes a model data processing agreement.

The Model Data Processing Agreement contains the following subjects:

- The processing of data at the controller's request, and in accordance with the controller's instructions;
- Confidentiality;
- Access to personal data;
- The use of sub-contractors or sub-processors;
- Security precautions;
- The obligation to report data breaches;
- The obligation to undergo auditing;
- Transfer of data to third countries
- How to deal with requests for investigations;
- The data processor's duty to be cooperative and lend assistance as and when necessary;
- How to deal with data subjects' requests;
- Liability and indemnity;
- Changes to the way in which personal data is processed;
- The duration and termination of the data processing operation;
- Applicable law and dispute resolution;
- Specific information on the type of processing operation to be carried out, including the nature of the personal data to be processed and the security precautions to be taken.

The Model Data Processing Agreement is appended to the Framework as Appendix A.

The Framework also comes with a separate appendix presenting additional information on each clause of the data processing agreement and instructions on how to fill out Appendix A to the Model Data Processing Agreement (specific information on the nature of the personal data and the security precautions to be taken).

3. Legal Affairs Committee

When the Framework was adopted, SURF decided to establish a Legal Affairs Committee. This Committee focuses on the further development of the Framework and discusses the application of the Framework to real-life situations.

The Committee is made up of 5 to 10 members, who are appointed for a two-year period. The Committee chooses a chairperson from its midst. A SURF representative acts as the secretary. Whenever the Committee convenes, a legal expert working for SURFmarket attends the meetings, as does SURF's Corporate Privacy Officer. SURF employees (including the secretary) do not serve as committee members.

CSCs are consulted on the appointment of the committee members. The appointment of the committee members is at the discretion of SURF's Board of Directors. The composition of the committee is published on SURF's website.

The Legal Affairs Committee convenes four times per year. The Legal Affairs Committee advises SURF's Board of Directors on the contents and application of the Framework. The Committee prepares revisions and ensures that the Framework is in line with developments in the area of legislation and other relevant developments.

SURF may consult the Committee on any revisions it wishes to make to the Framework. If the requested revisions are substantial, both with regard to the document and with regard to the methods used, the Committee will consult the Board, which will decide on the revisions.

The Board answers to the Council of Members in terms of the way in which it deals with recommendations. Minor revisions proposed by the Committee may be submitted to the Board member in charge of the privacy and security portfolio, who will be in a good position to make a decision on the subject.

The Committee compiles an annual report and submits it to the Board. The report is also shared with the Members Council.

4. Practical instruments and other useful information

The Framework has several appendices, which were drawn up to help educational institutions use and implement the Framework:

Appendix A: SURF Sample Data Processing Agreement
Appendix B: Instructions regarding the Sample Data Processing Agreement
Appendix C: Useful information on security precautions to be taken
Appendix D: Useful information on the service provider's obligation to undergo auditing

The Framework will continue to evolve and we seek to add even more useful information and practical tools to the Framework that will help educational institutions apply the Framework to real-life situations. This version of the Framework mainly focuses on privacy, but other subjects, such as reliable data availability and data confidentiality, will be discussed in more detail soon.