FPC model contract clause on cyber-risks

The Federal Procurement Conference FPC provides the procurement offices of the Federal Administration with a model clause on the protection of IT and telecommunication systems from attack and a corresponding reporting obligation, for use in procurement contract templates. The model clause is designed as a stand-alone contract provision with several sub-clauses which can be integrated into a procurement contract. The explanatory notes to the model clause aim to promote understanding and provide concrete examples for use, but are not intended to be used as contract content. The model clause is suitable mainly for procurements involving a high risk of cyberattack within the meaning of the provisions below. The need to use the model clause should be assessed on a case-by-case basis and its contents are dispositive in the sense that, for each contract, the risk-optimised design should be tailored to the specific circumstances.

The model contract clause is followed by notes on its use and content.

Clause X Protection of IT and telecommunication systems from attack, reporting obligation

1. The NN (designation according to the contract for partners of the Federal Administration)[1] is obliged to protect the IT and telecommunication systems in its area of responsibility as well as its own systems at contract conclusion (comprising in particular infrastructure systems, networks, devices and applications as well as data[2] and information[3]) – hereinafter referred to as "systems" – against attacks in accordance with the current state of the art using technically and organisationally possible and economically reasonable precautions.

2. Attack (equivalent term: cyberattack) means, in particular, unauthorised internal or external access, disruption, manipulation or misuse of systems. This includes, in particular, theft, unauthorised processing or destruction of information or data, and other illegal interventions in systems (see, in particular, Arts. 143, 143bis, 144bis, 147, 179^{novies} and 272 to 274 of the Criminal Code (SCC[4])).

3. The NN undertakes, in particular, to protect data and information provided to it and third parties commissioned by it[5] (e.g. subcontractors and suppliers) for the purpose of correct contract performance or created at the NN, in accordance with the provisions of this clause X. This applies especially to sensitive data or personal data. The requirements and provisions of the Data Protection Act (FADP[6]), the Ordinance on Protecting against Cyber-Risks in the Federal Administration[7] and the Information Protection Ordinance (IPO[8]) shall be taken into account and complied with.

---

1 Adjust the terminology to the contract template (e.g. contractor, company)
2 e.g. personal information on employees, email addresses, access codes, etc.
3 e.g. process descriptions, working procedures, plans, access rules, infrastructure, etc.
4 SR 311.0
5 This includes all parties involved in the supply and production chain, specifically also rights holders and manufacturers
6 SR 235.1
7 SR 120.73
8 SR 510.411

Bundesamt für Bauten und Logistik BBL
Fellerstrasse 21, 3003 Bern
Tel. +41 41 58 462 38 50, Fax +41 58 465 50 09
bkb@bbl.admin.ch
www.bbl.admin.ch/bkb

4. The NN shall inform the procurer[9] and/or the office designated in the contract of any detected incident which might adversely affect the performance of its obligations, immediately following occurrence or detection but at the latest within X hours. In particular, it shall report attempted or successful attacks as well as other suspected or actual technical compromise of systems, data and/or information and any resulting damage. It shall also provide information on the remedial measures planned and implemented. To prevent damage or further attacks, the NN shall, at the first time of asking, immediately grant the procurer or its commissioned third parties full and comprehensive access to analyses, investigation reports and other findings (documents, data, log data, objects, etc.) enabling incident analysis. The NN shall ensure that activities predefined together with the procurer are logged and evaluated for attack detection and prevention purposes. Detected security vulnerabilities must be remedied as soon as possible.

5. The procurer (or a third party commissioned by it) can conduct audits at the NN where necessary – at the most twice a year. These shall be announced X business days beforehand. Each party shall bear its own audit costs. However, if significant shortcomings within the meaning of this provision are identified during an audit, the NN shall bear the cost of remedying these shortcomings as well as the costs arising for the procurer from the audit. The NN is obliged to remedy identified shortcomings within a period of X following the report, and to inform the procurer of the completion of the remedial action.

6. The NN shall be liable to pay a contract penalty, unless it takes the required precautions under the preceding clause. This penalty shall amount to 10% of the entire remuneration per case of violation, but at least CHF 3,000 per case. Payment of the contract penalty shall not release the NN from compliance with its contractual obligations. Contract penalties shall be offset against any compensation for damages.

7. The NN shall be liable for damage to the procurer, unless it can prove that it was not at fault.

In the event of significant violations of this clause or lack of cooperation in the cases cited above, the procurer reserves the right not to procure any further services and to terminate the contractual relationship.

A possible sub-clause 8 regulating a liability insurance obligation may be inserted (*see corresponding notes with suggested wording below*).

For notes, see next pages

[9] Adjust the terminology to the contract template (e.g. client, purchaser)

Notes on the model clause:

Information on completing the clause:

When drawing up the contract, placeholders highlighted in yellow should be replaced with the desired content.

General:

The aim is the protection of data, information and systems, specifically against and in the event of cyberattacks.

The model template should be used as a general provision for transactions for which associated risks have been identified, specifically in IT and telecommunication procurement contracts in particularly risky situations. Risks should generally be expected in all situations where a contractual partner uses IT and telecommunication systems in the performance of its services. In particular, the aim is to prevent or minimise damage to or loss of Federal Administration data, information and systems as a result of a cyberattack on one of its business partners. The same applies if the business partner's information systems are used (or an attempt is made to use them) as a way to launch a cyberattack on the Federal Administration. For example, the aim is to protect codes and passwords or information such as occupancy plans, construction plans or plans for technical facilities (for further examples, see footnote 3 of the model clause).

If a contract with a business partner is being drawn up, this model clause should be used to take account of protection and information requirements.

This model clause should be adapted as necessary; the provisions are dispositive. In particular, where the contractual partner processes data and/or information that are specifically subject to professional secrecy or other confidentiality provisions or are designated as classified under the relevant federal information protection provisions, it must additionally be checked on a case-by-case basis whether the provisions of this clause will have to be fleshed out in more detail in the contract.

Conversely, it is also possible to accommodate less risky situations in individual cases by adjusting individual provisions of this clause as appropriate, for instance through a less stringent wording on the contractual penalty or audit rights.

Mutual agreements on protection and reporting measures are also not excluded in cases where business partners themselves share commercial secrets, sensitive information or data with the Federal Administration. However, when concluding a mutual agreement on these contractual provisions or parts thereof, both parties' obligations in terms of access and audit rights, and the contractual penalties for the contracting Federal Administration office should be thoroughly examined before the contract is concluded. In this regard, we recommend consulting the relevant legal service.

Notes on sub-clause 1:

"NN" stands for "nomen nominandum", the Latin for "name to be provided", and acts as a placeholder for "insert name here". This is the name of the contractual partner receiving, for the purpose of contract performance, Federal Administration data or information that require protection. When drawing up the contract, insert the correct name of the contractual partner.

Notes on sub-clause 2:

See also page 25 of the national strategy for the protection of Switzerland against cyber-risks, available here:

https://www.isb.admin.ch/isb/en/home/themen/cyber_risiken_ncs/ncs_strategie-2012.html

Notes on sub-clause 3:

"X" denotes the numbering of the model clause in the contract concerned. It must correspond to the numbering used in the title of this contract clause.

Compliance with Swiss laws and regulations can sometimes present problems for foreign contractual partners. Experience has shown that this brings an additional negotiating burden, although this does not prevent the contracting administrative unit from using the clause as a basis for negotiation and ironing out any differences during the contract negotiations. As regards the enforceability of Swiss law, it should be considered whether the service is provided in Switzerland or abroad. As a general rule it is recommended to agree on Swiss law with Bern as the place of jurisdiction.

Notes on sub-clause 4:

"The procurer" is the administrative unit concluding the contract.

The deadline for performing the reporting obligation (X hours) must be defined in the contract concerned according to the specific risks and requirements. There is no generally applicable rule.

It is advisable to set a short deadline appropriate to the level of potential risk; for example, when incidents and their consequences may be critical, a few hours.

The reporting obligation refers, in particular, to critical vulnerabilities and cyberincidents which could impair data protection or system functionality. It does not refer to phishing mails, spam or port scans. A system, database or individual dataset is said to be compromised if the integrity of the stored information can no longer be guaranteed, regardless of whether this occurred through a malicious attack or unintentionally (definition of terms in German according to Wikipedia[10]). The reporting content and method must be defined between the contractual partners, and must take account of the need to protect data and systems.

[10] https://de.wikipedia.org/wiki/Technische_Kompromittierung

Notes on sub-clause 5:

The notice period for an audit (X business days) must be defined in the contract concerned according to the specific risks and requirements. We recommend a notice period of 20 business days, as this is common practice. There is, however, no generally applicable rule. Where justified in individual cases, other audit arrangements can be defined.

The exact notice period, in days, should be inserted instead of "X". Alternatively, a specific date may also be entered, and the sentence adjusted accordingly.

Notes on sub-clause 6:

The rule on contractual penalties is based on the standard clause in the various terms and conditions of the Confederation. In individual specific cases, the amount and calculation can be contractually adjusted, where the risk assessment by the responsible specialist offices concludes that a different rule is appropriate.

Notes on sub-clause 7:

This provision may be omitted or will have to be adjusted if the liability and termination are regulated in other clauses of the contract concerned (see also CCPP contract templates and the General Terms and Conditions of the Confederation), or if the specific risk situation allows or demands it. As a general rule, liability covers all damage arising out of the attacks defined in sub-clause 2 of the model clause.

Notes on possible sub-clause 8:

Certain insurance companies offer the possibility of insuring cyberattack-related risks. As an option in individual cases and for contracts in which the key focus is on the performance of services through IT and telecommunication systems, when dealing with large companies (less so with SMEs) it can be advisable to oblige the contractual partner to take out appropriate additional insurance against potential damage.

Suggested wording for such an arrangement:

"8. The NN undertakes to take out liability insurance appropriate to the nature and risk of damage and to provide proof of adequate insurance cover at the time of contract conclusion."