**FPC model contract clause on cyberattacks**

The Federal Procurement Conference FPC provides the public contracting authorities[[1]](#footnote-1) of the Federal Administration with a model contract clause on procedures in the event of cyberattacks.

By agreeing to these provisions in the contract, the contracting parties contribute to the protection of federal data and information, and systems, in the event of cyberattacks, particularly in the case of security-sensitive activities[[2]](#footnote-2).

The Federal Administration is required to ensure compliance with data protection and information security legislation when working with third parties[[3]](#footnote-3). The administrative units are responsible for IT security within their area of responsibility.

The model contract clause serves as a template for the contracting authorities of the Federal Administration to agree on measures to protect against cyberattacks and the procedure to be followed after[[4]](#footnote-4) a cyberattack on a supplier or service provider[[5]](#footnote-5) that operates Federal Administration IT resources or processes sensitive federal data and information on its systems. The clause thus supports the administrative units' implementation of their obligations under Articles 9 paragraph 1 and Article 10 paragraph 1 of the ISA, Article 13 of the InfoSecO and Article 24 of the FADP (for the legal bases cited, see the references in footnotes 8 and 9).

The model contract clause is designed as an independent contractual provision with multiple sections and can typically be used as part of the contract for IT services, but can also be used in other areas[[6]](#footnote-6)[[7]](#footnote-7).

The explanatory notes that follow the model contract clause are intended to provide a better understanding and a concrete structure for usage scenarios, but are not intended to form part of the contract.

In particular, the protection needs and risk analyses of the competent specialist bodies, the classification of information and the security levels of IT resources are decisive for the assessment of whether agreement on the model contract provisions is appropriate. When used, they serve as a basis for assessing whether and which of the sections of the model contract clause should be integrated into the contract. In line with the purpose of the model contract clause, at least the provisions of sections X1 – X3 should be integrated together in the contract, as well as – unless otherwise regulated in the contract – liability for violation of duty. The proposed contractual penalty provision is available to promote compliance with the obligations, as are the supporting documentation and audit measures, particularly if an increased need for protection, risk or damage potential is identified. If the contract contains further provisions on information and data security, the contents of the model contract clause must be harmonised with these.

**Overview of the provisions** of the model contract clause:

Section **X1** governs the service provider's obligations to *protect* IT resources against cyberattacks and to take *measures* to prevent and remedy threats and vulnerabilities, and defines the term *"cyberattack"*.

Section **X2** obliges the service provider to comply with the relevant *legal bases* and *requirements* and to transfer these obligations to third parties engaged by it.

Section **X3** regulates the *obligation to report* cyberattacks.

Section **X4** obliges the service provider to provide *supporting documentation* for its cybersecurity and authorises the service procurer to carry out *audits* at the service provider's premises.

Section **X5** contains a *contractual penalty* provision.

Section **X6** is a *liability clause*.

Section **X7** serves to agree a *liability insurance obligation*.

The sections are explained after the model contract clause.

**Section X Protection of IT resources against cyberattacks and reporting**

**X1**. The service provider undertakes to protect its IT resources (i.e. means of information and communication technology, namely applications, information systems and data collections as well as facilities, products and services used for the electronic processing of information) which may potentially come into contact with the subject matter of this contract against cyberattacks in accordance with the latest state of the art.

The service provider shall ensure that the activities predefined by the service user are recorded and that these records are continuously analysed in order to allow early detection of and defence against cyberattacks.

The service provider is obliged to prevent a recognised risk from materialising in an effective manner, to initiate its remediation immediately and to inform the service user of this without delay.

The service provider shall rectify any vulnerabilities discovered before, during or after a cyberattack (i.e. weaknesses or defects in IT resources with the potential to enable a cyberattack), immediately and at its own expense.

A "cyberattack" is defined as any intentionally triggered event involving the use of IT resources that results in the confidentiality, availability or integrity of information, or the traceability of its processing, being compromised.

**X2**. When processing federal data and information, the service provider undertakes to observe and comply with the requirements and provisions of the Data Protection Act (FADP[[8]](#footnote-8)) and the Information Security Act (ISA[[9]](#footnote-9)), including the relevant implementing ordinances and the federal basic ICT security. It shall transfer these obligations to third parties it engages (e.g. suppliers, sub-suppliers, substitutes, subcontractors).

**X3**. The service provider shall report potentially successful cyberattacks, i.e. if the confidentiality, availability, integrity or traceability of federal information is directly or indirectly disrupted or jeopardised, or if this was intended. This applies in particular if the IT resources attacked have access to federal IT resources or if there are indications that these attacks were carried out in preparation for further cyberattacks, or are associated with blackmail, threats or coercion. The service provider shall report the type and execution of such a cyberattack within 24 hours of its discovery, at the latest. The parties shall then exchange information on an ongoing basis about the type and execution, possible and actual consequences, planned and implemented measures.

The reports shall be addressed to the following parties:

* Service user(s) (specify points of contact with contact details), and
* National Cyber Security Centre (NCSC) via online form[[10]](#footnote-10)

If the service user or the NCSC deem it necessary to protect the Confederation's data and information, the service provider shall immediately grant them and third parties engaged by them to process the incident access to analyses, investigation reports and other findings and information (documents, data, log data, objects, etc.) that allow the cyberattack and its effects to be analysed and averted.

**X4**. The service provider shall provide the service user with supporting documentation on its cybersecurity in the form of (specify and insert form) every six months spontaneously and without separate invoicing. If this supporting documentation is deemed insufficient or if there are any indications of deficiencies in cybersecurity, the service user (or a third party on its behalf) may conduct cybersecurity audits at the service provider and third parties engaged by it. Such audits shall be announced X working days in advance. Each party shall bear its own audit costs. However, if significant cybersecurity deficiencies are identified during an audit, the service provider shall bear the service user's audit costs in addition to its own costs and the costs of remediation.

**X5**. The service provider shall owe a contractual penalty if it fails to fulfil its reporting obligations to the service user under sections X1 - X4, or fails to do so in a timely manner, or fails to immediately remedy any vulnerabilities discovered or defects identified. This penalty shall amount to 10% of the entire remuneration per case of violation, but at least CHF 10,000 per case. Payment of the contractual penalty shall not release the service provider from compliance with its contractual obligations. Contract penalties shall be offset against any compensation for damages.

**X6**. The service provider shall be liable for any damages incurred by the service users as a result of cyberattacks and non-compliance with the provisions in sections X1 - X4, unless it can prove that it is not at fault.

A possible section **X7** regulating a liability insurance obligation may be inserted (*see corresponding notes with suggested wording below*)

Federal Procurement Conference (FPC)

Issued: 01.01.2024[[11]](#footnote-11)

Status: 01.03.2024[[12]](#footnote-12)

For notes, see next pages

**Explanatory notes on the model contract clause:**

 **Note on completing the clause**:

When drawing up the contract, placeholders highlighted in yellow should be replaced with the desired content. "X" refers to the numbering of this model clause in the respective contract in which it applies; it will have to be adapted accordingly.

**Notes on section X1:**

"Service provider" refers to the contractual partner who, for the purpose of contract performance, has received or gained access to data and/or information of the Federal Administration that requires protection from cyberattacks. When drawing up the contract, the name of the contractual partner must be inserted as it is used throughout the contract.

The term "service user" refers to the administrative unit concluding the contract. The organisational unit that signs the contract with the service provider is decisive. This may be the procurement office or the requesting office, or both.

The service provider's obligation to take protective measures is intended to prevent a directly or indirectly successful cyberattack, or at least minimise its impact. This includes, for example, the protection of codes and passwords, classified information and systems, and non-public information such as occupancy plans, construction plans and plans of technical facilities, personal data, process descriptions, workflows and access regulations.

Protection must be provided in accordance with the latest state of the art and commensurate with the risk, which in the specific case allows consideration of the technical and organisational possibilities and, if appropriate, economic reasonableness. The costs incurred by the service provider for the protection and its maintenance are borne by the service provider itself. As a result, the costs for the remediation of vulnerabilities that are discovered before, during or after a cyberattack are also borne by the service provider.

The obligation is not tied to a specific duration in the template. It shall apply at least for the duration of the contractual relationship. If, in a specific case, the IT resources are to be protected before and/or after the conclusion of the contract due to the risks involved, corresponding obligations are to be defined and agreed with the service provider in advance (e.g. during the tender process, contract negotiations, etc.). This also applies in particular to systems on which the service user's data or information remains after the provision of goods/services , e.g. until it is returned, deleted or destroyed (in this respect, it is recommended that a deadline be set, unless this is already specified in the Confederation's general terms and conditions, which are agreed for the contractual relationship).

The section's scope of application may – where appropriate – be limited to systems of the service provider that are relevant to the security of the Federal Administration.

In accordance with Article 5 of the revised ISA, cyberattacks are intentionally triggered cyberincidents, i.e. events involving the use of IT resources that result in the confidentiality, availability or integrity of information or the traceability of its processing being compromised.

Examples include unauthorised access, disruption, manipulation or misuse of systems and data from inside or outside, or the theft, unlawful processing or destruction of information or data, and other unlawful interventions in the systems and associated acts (see in particular Art. 143, 143bis, 144bis, 147, 179novies, 272 to 274 of the Swiss Criminal Code (SCC[[13]](#footnote-13))).

See also the explanations on Article 5 in the dispatch on the revised ISA and the information provided by the NCSC on the National Cyberstrategy NCS (at the following link: [National Cyberstrategy NCS (admin.ch)](https://www.ncsc.admin.ch/ncsc/en/home/strategie/cyberstrategie-ncs.html)).

**Notes on section X2:**

The obligation applies to the service provider and its engaged third parties (e.g. subcontractors, substitutes and suppliers). It guarantees to protect data and information made available or created and/or processed by it and/or the third parties it engages for the correct contract performance in accordance with the specifications. This applies in particular to security-relevant information and personal data.

**Notes on section X3:**

The contract must ensure that the parties are released from official secrecy for the notification of a cyberattack and the subsequent exchange and cooperation in order to avoid delays following a cyberattack.

The contract must specifically designate the contact points at the service user to whom the service provider must report the cyberattack (this is usually the service user's information security officer). The NCSC shall also receive the report. If necessary, other recipients of reports are also be named in the contract.

The constellations listed in this section each trigger the reporting obligation individually and do not have to be cumulative in the event of a cyberattack.

The obligation to report relates to cyberattacks that could impair data protection or the functionality of IT resources. There is no obligation to report unsuccessful and harmless cyberattacks, such as spam emails sent en masse or port scans. A cyberattack is successful if the confidentiality, availability, integrity or traceability of federal information can no longer be guaranteed, regardless of whether this occurs unintentionally or with malicious intent. The contract between the contracting parties must define the content and nature of this report. The protection requirements of the data and IT resources must be taken into account.

The report must be made within 24 hours of the cyberattack being discovered[[14]](#footnote-14). If, in individual cases, a different deadline is appropriate and indicated[[15]](#footnote-15), the template may be deviated from, provided that the organisational requirements for receiving and processing the report(s) are met by the service user. Within the agreed deadline, only the information known up to the time of the report must be provided; the report may be supplemented at a later date.

The purpose of the report and subsequent exchanges between the parties is to quickly communicate information on the nature and execution of the cyberattack, its possible effects, the measures taken and the planned next steps. The NCSC template for reporting cyberincidents provides guidance on the structure and content of a report: [NCSC report (admin.ch)](https://www.report.ncsc.admin.ch/en/chat?path=371%3E1%3E356)

Further information from the NCSC on how to respond to cyberattacks can be found here:

[Cyberattack – what to do? Information and checklists (admin.ch)](https://www.ncsc.admin.ch/ncsc/en/home/infos-fuer/infos-behoerden/vorfall-was-nun/checkliste-ciso.html)

**Notes on section X4:**

Supporting documentation can take the form of certain certifications or audit reports, for example; standard and recognised types of supporting documentation are acceptable. For the purposes of legal certainty and enforceability, the form of supporting documentation must be specified in provision X4 or in the contract (e.g. as an appendix).

The frequency of the semi-annual provision of supporting documentation can be adapted to the circumstances of the individual case or combined with an additional right of the service user to request supporting documentation at any time. The provision of supporting documentation does not entitle the service provider to additional, separate compensation for the associated costs and expenses.

The service user creates the conditions for audits to be carried out. It is advisable to specify the modalities of the audit in the contract. In this model contract template, the prerequisite for an audit is that the supporting documentation is deemed insufficient or that there are indications of deficiencies in cybersecurity. This is in line with common practice and also justifies the fact that each party bears its own expenses and costs arising from the audit. As a variant to this regulation, a general right of the service users to order and carry out an audit is also conceivable. In practice, however, an unconditional right to audit at any time with cost sharing will be difficult to agree with the service provider.

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

It is appropriate to transfer costs to the service provider in the event of significant deficiencies. The deficiencies and their significance depend on the specific circumstances of the individual case and must be specified in the contract as far as possible.

In principle and in accordance with section X1, the obligation to immediately remedy any weaknesses identified applies. If necessary, a separate deadline for the remediation of deficiencies discovered during an audit can be specified in the contract in line with common practice, depending on the type or category of deficiency and the circumstances.

**Notes on section X5:**

The contractual penalty provision is not the same as the standard contractual penalty clause in the various GTCs of the Confederation. The minimum amount is higher at CHF 10,000. In individual cases, it can be contractually adjusted in terms of amount and assessment in accordance with the risk assessment of the relevant specialist bodies. Alternatively, a general contractual penalty provision can also be included in the contract, provided that it covers the cases of violation regulated here. For the purposes of traceability, it is advisable to document the motives for an adjustment, particularly in the case of a reduction in the minimum amount (together with a comprehensible justification as to why a low risk is assumed in the specific case).

**Notes on section X6:**

In principle, liability covers all losses arising from attacks in accordance with section X1 and other non-compliance with the model contract provisions. The liability clause thus covers the damage caused by the cyberattack and other damage incurred by the service user as a result of non-compliance with the provisions of this model clause.

Whether this liability provision is appropriate for the specific circumstances must be examined by the service user in each case and adapted if necessary.

This provision can be omitted or must be adapted if the liability is regulated elsewhere in the contract and the liability cases from this model contract clause are included there (see also contract templates of the Federal Office for Buildings and Logistics FOBL, the Competence Centre for Federal Public Procurement CCPP and the Confederation's GTC), or if the specific risk situation permits or requires this.

In the contract, the conditions for termination must ensure that non-compliance with the provisions regarding cyberattacks is defined as a reason for termination for the service user (as an extraordinary reason for termination or as termination for good cause).

**Notes on possible section X7**:

Certain insurance companies offer the option of insuring against risks related to cyberattacks. In individual cases and for contracts in which the core object is the provision of IT services, it may be advisable to require the contractual partner to take out additional insurance to cover the potential loss. In practice, very different insurance solutions are available. To ensure that the insurance cover is appropriate, it is advisable to have the applicable insurance conditions submitted to the service user for review before taking out the insurance. The procedure for this must be specified in the contract.

Suggested wording for such an agreement:

*"X7. The service provider undertakes to take out liability insurance appropriate to the nature and risk of the damage and to provide evidence of sufficient insurance cover at the time the contract is concluded. The insurance conditions applicable to the insurance agreement must be submitted to the service user for review before the insurance is taken out."*

In this case, it must be stipulated as an eligibility criterion in the award procedure that the tenderer is obliged to provide the corresponding supporting documentation at the request of the contracting authority if the contract is awarded.

\*\*\*\*\*

1. This model contract clause is available to all service users in the Federal Administration, in particular the contracting authorities responsible for the procurement of ICT services. The rules on procurement powers are set out in the Ordinance of 24 October 2012 on the Organisation of Federal Public Procurement (OPPO, SR 172.056.15). [↑](#footnote-ref-1)
2. The contractual definition of the minimum requirements for IT resources and the guarantee of their security and protection by the service provider are not the purpose and content of these model provisions. [↑](#footnote-ref-2)
3. The Confederation's general terms and conditions (GTC) contain standard clauses on confidentiality, data protection and data security (including data return, deletion and destruction). The GTC are available on the FPC website ([www.bkb.admin.ch](http://www.bkb.admin.ch)). [↑](#footnote-ref-3)
4. Agreeing the model contract clause in the contract does not remove the responsibility to take into account the security procedures, regulations, specifications and requirements relating to data and information security (including basic ICT security) in all public contracts for IT services and, where necessary, to contractually agree measures (e.g. penetration tests) with the service provider (see footnote 5) that go beyond this model contract clause. [↑](#footnote-ref-4)
5. Referred to as "service provider" in the model contract clause. [↑](#footnote-ref-5)
6. Where contractual partners process federal information or data without providing IT services to the Confederation, such as printing companies, law firms, consulting firms, translation agencies, architecture and planning firms, etc. [↑](#footnote-ref-6)
7. In particular, where the contractual partner processes data and/or information that is specifically subject to official secrecy or other confidentiality provisions, or is classified in accordance with the relevant federal information protection provisions, it must also be examined on a case-by-case basis whether the provisions of this model contract clause need to be specified in the contract, regulated in more detail or supplemented by additional provisions. [↑](#footnote-ref-7)
8. Federal Act of 25 September 2022 on Data Protection, SR 235.1 [↑](#footnote-ref-8)
9. Federal Act of 18 December 2020 on Information Security in the Confederation, SR 128 [↑](#footnote-ref-9)
10. Available at https://www.ncsc.admin.ch/ncsc/en/home.html [↑](#footnote-ref-10)
11. This model clause replaces the FPC template on cyber-risks of 01.09.2020 (status 09.11.2022). [↑](#footnote-ref-11)
12. Compared to the status as of 1 January 2024 (only available in German), an incorrect reference to two footnotes has been corrected. [↑](#footnote-ref-12)
13. SR 311.0 [↑](#footnote-ref-13)
14. Analogue to the regulation in Article 74e of the revISA. [↑](#footnote-ref-14)
15. Clarification and consultation with the NCSC is recommended, as the report is also sent to the NCSC. [↑](#footnote-ref-15)