Clause contractuelle type de la CA pour les cyberrisques

La Conférence des achats de la Confédération (CA) met à disposition des services d'achat de l'administration fédérale, afin qu'ils puissent l'insérer dans leurs modèles de contrats, une clause type prévoyant la protection des systèmes informatiques et de télécommunication face aux attaques et l'obligation de déclarer de tels incidents. Il s'agit d'une disposition contractuelle à part entière, formée de plusieurs chiffres, qui peut être reprise dans un contrat d'achat. Les explications complémentaires qui suivent sont utiles pour mieux comprendre cette clause et pour la concrétiser dans les cas pratiques, mais ne font pas partie du contenu d'un tel contrat. La clause type convient en premier lieu aux achats comportant un risque élevé de cyberattaque au sens des dispositions ci-dessous. Les services d'achat examineront, en fonction de leurs besoins, si la clause s'applique, en gardant à l'esprit qu'il s'agit de droit dispositif, autrement dit qu'il leur faut adopter pour chaque contrat une version de cette clause optimisée en fonction des risques.

Le présent document renferme encore des explications portant sur les conditions d'utilisation du modèle de clause contractuelle et sur sa teneur matérielle.

Ch. X Protection des systèmes informatiques et de télécommunication face aux attaques et obligation de déclarer

1. Il incombe au N.N. (nom selon le contrat établi pour le partenaire de l'AF)[1], pour et pendant l'exécution du présent contrat, de protéger des attaques ses systèmes informatiques et de télécommunication (soit, en particulier, les systèmes d'infrastructure, les réseaux, les appareils et applications, ainsi que les données[2] et informations[3]) – ci-après «systèmes» –, en prenant dans son domaine de compétence toutes les précautions possibles d'un point de vue technique et organisationnel en l'état actuel des connaissances, pour autant qu'elles soient économiquement raisonnables.

2. Sont notamment considérés comme «attaques» (terme équivalent: «cyberattaques») les cas d'accès interne ou externe non autorisé, de perturbation, de manipulation ou d'utilisation abusive des systèmes. Il en va de même du vol, du traitement illicite ou de la destruction d'informations ou de données, ainsi que de toute autre forme d'intrusion illégale commise à cet effet dans les systèmes (voir, en particulier, les art. 143, 143bis, 144bis, 147, 179^{novies} et 272 à 274 du code pénal [CP[4]]).

3. Le N.N. s'engage en particulier à protéger, conformément aux dispositions du présent ch. X, les données et informations mises à sa disposition ou à celle des tiers mandatés par lui[5] (par ex. sous-traitants et fournisseurs) pour l'exécution correcte du contrat. Il en va notamment ainsi pour les données liées à la sécurité ou personnelles. Les exigences et les prescriptions

---

1 La terminologie sera adaptée au modèle de contrat (p. ex. mandataire, entrepreneur).
2 Par ex. données personnelles des collaborateurs, adresses électroniques, mots de passe et codes d'accès, etc.
3 Par ex. descriptions de processus, flux de travail, plans, réglementations d'accès, infrastructure, etc.
4 RS 311.0
5 Tous les intervenants de la chaîne d'approvisionnement et de production, titulaires de droits et fabricants compris, sont concernés ici.

Office fédéral des constructions et de la logistique OFCL
Fellerstrasse 21, 3003 Berne
Tél. +41 41 58 462 38 50, fax +41 58 465 50 09
bkb@bbl.admin.ch
www.bbl.admin.ch/bkb

de la loi fédérale sur la protection des données (LPD[6]), celles de l'ordonnance sur la protection contre les cyberrisques dans l'administration fédérale (ordonnance sur les cyberrisques, OPCy[7]), de l'ordonnance concernant la protection des informations (OPrI[8]) et de l'ordonnance sur l'informatique dans l'administration fédérale (OinF[9]) seront prises en compte et respectées dans ce contexte.

4. Le N.N. signalera spontanément au bénéficiaire de prestations[10] et/ou au service indiqué à cet effet dans le contrat, aussitôt après sa survenance ou sa découverte, mais au plus tard dans un délai de X heures, tout incident qui pourrait l'empêcher de respecter ses engagements contractuels. Il indiquera en particulier les attaques tentées ou fructueuses, ainsi que toute autre compromission technique réelle ou redoutée de systèmes, données et/ou informations, avec le cas échéant les dommages engendrés. Il précisera à cette occasion les mesures envisagées ou adoptées pour y remédier. Afin d'éviter tout dommage ou de nouvelles attaques, le N.N. accordera immédiatement au bénéficiaire de prestations ou au tiers mandaté par lui, à sa première demande, un plein accès à l'ensemble des analyses, des rapports d'enquêtes et autres constatations (documents, données, données du journal, objets, etc.) permettant d'analyser l'incident. Le N.N. veillera à ce que les activités prédéfinies avec le bénéficiaire de prestations soient enregistrées (journalisation) et analysées, afin d'identifier et de prévenir les attaques. Les failles de sécurité découvertes seront rapidement réparées.

5. Le bénéficiaire de prestations (ou un tiers mandaté par lui) peut réaliser en cas de besoin – mais au maximum deux fois par an – des audits auprès du N.N. Ils seront communiqués X jours ouvrés à l'avance. Chaque partie supporte ses propres coûts liés à l'audit. Mais si dans le cadre d'un audit, de graves lacunes au sens de la présente disposition devaient être constatées, le N.N. assumerait les coûts destinés à remédier à ces lacunes, ainsi que les coûts subis par le bénéficiaire de prestations au titre de cet audit. Le N.N. est tenu de corriger les lacunes constatées dans un délai de X à partir de leur signalement et de communiquer au bénéficiaire de prestations que les travaux ont été exécutés.

6. Le N.N. doit s'acquitter d'une peine conventionnelle, à moins d'avoir pris les précautions exigées par la présente clause. Celle-ci correspond à 10 % de la rémunération totale par infraction, mais au moins à 3000 francs par cas. Le paiement de la peine conventionnelle ne libère pas le N.N. de ses obligations contractuelles. La peine conventionnelle sera imputée aux éventuels dommages-intérêts à verser.

7. Le N.N. répond des dommages subis par le bénéficiaire de prestations, à moins de prouver qu'aucune faute ne lui est imputable.

En cas de violation substantielle de la présente clause ou de collaboration insuffisante dans les cas susmentionnés, le bénéficiaire de prestations se réserve le droit de ne pas acquérir d'autres prestations et de mettre fin à la relation contractuelle.

Évt, introduire un ch. 8 réglant l'obligation de conclure une assurance responsabilité civile *(voir ci-dessous les explications correspondantes et la proposition de texte)*

Conférence des achats de la Confédération (CA)
Publication le: 01.09.2020
État au: 01.09.2020

Des explications sont données aux pages suivantes.

---

6 RS 235.1
7 RS 120.73
8 RS 510.411
9 RS 172.010.58
10 La terminologie sera adaptée au modèle de contrat (par ex. mandant, acheteur).

Explications relatives à la clause type:

Remarque pour la finalisation de la clause type:

Les emplacements surlignés en jaune seront remplacés par le contenu souhaité lors de l'établissement du contrat.

Généralités:

Le but est d'assurer la protection des données, des informations et des systèmes, tant en amont que lors d'une cyberattaque.

Ce modèle s'utilisera comme disposition générale dans les affaires où de tels risques ont été identifiés, soit notamment pour les contrats portant sur des achats informatiques dans des situations particulièrement risquées. Des risques sont en principe à prévoir partout où un partenaire contractuel utilise des systèmes informatiques et de télécommunication pour fournir ses prestations. Il s'agit, en particulier, d'empêcher qu'une cyberattaque lancée contre un de ses partenaires commerciaux ne cause à l'administration fédérale des dommages ou des pertes au niveau de ses données, informations ou systèmes, et le cas échéant d'en atténuer les conséquences. Il en va de même au cas où les systèmes d'information de ses partenaires commerciaux seraient utilisés pour lancer une cyberattaque contre l'administration fédérale. Il s'agit par exemple d'assurer la protection des codes et des mots de passe ou d'informations telles que les plans d'occupation, les plans de construction ou les plans des installations techniques (pour d'autres exemples, voir la note de bas de page 3 de la clause type).

Si un contrat est en cours d'élaboration avec un partenaire commercial, il convient de tenir compte de tels besoins de protection et d'information en y insérant cette clause modèle.

Cette clause type sera adaptée là où c'est nécessaire, comme il s'agit de droit dispositif. En particulier, si le partenaire contractuel traite des données et/ou des informations qui sont soumises au secret de fonction ou à d'autres dispositions sur la confidentialité ou qu'il faut considérer comme classifiées en vertu des dispositions fédérales sur la protection des informations, il convient d'examiner dans le cas d'espèce s'il y a lieu de préciser dans le contrat les dispositions de cette clause.

A contrario il est possible de tenir dûment compte, dans un cas d'espèce, des situations à faible risque en adaptant certaines dispositions de cette clause, par exemple en allégeant la peine conventionnelle ou les conditions du droit d'audit.

Il n'est pas non plus exclu de conclure un accord prévoyant des mesures réciproques en matière de protection et de déclaration des incidents si, de leur côté, les partenaires commerciaux confient à l'administration fédérale des secrets d'affaires ou des données à protéger. Au cas où les présentes dispositions ou une partie d'entre elles seraient conclues sur une base de réciprocité pour les deux parties contractantes, il convient néanmoins d'examiner en détail, avant la conclusion du contrat, les engagements pris par l'unité administrative contractante à propos des droits d'accès, des droits d'audit ainsi que de la peine conventionnelle. Nous recommandons à cet effet de consulter le service juridique compétent.

ad ch. 1:

«N.N.» est l'acronyme de «nomen nominandum» (du latin «à nommer, à déterminer»). En l'occurrence, il remplace le nom du partenaire contractuel ayant reçu, aux fins de l'exécution du contrat, des données ou informations de l'administration fédérale qu'il s'agit de protéger des cyberattaques. Lors de l'établissement du contrat, il faudra inscrire le nom correct de ce partenaire contractuel.

ad ch. 2:

Voir aussi la «Stratégie nationale de protection de la Suisse contre les cyberrisques» (p. 28), téléchargeable sous le lien ci-après:

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

ad ch. 3:

«X» remplace le numéro donné à cette clause type dans le contrat où elle est utilisée. Il doit correspondre au numéro du titre de la clause contractuelle.

Le cas échéant, le respect des bases et des exigences légales peut soulever des difficultés avec les partenaires contractuels étrangers. Expérience à l'appui, des négociations supplémentaires sont à prévoir, ce qui n'empêche pas l'unité administrative contractante d'utiliser cette clause comme base de discussion et d'éliminer les éventuelles divergences lors des négociations. Par principe, pour faire valoir le droit suisse, il faut vérifier si la prestation est fournie en Suisse ou à l'étranger. Il est recommandé de convenir que le droit suisse s'applique et que le for est à Berne.

ad ch. 4:

L'expression «le bénéficiaire de prestations» désigne l'unité administrative contractante.

Le délai à respecter pour l'exercice de l'obligation de déclarer (X heures) sera fixé à chaque fois dans le contrat auquel il s'applique, en fonction des risques et besoins concrets. Il n'existe pas en la matière d'exigence générale qui s'appliquerait à tous les cas.

L'obligation de déclarer se réfère en particulier aux vulnérabilités critiques et aux cyberincidents pouvant mettre en péril la protection des données ou le bon fonctionnement du système. Ni les courriels de phishing, ni les pourriels ou le balayage des ports ne sont visés ici. Un système, une base de données ou même un simple jeu de données sont considérés comme techniquement compromis s'il n'est plus possible de garantir l'intégrité des informations sauvegardées. Peu importe en pareil cas que l'attaque ait été commise dans une intention malveillante ou que la compromission ait été accidentelle[11]. Les parties contractantes devront définir le contenu et le type de déclaration à faire. Il convient à cet effet de prendre en compte le besoin de protection des données et du système.

[11] Voir la notion de compromission technique définie (en allemand) dans Wikipedia sous https://de.wikipedia.org/wiki/Technische_Kompromittierung.

ad ch. 5:

Le délai de préavis d'un audit (X jours ouvrés) sera fixé dans le contrat auquel il s'applique, en fonction des risques et besoins concrets. Dans la pratique, un délai de 20 jours ouvrés est proposé. Il n'existe toutefois pas en la matière d'exigence générale qui s'appliquerait à tous les cas. Les modalités de l'audit pourront également être adaptées dans un cas d'espèce, pour autant que ce soit justifié.

À la place de «X», il convient d'inscrire le délai exact calculé en jours. Comme alternative, il est également possible de convenir d'une date concrète, en modifiant en conséquence cette partie de phrase.

ad ch. 6:

La réglementation sur les peines conventionnelles s'inspire de la clause habituelle figurant dans les diverses conditions générales (CG) de la Confédération. Son montant ou son mode de calcul pourront être adaptés contractuellement si dans le cas concret, il ressort de l'évaluation des risques menée par les services compétents qu'une réglementation différente serait adéquate.

ad ch. 7:

Cette disposition peut être biffée ou doit être adaptée si d'autres chiffres portent déjà sur la responsabilité et sur la résiliation du contrat (voir aussi les modèles de contrats du CCMP et les CG de la Confédération), ou si la situation de risque spécifique le permet ou l'exige. En principe, tous les dommages résultant des attaques visées au ch. 2 de la clause relèvent de la responsabilité du partenaire contractuel.

ad ch. 8 éventuel:

Certaines entreprises d'assurance offrent la possibilité d'assurer les risques liés aux cyberattaques. Dans des cas d'espèce et pour autant que les contrats aient pour point central la fourniture de prestations par des systèmes informatiques et de télécommunication, il peut être recommandé comme option, dans les contrats conclus avec de grandes entreprises (moins avec les PME) d'obliger le partenaire contractuel à contracter une assurance conforme au potentiel de dommages.

Proposition d'accord:

«8. Le N.N. s'engage à conclure une assurance responsabilité civile couvrant les cyberattaques et adaptée aux risques de dommages ainsi qu'à prouver, au moment de la conclusion du contrat, qu'il possède une couverture d'assurance suffisante.»