**Clause contractuelle type de la CA pour les cyberattaques**

La Conférence des achats de la Confédération (CA) met à la disposition des adjudicateurs publics[[1]](#footnote-2) de l’administration fédérale un modèle de clause contractuelle concernant la procédure à suivre en cas de cyberattaque.

En convenant de cette clause dans un contrat, les partenaires contractuels contribuent à la protection des données et des informations de la Confédération ainsi que des systèmes en cas de cyberattaques, en particulier dans le cadre d’activités sensibles sur le plan de la sécurité[[2]](#footnote-3).

Lorsqu’elle collabore avec des tiers, l’administration fédérale est tenue de veiller au respect des prescriptions légales en matière de protection des données et de sécurité de l’information[[3]](#footnote-4). Les unités administratives sont responsables de la sécurité informatique dans leur domaine de compétence respectif.

La clause contractuelle type sert de modèle aux pouvoirs adjudicateurs de l’administration fédérale pour convenir des mesures de protection à mettre en place contre les cyberattaques et de la procédure à suivre[[4]](#footnote-5) après une cyberattaque contre un fournisseur ou un prestataire[[5]](#footnote-6) qui exploite des moyens informatiques de l’administration fédérale ou traite sur ses systèmes des données et des informations sensibles de la Confédération. Elle soutient ainsi les unités administratives dans la mise en œuvre de leurs obligations au titre des art. 9, al. 1, et 10, al. 1, de la loi sur la sécurité de l’information (LSI), de l’art. 13 de l’ordonnance sur la sécurité de l’information (OSI) et de l’art. 24 de loi fédérale sur la protection des données (LPD) (pour les bases légales citées, voir les références dans les notes de bas de page 8 et 9).

Il s’agit d’une disposition contractuelle à part entière, articulée en plusieurs chiffres, qui s’applique typiquement dans le cadre des contrats de prestations informatiques, mais peut également être utilisée dans d’autres domaines[[6]](#footnote-7), en tant qu’élément du contrat[[7]](#footnote-8).

Les explications qui complètent la clause contractuelle type sont destinées à en faciliter la compréhension et à en concrétiser l’application, mais ne font pas partie intégrante du contrat.

Les analyses des besoins de protection et du risque effectuées par les services spécialisés, la classification des informations et les niveaux de sécurité des moyens informatiques sont déterminants pour décider s’il est indiqué d’appliquer les dispositions de la clause contractuelle type. Ils servent de base pour déterminer si la clause contractuelle type doit être intégrée dans le contrat et, le cas échéant, quels en sont les points. Conformément à l’objectif de la clause contractuelle type, les dispositions visées aux points X1 à X3 devraient au moins y figurer, de même que - sauf disposition contraire dans le contrat - la responsabilité en cas de manquement à une obligation. Pour encourager le respect des obligations, la réglementation proposée relative aux peines conventionnelles ainsi que – en particulier si un besoin accru de protection, un risque ou un potentiel de dommages sont identifiés – des mesures d’audit et de fourniture de justificatifs peuvent être appliquées. Si le contrat prévoit d’autres dispositions relatives à la sécurité de l’information et des données, le contenu de la clause contractuelle type doit être adapté en conséquence.

**Aperçu des dispositions** de la clause contractuelle type :

Le chiffre **X1** règle les obligations du fournisseur de prestations en matière de *protection* des moyens informatiques contre les cyberattaques ainsi que les *mesures* de prévention et d’élimination des dangers et des vulnérabilités. Il définit en outre la notion de «*cyberattaque*».

Le chiffre **X2** oblige le fournisseur de prestations à respecter les *bases légales* et *les directives* pertinentes, et à transférer ces obligations aux tiers qu’il a mandatés.

Le chiffre **X3** règle l’*obligation de signaler* les cyberattaques.

Le chiffre **X4** oblige le fournisseur de prestations à *prouver* sa cybersécurité et autorise le bénéficiaire des prestations à effectuer des *audits* chez le fournisseur de prestations.

Le chiffre **X5** contient une réglementation sur les *peines conventionnelles*.

Le chiffre **X6** consiste en une *clause de responsabilité*.

Le chiffre **X7** concerne la souscription d’une assurance responsabilité civile.

Les chiffres sont expliqués à la suite de la clause contractuelle type.

**Chiffre X Protection des moyens informatiques contre les cyberattaques et obligation de signaler**

**X1**. Le fournisseur de prestations s’engage à protéger ses moyens informatiques (c’est-à-dire les moyens des technologies de l’information et de la communication, à savoir les applications, les systèmes d’information et les fichiers de données ainsi que les installations, les produits et les services utilisés pour le traitement électronique de l’information) qui peuvent entrer en contact avec l’objet du présent contrat contre les cyberattaques, conformément à l’état actuel de la technique.

Le fournisseur de prestations veille à ce que les activités prédéfinies par le bénéficiaire des prestations soient enregistrées et à ce que ces enregistrements soient analysés en permanence afin de pouvoir détecter et contrer à temps les cyberattaques.

Le fournisseur de prestations est tenu d’empêcher efficacement la concrétisation d’un danger identifié, de l’éliminer immédiatement et d’en informer sans délai le bénéficiaire des prestations.

Le fournisseur de prestations élimine immédiatement et à ses frais les vulnérabilités identifiées (c’est-à-dire les vulnérabilités ou les défauts dans les moyens informatiques qui pourraient permettre une cyberattaque) avant, pendant ou après une cyberattaque.

Par « cyberattaque », on entend tout événement provoqué intentionnellement qui, par l’utilisation de moyens informatiques, compromet la confidentialité, la disponibilité ou l’intégrité des informations ou la traçabilité de leur traitement.

**X2**. Lors du traitement de données et d’informations de la Confédération, le fournisseur de prestations s’engage à respecter les exigences et les dispositions de la loi sur la protection des données (LPD[[8]](#footnote-9)) et de la loi sur la sécurité de l’information (LSI[[9]](#footnote-10)), y compris les ordonnances d’exécution correspondantes, ainsi que de protection informatique de base de la Confédération. Il transfère ces obligations aux tiers qu’il a mandatés (par ex. fournisseurs, sous-traitants et suppléants).

**X3**. Le fournisseur de prestations signale les cyberattaques potentiellement réussies, c’est-à-dire lorsque la confidentialité, la disponibilité, l’intégrité ou la traçabilité des informations de la Confédération sont directement ou indirectement touchées ou compromises, ou que l’intention est d’aboutir à un tel résultat. C’est notamment le cas lorsque les moyens informatiques attaqués ont accès à des moyens informatiques de la Confédération ou lorsque des indices laissent penser que ces attaques ont été menées en vue de préparer d’autres cyberattaques ou qu’elles s’accompagnent d’actes de chantage, de menaces ou de contrainte. Le fournisseur de prestations signale le type et l’exécution d’une telle cyberattaque dans les 24 heures suivant sa découverte. Les parties s’informent mutuellement et en continu du type et de l’exécution de la cyberattaque, des conséquences possibles et réelles, des mesures prévues et mises en œuvre.

Les signalements doivent être adressés aux organismes suivants :

* bénéficiaire des prestations (désigner les interlocuteurs avec leurs coordonnées), et
* Office fédéral de la cybersécurité (OFCS, ex NCSC), via un formulaire en ligne[[10]](#footnote-11)

Si le bénéficiaire des prestations ou l’OFCS le jugent nécessaire pour protéger les données et informations de la Confédération, le fournisseur de prestations leur accorde, ainsi qu’aux tiers auxquels ils font appel pour le traitement de l’incident, un accès immédiat aux analyses, aux rapports d’enquête et aux autres résultats et informations (documents, données, données du journal, objets, etc.) qui permettent d’analyser la cyberattaque et ses conséquences, et de contrer ces dernières.

**X4**. Le fournisseur de prestations fournit tous les six mois au bénéficiaire des prestations, spontanément et sans facturation distincte, des justificatifs relatifs à sa cybersécurité sous forme de (concrétiser et insérer la forme). Si ces justificatifs sont jugés insuffisants ou s’il existe des indices de lacunes en matière de cybersécurité, le bénéficiaire des prestations (ou un tiers mandaté par lui) peut procéder à des audits de cybersécurité auprès du fournisseur de prestations et des tiers qu’il a mandatés. Ces audits sont communiqués X jours ouvrés à l’avance. Chaque partie supporte ses propres coûts liés à de tels audits. Toutefois, si de graves lacunes en matière de cybersécurité sont constatées dans le cadre d’un audit, le fournisseur de prestations prend en charge, outre ses propres coûts et les dépenses engagées pour y remédier, les coûts d’audit supportés par le bénéficiaire des prestations.

**X5**. Le fournisseur de prestations est redevable d’une peine conventionnelle s’il ne remplit pas, ou pas dans les délais, ses obligations de signalement au titre des chiffres X1 à X4 envers le bénéficiaire des prestations, ou s’il n’élimine pas immédiatement les vulnérabilités identifiées ou les défauts constatés. La peine conventionnelle se monte à 10 % de la rémunération totale par infraction, mais au moins à 10 000 francs par cas. Le paiement de la peine conventionnelle ne libère pas le fournisseur de prestations de ses obligations contractuelles. La peine conventionnelle est déduite des éventuels dommages-intérêts.

**X6**. Le fournisseur de prestations répond des dommages causés au bénéficiaire des prestations à la suite d’une cyberattaque et du non-respect des dispositions visées aux chiffres X1 à X4, à moins qu’il ne prouve qu’aucune faute ne lui est imputable.

Évt, introduire un ch. **X7** réglant l’obligation de souscrire une assurance responsabilité civile *(voir ci-dessous les explications correspondantes et la proposition de texte).*

Conférence des achats de la Confédération (CA)

Publication : 1.1.2024[[11]](#footnote-12)

État au 1.3.2024[[12]](#footnote-13)

Les explications figurent sur les pages suivantes.

**Explications relatives à la clause contractuelle type :**

**Explications pour compléter la clause type :**

Lors de l’établissement du contrat, les éléments surlignés en jaune doivent être remplacés par le contenu souhaité. La lettre « X » reprend la numérotation du contrat dans lequel la clause est insérée et doit être adaptée en conséquence.

**ad chiffre 1 :**

Le « fournisseur de prestations » est le partenaire contractuel qui, dans le cadre de l’exécution du contrat, a reçu des données et / ou des informations de l’administration fédérale qui nécessitent une protection contre les cyberattaques, ou en a obtenu l’accès. Lors de l’établissement du contrat, le nom du partenaire contractuel doit être inséré tel qu’il est utilisé dans l’ensemble du contrat.

Le terme « bénéficiaire des prestations » désigne l’unité administrative contractante. L’unité organisationnelle qui signe le contrat avec le fournisseur de prestations est déterminante. Il peut s’agir du service d’achat, du service demandeur ou des deux.

L’obligation du fournisseur de prestations de prendre des mesures de protection vise à empêcher directement ou indirectement la réussite d’une cyberattaque, ou du moins à réduire l’impact de celle-ci. Il s’agit, par exemple, d’assurer la protection des codes et des mots de passe, des informations et des systèmes classifiés, ou d’informations non publiques telles que les plans d’occupation, les plans de construction ou les plans des installations techniques, les données personnelles, les descriptions de processus et les procédures de travail ou les règles d’accès.

La protection doit être assurée conformément à l’état actuel de la technique et en fonction du risque, ce qui, dans chaque cas concret, permet de tenir compte des possibilités techniques et organisationnelles ainsi que, le cas échéant, du caractère raisonnable sur le plan économique. Le fournisseur de prestations supporte les coûts de la protection et de son entretien, ainsi que les coûts de l’élimination des vulnérabilités identifiées avant, pendant ou après une cyberattaque.

Dans le texte du modèle, l’obligation n’est pas délimitée dans le temps, mais s’applique au moins pendant la durée de validité de la relation contractuelle. Si, dans un cas particulier, les risques encourus imposent de protéger les moyens informatiques avant la conclusion du contrat ou après son échéance, les obligations correspondantes doivent être définies et convenues à l’avance avec le fournisseur de prestations (par ex., au cours de la procédure d’appel d’offres, des négociations contractuelles, etc.). Cela concerne notamment les contrats portant sur des systèmes sur lesquels des données ou des informations du bénéficiaire des prestations restent stockées même au-delà de l’échéance du contrat, par exemple jusqu’à leur restitution, leur effacement ou leur destruction (à cet égard, il est recommandé de fixer un délai, à moins que cela ne soit déjà spécifié dans les CG de la Confédération convenues pour la relation contractuelle).

Le champ d’application de ce chiffre peut, le cas échéant, être limité aux systèmes du fournisseur de prestations qui sont pertinents pour la sécurité de l’administration fédérale.

Selon l’art. 5 de la LSI révisée, les cyberattaques sont des cyberincidents provoqués intentionnellement, c’est-à-dire des événements impliquant l’utilisation de moyens informatiques qui ont pour conséquence de compromettre la confidentialité, la disponibilité ou l’intégrité des informations ou à la traçabilité de leur traitement.

Les exemples incluent l’accès non autorisé, la perturbation, la manipulation ou l’utilisation abusive des systèmes et des données de l’intérieur ou de l’extérieur, ou le vol, le traitement illicite ou la destruction d’informations ou de données, ainsi que de toute autre forme d’intrusion illégale commise à cet effet dans les systèmes et les actes associés (voir, en particulier, les art. 143, 143bis,144bis, 147,179novies et 272 à 274 du code pénal (CP[[13]](#footnote-14)).

Cf. également les explications relatives à l’art. 5 dans le message relatif à la modification de la LSI ainsi que les informations de l’OFCS sur la « Cyberstratégie nationale CSN » (sous le lien suivant : [Cyberstratégie nationale CSN (admin.ch)](https://www.ncsc.admin.ch/ncsc/fr/home/strategie/cyberstrategie-ncs.html)).

**Ad chiffre X2 :**

Cette obligation s’applique au fournisseur de prestations et aux tiers qu’il a mandatés (par ex. sous-traitants, suppléants et fournisseurs). Celui-ci garantit la protection des données et des informations mises à disposition ou créées et/ou traitées par lui et/ou les tiers qu’il a mandatés pour la bonne exécution du contrat conformément aux prescriptions. Cela vaut en particulier pour les informations relatives à la sécurité et aux données personnelles.

**Ad chiffre X3 :**

Le contrat doit garantir que les parties sont déliées du secret de fonction pour le signalement d’une cyberattaque ainsi que pour l’échange et la coopération qui s’ensuivent, afin d’éviter les retards consécutifs à une cyberattaque.

Le contrat doit désigner spécifiquement l’interlocuteur chez le bénéficiaire des prestations auquel le fournisseur de prestations doit signaler la cyberattaque (il s’agit généralement du responsable de la sécurité des informations auprès du bénéficiaire des prestations). L’OFCS reçoit également le signalement. Si nécessaire, d’autres destinataires sont également désignés dans le contrat.

Les cas de figure illustrés dans ce chiffre concernent des obligations de signalement individuelles et, dans le cas d’une cyberattaque, ne sont pas cumulatifs.

L’obligation de signalement concerne les cyberattaques susceptibles de compromettre la protection des données ou le fonctionnement des moyens informatiques. Les cyberattaques infructueuses ou inoffensives, telles que les spams en masse ou les balayages de ports, ne sont pas soumises à l’obligation de signalement. Une cyberattaque est réussie si la confidentialité, la disponibilité, l’intégrité ou la traçabilité des informations de la Confédération ne peuvent plus être garanties, que ce soit de manière involontaire ou avec une intention malveillante. Le contrat entre les parties contractantes doit définir le contenu et la nature de ce signalement en tenant compte de la nécessité de protéger les données et les moyens informatiques.

Le signalement doit être fait dans les 24 heures suivant la détection de la cyberattaque[[14]](#footnote-15). Si, dans un cas particulier, un autre délai est indiqué et approprié[[15]](#footnote-16), il est possible de s’écarter du modèle, à condition que les conditions organisationnelles pour la réception et le traitement des signalements soient remplies chez le bénéficiaire des prestations. Seules les informations connues au moment du signalement doivent être communiquées dans le délai convenu ; le signalement peut être complété par la suite.

Le signalement et les échanges ultérieurs entre les parties servent à diffuser rapidement des informations sur le type de cyberattaque et son exécution, ses répercussions éventuelles, les mesures prises et la suite envisagée. Le modèle de l’OFCS pour le signalement de cyberincidents fournit des indications sur la structure et le contenu d’un signalement : [signalement (admin.ch)](https://www.report.ncsc.admin.ch/fr/).

Vous trouverez ici d’autres informations de l’OFCS sur la manière de réagir en cas de cyberattaque :

[Cyberattaque – que faire ? Informations et aide-mémoire (admin.ch)](https://www.ncsc.admin.ch/ncsc/fr/home/infos-fuer/infos-behoerden/vorfall-was-nun/checkliste-ciso.html).

**Ad chiffre X4 :**

La preuve peut être apportée, par exemple, sous la forme de certaines certifications ou de rapports d’audit ; les certificats usuels ou reconnus peuvent être pris en compte. Pour des raisons de sécurité juridique et d’applicabilité, la forme des justificatifs doit être précisée dans la disposition X4 ou dans le contrat (par ex. en annexe).

La fréquence de la fourniture semestrielle des justificatifs peut être adaptée aux circonstances du cas d’espèce ou combinée avec un droit supplémentaire du bénéficiaire des prestations de pouvoir demander des pièces justificatives à tout moment. La fourniture de justificatifs ne donne pas au fournisseur de prestations le droit à une compensation supplémentaire et distincte pour les dépenses et les coûts et associés.

Le bénéficiaire des prestations crée les conditions nécessaires à la réalisation des audits. Il est conseillé de préciser les modalités de l’audit dans le contrat. Dans ce modèle de contrat, la condition préalable à un audit est que les justificatifs soient jugés insuffisants ou qu’il y ait des indices de lacunes en matière de cybersécurité. Cette approche est conforme à la pratique et justifie également le fait que chaque partie supporte ses propres dépenses et coûts résultant de l’audit. Comme variante à cette disposition, il est possible d’introduire un droit général pour le bénéficiaire des prestations de demander et d’effectuer un audit. Dans la pratique, cependant, un droit inconditionnel d’audit à tout moment avec partage des coûts sera difficile à convenir avec le fournisseur de prestations.

Le délai de préavis pour un audit (X jours ouvrés) doit être fixé dans le contrat auquel ce délai s’applique, en fonction des risques et des besoins concrets. À la place de « X », il convient d’inscrire le délai de préavis exact, calculé en jours. Il est également possible d’indiquer une date concrète, en modifiant en conséquence cette partie de phrase. Nous recommandons un délai de préavis de 20 jours ouvrés, car il s’agit d’une pratique courante. Il n’existe cependant pas de règle générale.

Il convient de transférer les coûts au fournisseur de prestations en cas de manquements graves. Les manquements et leur importance dépendent des circonstances spécifiques du cas d’espèce et doivent, dans la mesure du possible, être précisés dans le contrat.

En principe et conformément au chiffre X1, l’obligation d’éliminer immédiatement les vulnérabilités identifiées s’applique. Si nécessaire, le contrat peut spécifier de manière pratique un délai distinct pour la correction des défauts identifiés au cours d’un audit, en fonction du type ou de la catégorie de défauts et des circonstances.

**Ad chiffre X5 :**

La clause sur les peines conventionnelles n’est pas la même que la clause type sur les peines conventionnelles figurant dans les différentes CG de la Confédération. Le montant minimum est plus élevé et s’élève à 10 000 francs. Le montant et le calcul de la peine peuvent être adaptés dans le contrat après évaluation du risque par les services spécialisés compétents. Il est également possible d’inclure dans le contrat une clause sur les peines conventionnelles, à condition qu’elle couvre les cas d’infraction réglementés ici. Pour des raisons de traçabilité, il est conseillé de documenter les motifs de l’adaptation, en particulier dans le cas d’une réduction du montant minimum (accompagnée d’une justification compréhensible de la raison pour laquelle on suppose un faible risque dans le cas spécifique).

**Ad chiffre X6 :**

En principe, la responsabilité couvre tous les dommages résultant des attaques visées au point X1 et d’autres cas de manquements aux dispositions de la clause type. La clause de responsabilité couvre donc les dommages causés par la cyberattaque et les autres dommages subis par le bénéficiaire des prestations en raison du non-respect des dispositions de cette clause type.

C’est au bénéficiaire des prestations qu’il revient de vérifier si ce régime de responsabilité est adapté aux circonstances concrètes et, le cas échéant, de l’adapter.

Cette disposition peut être omise ou doit être adaptée si la responsabilité est réglée ailleurs dans le contrat et que les cas de responsabilité de cette clause contractuelle type y sont inclus (voir également les modèles de contrat de l’Office fédéral des constructions et de la logistique [OFCL], du Centre de compétence pour les marchés publics de la Confédération [CCMP] et des CG de la Confédération), ou si la situation spécifique en matière de risques le permet ou l’exige.

Les conditions de résiliation inscrites dans le contrat doivent garantir que le non-respect des dispositions relatives aux cyberattaques est défini comme un motif de résiliation pour le bénéficiaire des prestations (comme motif de résiliation extraordinaire ou de résiliation pour justes motifs).

**Ad à un éventuel chiffre X7:**

Certaines compagnies d’assurance offrent la possibilité d’assurer les risques liés aux cyberattaques. Dans certains cas et pour les contrats dont l’objet principal est la fourniture de prestations informatiques, il peut être judicieux d’obliger le partenaire contractuel à souscrire une assurance supplémentaire pour couvrir les dommages potentiels. Dans la pratique, il existe des solutions d’assurance très différentes. Pour s’assurer que la couverture d’assurance est appropriée, il est conseillé au bénéficiaire des prestations de demander à examiner les conditions d’assurance applicables avant la souscription par le fournisseur de prestations d’une police d’assurance. Les modalités doivent être définies dans le contrat.

Proposition de l’accord correspondant :

*« X7. Le fournisseur de prestations s’engage à souscrire une assurance responsabilité civile appropriée pour couvrir les risques de cyberattaques et les risques de dommages ainsi qu’à fournir la preuve d’une couverture d’assurance suffisante au moment de la conclusion du contrat. Les conditions d’assurance applicables à la convention d’assurance doivent être soumises à l’examen du bénéficiaire des prestations avant la souscription de la police d’assurance. »*

Dans ce cas, il convient de définir comme critère d’aptitude dans la procédure d’adjudication que, en cas d’attribution du marché, le soumissionnaire est tenu de fournir les justificatifs correspondants à la demande de l’adjudicateur.

\*\*\*\*\*

1. Cette clause type est destinée à tous les bénéficiaires de prestations au sein de l’administration fédérale, en particulier aux adjudicateurs publics responsables de l’acquisition de prestations informatiques. Le régime des compétences en matière de marchés publics est réglé dans l’ordonnance du 24 octobre 2012 sur l’organisation des marchés publics de l’administration fédérale (Org-OMP ; RS**172.056.15**). [↑](#footnote-ref-2)
2. L’objectif et le contenu des dispositions de la clause type ne consistent aucunement à définir contractuellement les exigences minimales relatives aux moyens informatiques et à garantir leur sécurité et leur protection par le prestataire de services. [↑](#footnote-ref-3)
3. Les conditions générales de la Confédération (CG) contiennent des clauses standard relatives au maintien du secret ainsi qu’à la protection et à la sécurité des données (y compris leur restitution, leur effacement et leur destruction). Les CG sont disponibles sur le site Internet de la CA ([www.bkb.admin.ch](http://www.bkb.admin.ch)). [↑](#footnote-ref-4)
4. L’utilisation de la clause contractuelle type dans un contrat ne délie pas de la responsabilité de prendre en compte les procédures de sécurité, les prescriptions, les directives et les exigences relatives à la sécurité des données et de l’information (y compris la protection informatique de base) dans tous les marchés publics de prestations informatiques et, si nécessaire, de convenir contractuellement avec le fournisseur de prestations (voir note de bas de page 5) de mesures allant au-delà de cette clause (par ex. tests d’intrusion). [↑](#footnote-ref-5)
5. Désigné comme « fournisseur de prestations » dans la clause contractuelle type. [↑](#footnote-ref-6)
6. Par exemple, dans les cas où des partenaires contractuels traitent des informations ou des données de la Confédération sans lui fournir de prestations informatiques, comme dans les imprimeries, les cabinets d’avocats, les entreprises de conseil, les agences de traduction, les bureaux d’architectes ou d’études. [↑](#footnote-ref-7)
7. En particulier, si le partenaire contractuel traite des données ou des informations qui sont soumises au secret de fonction ou à d’autres dispositions sur la confidentialité des données ou qu’il faut considérer comme classifiées en vertu des dispositions fédérales sur la protection des informations, il convient d’examiner dans chaque cas d’espèce si les dispositions de la clause contractuelle type doivent être précisées dans le contrat, réglées de manière plus détaillée ou complétées par d’autres dispositions. [↑](#footnote-ref-8)
8. RS **235.1** [↑](#footnote-ref-9)
9. RS **128** [↑](#footnote-ref-10)
10. Disponible sur <https://www.report.ncsc.admin.ch/fr/> [↑](#footnote-ref-11)
11. La présente clause contractuelle type remplace la clause contractuelle type de la CA pour les cyberrisques (état au 9.11.2022). [↑](#footnote-ref-12)
12. Par rapport à la version du 01.01.2024 (disponible uniquement en allemand), la désignation de l’OFCS a été adaptée, des liens ont été mis à jour et un renvoi erroné à deux notes de bas de page a été corrigé. [↑](#footnote-ref-13)
13. RS **311.0** [↑](#footnote-ref-14)
14. Par analogie avec la réglementation de l’art. 74*e* LSI révisée. [↑](#footnote-ref-15)
15. Une clarification et une concertation avec l’OFCS sont recommandées, car le signalement lui est également adressé. [↑](#footnote-ref-16)