**Modello di clausola contrattuale della CA concernente i ciberattacchi**

La Conferenza degli acquisti della Confederazione (CA) ha elaborato per i committenti pubblici[[1]](#footnote-1) dell’Amministrazione federale un modello di clausola contrattuale relativo alle procedure da seguire in caso di ciberattacchi.

Stabilendo contrattualmente tali disposizioni, le parti contraenti contribuiscono alla protezione dei dati e delle informazioni della Confederazione nonché dei sistemi in caso di ciberattacchi, soprattutto per quanto riguarda le attività sensibili sotto il profilo della sicurezza[[2]](#footnote-2).

Nell’ambito della collaborazione con terzi, l’Amministrazione federale è obbligata a garantire il rispetto delle prescrizioni in materia di protezione dei dati e della sicurezza delle informazioni[[3]](#footnote-3). Le unità amministrative sono responsabili della sicurezza informatica del proprio ambito di competenza.

Il presente documento funge da modello per i committenti pubblici dell’Amministrazione federale. Ha lo scopo di concordare misure di protezione dai ciberattacchi, nonché di stabilire la procedura da seguire dopo[[4]](#footnote-4) un ciberattacco contro un fornitore o un fornitore di servizi[[5]](#footnote-5) che gestisce mezzi informatici dell’Amministrazione federale o che tratta nei propri sistemi informazioni e dati della Confederazione degni di protezione. Esso sostiene l’attuazione degli obblighi delle unità amministrative secondo gli articoli 9 capoverso 1 e 10 capoverso 1 LSIn, l’articolo 13 OSIn nonché l’articolo 24 LPD (per quanto riguarda le basi legali citate, vedi le note a piè di pagina 8 e 9).

Si tratta di una disposizione contrattuale a sé stante, articolata in vari numeri che può essere generalmente ripresa nel caso di prestazioni informatiche, ma anche in altri ambiti[[6]](#footnote-6) come elemento del contratto[[7]](#footnote-7).

Le spiegazioni a complemento del modello di clausola contrattuale sono intese ad agevolarne la comprensione e a concretizzarne l’applicazione, tuttavia non sono parte integrante del contratto.

Per stabilire se sia opportuno convenire le disposizioni del modello di clausola contrattuale sono determinanti soprattutto le analisi del bisogno di protezione e quelle dei rischi effettuate dai servizi specializzati competenti, la classificazione delle informazioni nonché i livelli di sicurezza dei mezzi informatici. In caso di necessità fungono da base per valutare se e quali numeri del modello di clausola contrattuale occorre integrare nel contratto. Conformemente allo scopo del modello di clausola contrattuale, nel contratto occorre integrare almeno le disposizioni dei numeri X1–X3 e, salvo deroghe contrattuali, la responsabilità per violazione degli obblighi. Ai fini della promozione del rispetto degli obblighi si possono applicare le disposizioni relative alle pene convenzionali proposte nonché, soprattutto in caso di constatazione di un elevato bisogno di protezione, di un potenziale di rischio o danno, le misure di audit e di fornitura delle prove. Se nel contratto vengono definite ulteriori disposizioni sulla sicurezza dei dati e delle informazioni, i contenuti del modello di clausola contrattuale devono essere armonizzati con tali disposizioni.

**Riassunto dei contenuti delle disposizioni** nel modello di clausola contrattuale:

Numero **X1** disciplina gli obblighi del fornitore della prestazione per quanto riguarda la *protezione* dei mezzi informatici da ciberattacchi e le *misure* volte a prevenire ed eliminare pericoli e vulnerabilità, definendo inoltre il concetto di «*ciberattacco*».

Numero **X2** obbliga il fornitore della prestazione a rispettare le pertinenti *basi legali* e *direttive* nonché a trasferire tali obblighi a terzi da lui incaricati.

Numero **X3** disciplina l’*obbligo di segnalare* ciberattacchi.

Numero **X4** obbliga il fornitore di prestazioni a *comprovare* la sua cibersicurezza e autorizza il beneficiario della prestazione a svolgere degli *audit* presso il fornitore della prestazione.

Numero **X5** contiene disposizioni relative alle *pene convenzionali*.

Numero **X6** consiste in una *clausola di responsabilità*.

Numero **X7** serve per stipulare un’*assicurazione di responsabilità civile*.

I numeri sono spiegati successivamente nel modello di clausola contrattuale.

**Numero X protezione dei mezzi informatici da ciberattacchi e obbligo di segnalazione**

**X1**. Il fornitore della prestazione si impegna a proteggere da ciberattacchi, in modo adeguato ai rischi e conformemente all’attuale stato della tecnica, i suoi mezzi informatici (ovvero mezzi delle tecnologie dell’informazione e della comunicazione, in particolare applicazioni, sistemi d’informazione e raccolte di dati nonché installazioni, prodotti e servizi utilizzati per il trattamento elettronico di informazioni) che potrebbero essere in relazione con il presente oggetto del contratto.

Il fornitore della prestazione garantisce la registrazione delle attività predefinite dal beneficiario della prestazione e la costante valutazione di tali registrazioni, in modo da poter individuare e respingere i ciberattacchi in maniera tempestiva.

Il fornitore della prestazione è obbligato a impedire in modo efficace la realizzazione di un pericolo individuato, a provvedere immediatamente a eliminarlo e a informare senza indugio il beneficiario della prestazione.

Il fornitore della prestazione elimina, immediatamente e a proprie spese, le vulnerabilità individuate (ovvero lacune o errori nei mezzi informatici che potrebbero consentire un ciberattacco) prima, durante o dopo un ciberattacco.

Per «ciberattacco» si intende qualsiasi evento provocato intenzionalmente che, nell’utilizzo di mezzi informatici, compromette la confidenzialità, la disponibilità o l’integrità delle informazioni o la tracciabilità del loro trattamento.

**X2**. Il fornitore della prestazione si impegna a osservare, nell’ambito del trattamento di dati e informazioni della Confederazione, i requisiti e le direttive della legge federale del 25 settembre 2020[[8]](#footnote-8) sulla protezione dei dati (LPD) e della legge del 18 dicembre 2020[[9]](#footnote-9) sulla sicurezza delle informazioni (LSIn), comprese le relative ordinanze esecutive nonché le direttive sulla protezione di base delle TIC della Confederazione. Egli trasferisce tali obblighi a terzi da lui incaricati (ad es. fornitori e sottofornitori, sostituti, subappaltatori).

**X3**. Il fornitore della prestazione segnala ciberattacchi potenzialmente riusciti nei casi in cui vengono ostacolate o compromesse in modo diretto o indiretto la confidenzialità, la disponibilità, l’integrità o la tracciabilità delle informazioni della Confederazione oppure in caso di intenzionalità. Ciò vale in particolare se i mezzi informatici attaccati hanno accesso ai mezzi informatici della Confederazione o se vi sono indizi che tali attacchi siano avvenuti in preparazione per ulteriori ciberattacchi o siano connessi al reato di estorsione, minaccia o coazione. Il fornitore di prestazioni segnala il tipo e l’esecuzione di un simile ciberattacco entro le 24 ore successive all’individuazione. Le parti si confrontano regolarmente sul tipo e sull’esecuzione, sulle ripercussioni possibili ed effettive nonché sulle misure pianificate e adottate.

Le segnalazioni vanno inoltrate al:

* beneficiario della prestazione (indicare le informazioni di contatto) e all’
* Ufficio federale della cibersicurezza (UFCS; ex NCSC) tramite modulo online [[10]](#footnote-10)

A condizione che il beneficiario della prestazione o l’UFCS lo ritenga necessario allo scopo di proteggere dati e informazioni della Confederazione, il fornitore della prestazione accorda loro e a terzi da loro incaricati per l’elaborazione del ciberincidente l’accesso immediato ad analisi, rapporti d’indagine nonché altre constatazioni e informazioni (documenti, dati, dati d’accesso, oggetti ecc.) che consentono di analizzare e contrastare il ciberattacco e le sue ripercussioni.

**X4**. A cadenza semestrale, il fornitore della prestazione fornisce al beneficiario della prestazione, spontaneamente e senza fatturazione separata, prove della sua cibersicurezza sotto forma di (concretizzare e aggiungere la forma). Se tali prove sono giudicate insufficienti oppure se vi sono indizi su lacune per quanto concerne la cibersicurezza, il beneficiario della prestazione (o un terzo da esso incaricato) può svolgere presso il fornitore della prestazione e presso terzi da quest’ultimo incaricati degli audit in materia di cibersicurezza. Simili audit vengono preannunciati X giorni lavorativi in anticipo. Ciascuna parte si assume i propri costi dell’audit. Tuttavia, se nell’ambito dell’audit si dovessero constatare lacune gravi in materia di cibersicurezza, oltre ai propri costi e alle spese per l’eliminazione delle lacune, il fornitore della prestazione si assume anche i costi dell’audit del beneficiario della prestazione.

**X5**. Il fornitore della prestazione deve pagare una pena convenzionale se non adempie, o non entro i termini, gli obblighi di segnalazione di cui ai numeri X1–X4 nei confronti del beneficiario della prestazione nonché se non elimina immediatamente le vulnerabilità individuate e le lacune constatate. Per ogni violazione essa ammonta al 10 per cento della retribuzione totale, ma almeno a 10 000 franchi. Il pagamento della pena convenzionale non esonera il fornitore della prestazione dall’osservanza dei propri obblighi contrattuali. La pena convenzionale è computata in un eventuale risarcimento dei danni.

**X6**. Il fornitore della prestazione risponde per il danno arrecato al beneficiario della prestazione in seguito ai ciberattacchi e all’inosservanza delle disposizioni dei numeri X1–X4, a meno che non provi che non gli è imputabile alcuna colpa.

Eventualmente introdurre il numero **X7** per disciplinare l’obbligo di stipulare un’assicurazione di responsabilità civile *(v. relative spiegazioni più avanti con proposta di testo)*

Conferenza degli acquisti della Confederazione (CA)

Edizione: 1.1.2024[[11]](#footnote-11)

Stato: 1.3.2024[[12]](#footnote-12)

Le spiegazioni figurano sulle pagine seguenti.

**Spiegazioni relative al modello di clausola contrattuale**

**Indicazione sul completamento del modello**

Nella redazione del contratto occorre sostituire le parti evidenziate in giallo con i contenuti desiderati. «X» riprende la numerazione del contratto in cui si inserisce la clausola e va quindi adeguata di conseguenza.

**Numero X1**

Con «fornitore della prestazione» si intende la parte contraente che, ai fini dell’esecuzione del contratto, deve proteggere dai ciberattacchi i dati e/o le informazioni trasmessi dall’Amministrazione federale o per i quali ha ricevuto l’accesso. Nella redazione del contratto occorre indicare la designazione della parte contraente così come viene utilizzata nell’intero contratto.

Per «beneficiario della prestazione» si intende l’unità contraente dell’Amministrazione federale. A essere determinante è l’unità organizzativa che firma il contratto con il fornitore della prestazione. Può trattarsi del servizio d’acquisto, del servizio richiedente o di entrambi.

L’obiettivo dell’impegno del fornitore della prestazione ad adottare misure di protezione è quello di impedire la riuscita diretta o indiretta di un ciberattacco o almeno di limitarne le ripercussioni. In simili casi occorre, ad esempio, proteggere i codici e le password, i sistemi e le informazioni classificati oppure le informazioni non pubbliche come i piani di occupazione, i piani di costruzione o i piani degli impianti tecnici, i dati personali, le descrizioni di processi, le fasi lavorative o le regole di accesso.

La protezione deve essere conforme all’attuale stato della tecnica e adeguata ai rischi. Nel caso concreto ciò permette di tenere conto delle possibilità tecniche e organizzative ed eventualmente anche della ragionevolezza economica. Il fornitore della prestazione si assume i costi derivanti dalla protezione e dal rispettivo mantenimento, come anche quelli per l’eliminazione delle vulnerabilità individuate prima, durante o dopo un ciberattacco.

Nel modello di testo l’impegno non è vincolato a un determinato periodo, ma vale almeno per la durata di validità del rapporto contrattuale. Se, nel caso concreto, i mezzi informatici devono essere protetti già prima e/o dopo la conclusione del contratto in considerazione dei rischi, occorre definire e convenire già in precedenza i rispettivi impegni con il fornitore della prestazione (ad es. al momento del bando, delle trattative contrattuali ecc.). Ciò riguarda in particolare anche i sistemi nei quali rimangono memorizzati dati o informazioni del beneficiario della prestazione anche dopo la fornitura della stessa, ad esempio fino alla sua restituzione, cancellazione o distruzione (a tale proposito si raccomanda di definire una data, tranne che non sia già stata fissata nelle CG della Confederazione convenute per il rapporto contrattuale).

Il campo di applicazione di questo numero può, se opportuno, essere limitato ai sistemi del fornitore della prestazione rilevanti per la sicurezza dell’Amministrazione federale.

Ai sensi dell’articolo 5 della LSIn riveduta, i ciberattacchi sono ciberincidenti provocati intenzionalmente, vale a dire eventi che si verificano nell’utilizzo di mezzi informatici e che compromettono la confidenzialità, la disponibilità o l’integrità delle informazioni o la tracciabilità del loro trattamento.

Si tratta ad esempio di accesso indebito, perturbazioni, manipolazioni o utilizzo abusivo dei sistemi e dei dati dall’interno o dall’esterno, furto, elaborazione illecita o distruzione di dati o informazioni nonché ogni altra intrusione illecita nei sistemi e azioni correlate (cfr. in particolare art. 143, 143bis,144bis, 147,179novies, 272–274 del Codice penale [CP[[13]](#footnote-13)])

A complemento si veda anche il commento all’articolo 5 nel messaggio concernente la modifica della legge sulla sicurezza delle informazioni nonché le informazioni dell’UFCS sulla «Ciberstrategia nazionale CSN» (al seguente link: [Ciberstrategia nazionale CSN (admin.ch)](https://www.ncsc.admin.ch/ncsc/it/home/strategie/cyberstrategie-ncs.html)).

**Numero X2**

L’impegno vale per il fornitore della prestazione e per i terzi da esso incaricati (ad es. subappaltatori, sostituti e fornitori). Il fornitore della prestazione garantisce di proteggere, conformemente alle direttive, i dati e le informazioni messi a sua disposizione e/o a disposizione di terzi incaricati e/o prodotti da egli o da terzi incaricati al fine della corretta applicazione del contratto. Questo vale soprattutto se si tratta di dati rilevanti per la sicurezza o di dati personali.

**Numero X3**

Nel contratto bisogna garantire che, per la segnalazione di un ciberattacco e la successiva collaborazione, le parti siano esonerate dal segreto d’ufficio, onde evitare ritardi dopo un simile attacco.

Nel contratto occorre specificare concretamente le informazioni di contatto del beneficiario della prestazione, in modo che il fornitore della prestazione possa inoltrare la sua segnalazione sul ciberattacco (di regola si tratta del responsabile della sicurezza delle informazioni del beneficiario della prestazione). Anche l’UFCS riceve la segnalazione e nel contratto possono essere definiti anche altri destinatari.

Le costellazioni illustrate in questo numero comportano obblighi individuali di segnalazione e, nel caso di un ciberattacco, non sono cumulative.

L’obbligo di segnalazione si riferisce a ciberattacchi che possono compromettere la protezione dei dati o la funzionalità dei mezzi informatici. Non sono soggetti all’obbligo di segnalazione i ciberattacchi non riusciti o non pericolosi, come gli invii di massa di e-mail di spam oppure i port scan. Un ciberattacco è considerato riuscito se non sono più garantite la confidenzialità, la disponibilità, l’integrità o la tracciabilità di informazioni della Confederazione, indipendentemente dal fatto che esso sia avvenuto in maniera intenzionale o indebita. Il contenuto e la forma della segnalazione devono essere definiti nel contratto dalle parti contraenti, in considerazione dell’esigenza di proteggere i dati e i mezzi informatici.

La segnalazione deve avvenire entro le 24 ore successive all’individuazione del ciberattacco[[14]](#footnote-14). Se, in un caso specifico, un altro termine risulta congruo e opportuno[[15]](#footnote-15), è possibile derogare al modello, a condizione che presso il beneficiario della prestazione siano soddisfatte le condizioni organizzative per la ricezione e il trattamento delle segnalazioni. Entro il termine concordato devono essere segnalate solo le informazioni note fino al momento della segnalazione; quest’ultima può essere completata successivamente.

La segnalazione e l’ulteriore scambio tra le parti servono per diffondere rapidamente le informazioni sul tipo di ciberattacco e sulla sua esecuzione, sulle sue possibili ripercussioni, sulle misure adottate e su quelle previste. Il modello dell’UFCS per la segnalazione di ciberincidenti mostra la sua struttura e il suo contenuto: [segnalazione (admin.ch)](https://www.report.ncsc.admin.ch/it/)

Ulteriori informazioni dell’UFCS su come procedere in caso di ciberattacchi sono disponibili qui:

[Attacco informatico - E adesso? Informazioni e lista di controllo (admin.ch)](https://www.ncsc.admin.ch/ncsc/it/home/infos-fuer/infos-behoerden/vorfall-was-nun/checkliste-ciso.html)

**Numero X4**

La prova può essere fornita, ad esempio, sotto forma di determinate certificazioni o di rapporti di audit; possono essere prese in considerazione attestazioni abituali o riconosciute. Ai fini della certezza del diritto e dell’applicabilità, la forma delle prove deve essere definita nella disposizione numero X4, ovvero nel contratto (ad es. come allegato).

Le prove vanno presentate semestralmente, tuttavia la frequenza della loro presentazione può essere adeguata in base alle necessità e alla situazione oppure essere correlata a un diritto supplementare del beneficiario della prestazione di poter richiedere prove in qualsiasi momento. Per il fornitore della prestazione la fornitura della prova non comporta alcun diritto a un indennizzo supplementare e separato per le spese e i costi correlati.

Il beneficiario della prestazione crea le condizioni per l’esecuzione di audit. Si consiglia di concretizzare nel contratto le modalità dell’audit. Nel presente modello di contratto, la condizione per un audit è che le prove siano giudicate insufficienti o che vi sono indizi di lacune in materia di cibersicurezza. Ciò è conforme alla prassi e inoltre giustifica il fatto che ogni parte si assume i propri costi e le spese risultanti dall’audit. Come variante a questa disposizione è inoltre possibile introdurre un diritto generale per il beneficiario della prestazione di ordinare ed eseguire un audit. Tuttavia, nella prassi è difficile convenire con il fornitore della prestazione il diritto a eseguire in maniera incondizionata e in qualsiasi momento un audit con una ripartizione dei costi.

Il termine per il preavviso di un audit (X giorni lavorativi) deve essere fissato di volta in volta nel contratto in cui tale preavviso trova applicazione, in funzione delle necessità e dei rischi concreti. Al posto della «X» occorre indicare il numero preciso di giorni. In alternativa è possibile convenire una data concreta e adeguare la frase di conseguenza. Per esperienza si propone un termine di 20 giorni lavorativi. In tale ambito non esiste però alcuna regola generalizzabile.

Addossare i costi al fornitore della prestazione in caso di lacune gravi risulta appropriato. Le lacune e la loro rilevanza dipendono dalle circostanze concrete del caso specifico e devono essere stabilite, per quanto possibile, nel contratto.

In linea di massima e conformemente al numero X1 vale l’impegno a eliminare immediatamente le vulnerabilità constatate. In caso di necessità, nel contratto è possibile definire in modo conforme alla pratica un termine separato per l’eliminazione delle lacune individuate durante un audit, a seconda del tipo o della categoria della lacuna e della situazione.

**Numero X5**

Le disposizioni relative alle pene convenzionali non corrispondono alla clausola standard delle pene convenzionali di cui nelle varie CG della Confederazione. La somma minima è superiore e ammonta a 10 000 franchi. L’importo e il calcolo della pena possono essere adeguati nel contratto dopo la valutazione dei rischi da parte dei servizi competenti. In alternativa, nel contratto può essere definita anche una disposizione generale relativa alle pene convenzionali, a condizione che essa includa i casi di violazione qui disciplinati. A scopo della tracciabilità si raccomanda di documentare i motivi dell’adeguamento, in particolare in caso di diminuzione della somma minima (dovuta a una valida spiegazione del motivo per cui, nel caso concreto, si presume un rischio esiguo).

**Numero X6**

Di norma, la parte contraente risponde di tutti i danni arrecati a seguito degli attacchi di cui al numero X1 e delle altre inosservanze delle disposizioni del modello di clausola contrattuale. Di conseguenza, la clausola di responsabilità comprende i danni del ciberattacco e gli altri danni arrecati al beneficiario della prestazione a seguito dell’inosservanza delle disposizioni contenute nel modello di clausola.

Il beneficiario della prestazione deve giudicare se tale disposizione in materia di responsabilità risulta appropriata nella situazione concreta ed eventualmente adeguarla.

Questa disposizione può essere tralasciata o deve essere adeguata se la responsabilità è disciplinata in un altro numero del contratto, dove sono trattati i casi di responsabilità del presente modello di clausola contrattuale (cfr. anche i modelli di contratto dell’Ufficio federale delle costruzioni e della logistica [UFCL] e del Centro di competenza per gli acquisti pubblici della Confederazione [CCAP] nonché le CG della Confederazione), oppure se la situazione di rischio specifica lo permette o lo richiede.

Nei requisiti di disdetta del contratto occorre accertarsi che l’inosservanza delle disposizioni relative ai ciberattacchi sia definita come motivo di disdetta per il beneficiario della prestazione (quale motivo di disdetta straordinario o per motivi gravi).

**Eventuale numero X7**

Determinate imprese di assicurazione offrono la possibilità di assicurare i rischi legati ai ciberattacchi. Nel caso specifico e nei contratti che vertono sulla fornitura di prestazioni informatiche può essere opportuno obbligare la parte contraente a stipulare un’assicurazione supplementare in base al danno potenziale. Nella prassi vengono offerte soluzioni assicurative molto diverse. In considerazione dell’adeguatezza della copertura assicurativa, prima di stipulare l’assicurazione si consiglia di sottoporre per controllo al beneficiario della prestazione le condizioni assicurative applicabili. Le modalità vanno definite nel contratto.

Proposta di un accordo corrispondente:

*«X7. «Il beneficiario della prestazione si impegna a stipulare un’assicurazione di responsabilità civile adatta a coprire i rischi legati ai ciberattacchi e il rischio di danni nonché a comprovare, al momento della conclusione del contratto, di disporre di una copertura assicurativa sufficiente. Le condizioni assicurative applicabili al rapporto assicurativo devono essere sottoposte per controllo al beneficiario della prestazione prima di stipulare l’assicurazione.»*

In questo caso, come criterio di idoneità nella procedura di aggiudicazione occorre definire che, in caso di aggiudicazione, l’offerente può essere obbligato a fornire le rispettive prove su richiesta del committente.

\*\*\*\*\*

1. Il presente modello di clausola contrattuale è a disposizione di tutti i beneficiari di prestazioni dell’Amministrazione federale, in particolare dei committenti pubblici responsabili dell’acquisto di prestazioni TIC. La ripartizione delle competenze in materia di acquisti è disciplinata nell’ordinanza del 24 ottobre 2012 concernente l’organizzazione degli acquisti pubblici dell’Amministrazione federale (OOAPub; RS **172.056.15**). [↑](#footnote-ref-1)
2. Le presenti disposizioni modello non contemplano nei contenuti e negli scopi né l’indicazione contrattuale dei requisiti minimi per i mezzi informatici né la garanzia della loro sicurezza e protezione da parte del fornitore della prestazione. [↑](#footnote-ref-2)
3. Le condizioni generali di contratto della Confederazione (CG) contengono clausole generali in materia di tutela del segreto, della protezione e sicurezza dei dati (compresa la restituzione, la cancellazione e la distruzione dei dati). Le CG della Confederazione sono disponibili sulla pagina web della CA ([www.bkb.admin.ch](https://www.bkb.admin.ch/bkb/it/home.html)). [↑](#footnote-ref-3)
4. L’accordo contrattuale del modello di clausola non dispensa dall’obbligo di tenere conto, in tutti gli appalti pubblici relativi a prestazioni informatiche, delle procedure di sicurezza, delle prescrizioni, delle direttive e dei requisiti in relazione alla sicurezza dei dati e delle informazioni (compresa la protezione di base delle TIC) e, laddove necessario, di convenire contrattualmente con il fornitore della prestazione (v. nota a piè di pagina 5) misure al di fuori del presente modello di clausola contrattuale (ad es. test di sicurezza «penetration test»). [↑](#footnote-ref-4)
5. Designato come «fornitore della prestazione» nel modello di clausola contrattuale. [↑](#footnote-ref-5)
6. Nei casi in cui le parti contraenti elaborano informazioni o dati della Confederazione senza però fornire prestazioni informatiche a quest’ultima, ad esempio tipografie, studi legali, società di consulenza, agenzie di traduzione, studi di architettura o uffici di pianificazione. [↑](#footnote-ref-6)
7. Se la parte contraente elabora dati e/o informazioni che soggiacciono al segreto d’ufficio o ad altre disposizioni sulla tutela del segreto oppure che sono considerate classificate ai sensi delle vigenti disposizioni sulla protezione delle informazioni della Confederazione, occorre inoltre verificare se, nel singolo caso, le disposizioni del presente modello di clausola contrattuale devono essere concretizzate e definite in modo più dettagliato nel contratto oppure completate con ulteriori disposizioni. [↑](#footnote-ref-7)
8. RS **235.1** [↑](#footnote-ref-8)
9. RS **128** [↑](#footnote-ref-9)
10. disponibile all’indirizzo: <https://www.report.ncsc.admin.ch/it/> [↑](#footnote-ref-10)
11. Il presente modello di clausola sostituisce il modello della CA concernente i ciber-rischi del 1° settembre 2020 (stato: 9.11.2022). [↑](#footnote-ref-11)
12. Rispetto allo stato al 1° gennaio 2024 (disponibile solo in tedesco), il nome dell'UFCS è stato adeguato, i link aggiornati e un riferimento errato a due note a piè di pagina è stato corretto. [↑](#footnote-ref-12)
13. RS **311.0** [↑](#footnote-ref-13)
14. In analogia con la disposizione nell’articolo 74*e* della LISn riveduta. [↑](#footnote-ref-14)
15. Si raccomanda di chiarire e discutere quest’aspetto con l’UFCS, dato che la segnalazione riguarda anche quest’ultimo. [↑](#footnote-ref-15)