TECHNISCHE DATENSCHUTZRICHTLINIE

1. Ziel und Geltungsbereich

Ziel dieser Richtlinie ist es, die Datenschutzbedingungen zu bestimmen, nach denen ConstructSecure seine allgemeine Website betreibt und die Daten nutzt, verarbeitet und speichert, die von registrierten Kunden erfasst werden, die sich für die Vorauswahl von Lieferanten anmelden und diese nutzen.

Diese Richtlinie gilt für die öffentliche Website von ConstructSecure (www.constructsecure.com) und die Netzwerke und IT-Systeme von ConstructSecure, sowie alle Endnutzerdaten, die angemeldete Nutzer im Zusammenhang mit der Nutzung des Systems von CS bereitstellen. Endnutzerdaten umfassen unter anderem Namen sowie geschäftliche E-MailAdressen und Telefonnummern. Nutzer des Moduls CS Inspect können sich auch dafür entscheiden, ihre geschäftlichen Mobilfunknummern bereitzustellen. Sie erhalten dann Meldungen zu Untersuchungsergebnissen. Diese personenbezogenen Endnutzerdaten sind erforderlich, damit Nutzer mit der Anwendung von CS interagieren und diese nutzen können, um sichere Konten einzurichten und Nachrichten und Meldungen des Systems zu erhalten. So lange ein Kundenkonto aktiv ist, ist diese Richtlinie vollständig in Kraft.

Die Datenschutzrichtlinie von CS soll unsere Richtlinien in Bezug auf Cookies, Datenerfassung, Datennutzung, Datenverarbeitung, Datenübertragung, Datenspeicherung und Datenlöschung, die Bekanntgabe von Datenpannen und wie Sie ConstructSecure kontaktieren können, um Ihre Informationen/Ihr Konto zu verwalten oder zu löschen, genau und umfassend erläutern.

2. Besucher und Nutzer

Die Website von ConstructSecure ist öffentlich zugänglich. ***Besucher*** der Website müssen keine persönlichen Informationen eingeben, um sich unsere Seiten anzusehen und mehr über unsere Produkte zu erfahren. ConstructSecure verwendet allerdings Cookies. So können wir die Erfahrung von Besuchern verbessern. Im nachstehenden Abschnitt 4 wird dies näher beschrieben. Beim erstmaligen Besuch der Seite von CS öffnet sich ein Feld, in dem Besucher darüber informiert werden, dass wir Cookies verwenden. In diesem sich öffnenden Textfeld sowie am Ende jeder einzelnen Seite befindet sich zudem ein Link zu dieser Richtlinie.

Nutzer des Systems von ConstructSecure werden im Rahmen dieser Richtlinie definiert als Personen, die bei mindestens einem Softwareprodukt von CS angemeldet sind. Hierzu zählen CS Safety, CS Financial, CS Tracker und/oder CS Inspect. Diese Richtlinie umfasst alle *Endnutzer* auf Kundenseite, die ein Element des Systems von CS nutzen und Mitarbeiter von ConstructSecure.

Nutzer haben zwei Zugangsmöglichkeiten zur webbasierten Anwendung von CS (Administration oder Allgemein) und werden für eine davon eingerichtet. Die beiden standardmässigen Zugriffsberechtigungen unterscheiden sich nur folgendermassen: Administratoren werden anfangs von ConstructSecure im System eingerichtet. Diese wiederum können dann allgemeine Nutzer erstellen und so intern die Liste ihrer Mitarbeiter verwalten, welche die Anwendung von CS je nach spezifischen Geschäftsanforderungen nutzen.

Wenn ein Kunden-Administrator einen allgemeinen Nutzer hinzufügt, stellt der Administrator als einzige identifizierbare Daten lediglich den Namen sowie die geschäftliche E-Mail-Adresse und Telefonnummer des allgemeinen Nutzers bereit. Nachdem ein Kunden-Administrator einen allgemeinen Nutzer mit einem Profil eingerichtet hat, sendet das System von CS automatisch eine E-Mail an den allgemeinen Nutzer. Diese enthält einen Link, über den das eigene Profil des allgemeinen Nutzers formal erstellt wird. Während der Einrichtung verwenden wir einen CAPTCHA (vollautomatischer öffentlicher Turing-Test zur Unterscheidung von Computern und Menschen). Dabei handelt es sich um ein Aufforderung-Antwort-Verfahren. Es dient dazu, Menschen von automatischen Programmen zu unterscheiden. Ein CAPTCHA unterscheidet Menschen von einem Bot, indem eine Aufgabe ausgeführt werden muss. Für die meisten Menschen ist dies einfach. Für Bots ist es gegenwärtig jedoch schwieriger und zeitaufwändiger, die Aufgaben auszuführen. Während der Einrichtung müssen alle Nutzer ein strenges Passwortsystem erstellen und sich daran halten. In der Passwortrichtlinie von CS wird dies eingehend beschrieben.

Endnutzer haben eindeutige Konten, die nie geteilt werden. Mit seinem eindeutigen Benutzernamen und Passwort hat ein allgemeiner Nutzer nur Zugriff auf die spezifischen Daten, die er eingegeben hat. Zudem haben Endnutzer nur Zugriff auf die spezifischen Module der Anwendung von CS (z. B. CS Safety, CS Financial, CS Tracker, CS Inspect) gemäss ihrer vertraglichen Kundenvereinbarung.

3. Referenzdokumente

Für diese Richtlinie sind u. a. die folgenden speziellen Vorschriften und Rahmenordnungen von Bedeutung:

- Norm ISO/IEC 27001. Klauseln A.9.1.1, A.9.1.2, A.9.2.1 – A.9.2.6, A.9.3.1, A.9.4.1, A.9.4.3.
- Datenschutz-Grundverordnung (DSGVO), 25.05.2018
- Datenschutzschild zwischen der EU und den USA und zwischen der Schweiz und den USA, US-Handelsministerium/Europäische Kommission/Schweizer Regierung
- Kalifornisches Verbraucherdatenschutzgesetz (California Consumer Privacy Act, CCPA), 01.01.2020
- Allgemeines Datenschutzgesetz (LGPD) vom 01.02.2020

Diese Datenschutzrichtlinie und die Richtlinie für Informationssicherheit von CS sind übergeordnete Richtlinien und bringen die Verpflichtung in Bezug auf Informationssicherheit von ConstructSecure zum Ausdruck. Die Richtlinie für Informationssicherheit von CS soll auf höchster Ebene eine Verständnis vermitteln für die Grundsätze und Praktiken des Managementsystems für Informationssicherheit (ISMS) von ConstructSecure. Die Richtlinie für Informationssicherheit von CS bietet einen allgemeinen Ansatz für Informationssicherheit. Ergänzend hierzu gibt es die folgenden speziellen technischen Richtlinien. Darin werden die Massnahmen festgelegt, die wir ergreifen, um die Vertraulichkeit und Integrität Ihrer Daten sicherzustellen:

- Nutzungsrichtlinie von CS
- Zugriffsrichtlinie von CS
- Richtlinie von CS für Veränderungsmanagement und sichere technische Entwicklung/Planung
- Clear-Desk- und Clear-Screen-Richtlinie von CS
- Datensicherungsrichtlinie von CS
- Richtlinie von CS zur Dokumenten- und Informationslenkung
- Verschlüsselungsrichtlinie von CS
- Vorfallmanagementrichtlinie von CS
- Richtlinie von CS für Innenrevision und Betriebsprüfungen
- Protokollierungs- und Verfolgungsrichtlinie von CS
- Passwortrichtlinie von CS

Nachstehend sind zudem verschiedene interne Leitfäden von CS aufgeführt. Sie enthalten organisationsbezogene Informationen, die wichtig sind für unsere Informationssicherheit und unsere diesbezügliche Kommunikation mit Mitarbeitern und Kunden:

- Administrativer Leitfaden von CS
- Leitfaden von CS für die Bindung und Betreuung von Kunden/Lieferanten
- Leitfaden von CS für die Notfallwiederherstellung und Geschäftskontinuität
- Leitfaden von CS für die Risikobewertungs- und Risikobehandlungsmethode des Managementsystems für Informationssicherheit
- Leitfaden von CS für den Risikobewertungs- und Risikobehandlungsbericht des Managementsystems für Informationssicherheit
- Mitarbeiterhandbuch von CS
- Handbuch von CS zur Systemarchitektur

4. Cookie-Richtlinie

Auf dem Gerät eines Besuchers oder Nutzers werden manchmal kleine Dateien, so genannte Cookies, platziert. Dies dient der korrekten Funktionsweise der Website von ConstructSecure. Diese Cookies werden in Textdateien auf dem Gerät gespeichert. So „erinnert" sich der Browser an die Präferenzen des Besuchers oder Nutzers (etwa Sprache, Schriftgrösse,

Anmeldung und andere Anzeigepräferenzen), wenn die Website von CS erneut aufgerufen wird. Diese gängige Praxis steht der Verpflichtung von ConstructSecure in keiner Weise entgegen, die Kundendaten weiterhin nach höchsten Standards zu sichern und zu schützen. Mithilfe von Cookies gewährleistet die Website von ConstructSecure, wie die meisten anderen auch, eine einheitliche und gut funktionierende Besucher- und Nutzererfahrung. Ausserdem wird die Ausführung grundlegender Funktionen gewährleistet, sodass sich Nutzer etwa registrieren und angemeldet bleiben können.

Weiterhin kann ConstructSecure mithilfe von Cookies die Interaktion und das Navigieren von Besuchern und Nutzern auf unseren Seiten analysieren, damit wir sie verbessern können. Cookie-bezogene Informationen dienen auch der Erinnerung und Protokollierung von Aktionen angemeldeter Nutzer. Cookies werden nur zu den hier beschriebenen Zwecken verwendet. Insbesondere ermöglicht ConstructSecure keine Verfolgungsmechanismen Dritter, um über einen längeren Zeitraum und auf externen Websites Daten zu erfassen und diese für internetbasierte Werbung zu nutzen. Darüber hinaus markiert ConstructSecure alle Cookies auf besondere Weise mit „HttpOnly". So weiss der Browser, dass nur der Browser Zugriff auf dieses spezielle Cookie hat. Die „HttpOnly"-Kennzeichnung stellt sicher, dass Zugriffsversuche von Angreifern auf das Cookie mit schadhaftem JavaScript grundsätzlich nicht zulässig sind.

Besucher und Nutzer können Cookies von Websites in ihren Browsereinstellungen blockieren. Je nach Browser werden die Einstellungen und Cookies in unterschiedlicher Weise geändert. Auf den folgenden Websites der wichtigsten Browser finden Sie weitere Informationen und Anleitungen dazu, wie man Cookies deaktiviert:

- Internet Explorer (http://support.microsoft.com/gp/cookies/en)
- Mozilla Firefox (http://support.mozilla.com/en-US/kb/Cookies)
- Google Chrome (http://www.google.com/support/chrome/bin/answer.py?hl=en&answer=95647)
- Safari (http://support.apple.com/kb/PH5042)
- Opera (http://www.opera.com/browser/tutorials/security/privacy/)

Man kann nicht nur die Browsereinstellungen ändern, damit keine Cookies platziert werden, sondern auch alle Cookies löschen, die bereits auf einem Gerät gespeichert sind. Besucher oder Nutzer, die diese Option wählen, müssen unter Umständen bei jedem Besuch der Seite von ConstructSecure gewisse Einstellungen manuell ändern. Bestimmte Dienste und Funktionen funktionieren dann möglicherweise überhaupt nicht.

Wen man die Website von ConstructSecure zum ersten Mal besucht, öffnet sich ein Feld, indem man darüber informiert wird, dass ConstructSecure Cookies verwendet.

5. Datenerfassung

Wenn man sich bei der Anwendung von ConstructSecure anmeldet, werden Endnutzerdaten erfasst. Dabei handelt es sich um persönliche Angaben oder personenbezogene Daten. Hierzu zählen vollständige Namen sowie geschäftliche E-Mail-Adressen und Telefonnummern. Nutzer des Moduls CS Inspect können sich auch dafür entscheiden, ihre geschäftlichen Mobilfunknummern bereitzustellen. Sie erhalten dann Meldungen zu Untersuchungsergebnissen. Diese personenbezogenen Endnutzerdaten sind erforderlich, damit Nutzer mit der Anwendung von CS interagieren und diese nutzen können, um sichere Konten einzurichten und Nachrichten und Meldungen des Systems zu erhalten.

6. Datennutzung

Das Managementsystem für Informationssicherheit von ConstructSecure wird intern von unserem technischen Direktor (CTO) geleitet. Er ist unser Verantwortlicher für Informationssicherheit (CISO) gemäss ISO 27001 und unser Datenschutzbeauftragter gemäss der Definition in Artikel 37 der DSGVO. Der CTO etabliert eindeutige Rahmenbedingungen für die Nutzung der Daten von Kunden bei deren Inanspruchnahme unserer Dienste und Systeme und den Schutz von Nutzerdaten. Dies beinhaltet u. a. Folgendes:

- ConstructSecure verarbeitet die Daten von Nutzern des Systems von CS ausschliesslich zu den Zwecken, die im Softwarelizenzvertrag und im Dienstleistungsvertrag für Kunden und/oder im Beteiligungsvertrag für Subunternehmer festgelegt sind. Im Bereich CloudComputing nutzt ConstructSecure Amazon Web Services wie nachstehend in Abschnitt 7 beschrieben;
- ConstructSecure garantiert die Vertraulichkeit der verarbeiteten personenbezogenen Daten gemäss der Definition in den vertraglichen Vereinbarungen und in diesem Dokument;
- ConstructSecure gibt Daten nicht an Dritte weiter und nutz keine dritten Werbeanbieter;
- wie in im administrativen Leitfaden und im Mitarbeiterhandbuch von CS definiert, durchlaufen die Mitarbeiter von ConstructSecure auf jeden Fall eine vollständige Sicherheitsprüfung und werden zum Schutz personenbezogener Daten angemessen geschult;
- Mitarbeiter von ConstructSecure bestätigen und unterzeichnen die im Mitarbeiterhandbuch von CS aufgeführten Geheimhaltungsvorgaben;
- Daten werden stets über das SSL-Protokoll übermittelt oder heruntergeladen;
- wie in der Passwortrichtlinie von CS umfassend definiert, müssen sich Nutzer mit einem Benutzernamen/Passwort anmelden, um auf Daten zuzugreifen;
- wie in der Verschlüsselungsrichtlinie von CS umfassend definiert, werden Dateien beim Hochladen von Daten verschlüsselt und gespeichert, wobei auch gefordert wird, dass jede verschlüsselte Datei einen eigenen Schlüssel hat;

- wie in der Datensicherungsrichtlinie von CS umfassend definiert, werden gespeicherte Sicherungskopien und Protokolle verschlüsselt, wobei auch gefordert wird, dass ConstructSecure keine Zwischenspeicher nutzt.

7. Datenverarbeitung

Wie bereits erwähnt verarbeitet ConstructSecure die personenbezogenen Daten ausschliesslich zu den Zwecken, die im Softwarelizenzvertrag und im Dienstleistungsvertrag für Kunden und/oder im Beteiligungsvertrag für Subunternehmer festgelegt sind. Aus dem administrativen Leitfaden von CS geht zudem hervor, dass ConstructSecure den führenden Anbieter von CloudTechnologie Amazon Web Services damit beauftragt hat, innerhalb von AWS einen logisch isolierten Abschnitt einzurichten, damit wir dort für unser System eine virtuelle private Cloud (VPC) erstellen können. AWS liegt ausserhalb des Geltungsbereichs des Managementsystems für Informationssicherheit von ConstructSecure und einer der Gründe für die Entscheidung für AWS war dessen eigene Zertifizierung gemäss ISO/IEC 27001:2013. Am 18.11.2010 erhielt AWS das Zertifikat #2013-009. Zuletzt wurde es am 27.03.2020 aktualisiert und neu aufgelegt.

Im Rahmen unserer Vereinbarung mit AWS beteiligen wir uns zudem an dessen Auftragsverarbeitungsvertrag (Data Processing Addendum, DPA). Dies ist ein entscheidender Bestandteil unserer Verpflichtung zu Datensicherheit und Datenschutz, denn der Auftragsverarbeitungsvertrag von Amazon ist vollständig konform mit der Datenschutzgrundverordnung, dem Datenschutzschild zwischen der EU und den USA und zwischen der Schweiz und den USA sowie dem kalifornischen Verbraucherdatenschutzgesetz und erfüllt deren Anforderungen voll und ganz. Unser Auftragsverarbeitungsvertrag mit AWS bietet uns Gewissheit in Bezug auf Datensicherheitsvorgaben. Dies beinhaltet u. a. Folgendes:

- AWS verarbeitet Kundendaten nur im Einklang mit Kundenanweisungen;
- AWS hat für sein Netzwerk solide technische und organisatorische Vorkehrungen getroffen und behält diese bei;
- AWS teilt seinen Kunden unverzüglich nach deren Bekanntwerden mit, wenn es zu Sicherheitsvorfällen kommt.

8. Datenübermittlungen

ConstructSecure gibt Daten nicht an Dritte weiter, übermittelt Daten nicht an Dritte und nutzt keine dritten Werbeanbieter.

Die Anwendung von ConstructSecure ist eine SaaS-basierte Anwendung mit Webhosting. Wie bereits erwähnt beauftragt ConstructSecure Amazon Web Services mit Cloud-Diensten. Im Rahmen dessen betreibt AWS für ConstructSecure Server in den USA und Europa (in Frankfurt). Auf diese Weise wird sichergestellt, dass Daten aus Ländern der Europäischen Union (EU) (einschliesslich Island, Liechtenstein, Norwegen und der Schweiz) in einem EU-Land bleiben.

AWS ist konform mit dem Datenschutzschild zwischen der EU und den USA und zwischen der Schweiz und den USA. Beide Zertifizierungen werden als „aktiv" eingestuft und die nächste Zertifizierung ist am 16.01.2021 fällig.

9. Speicherung und Löschung von Daten

ConstructSecure speichert alle Endnutzerdaten im Rahmen eines Kunden- oder Subunternehmervertrags nur, so lange dies rechtmässigerweise erforderlich ist. Spezifische Kundenkonten und personenbezogene Daten werden sofort nach Löschung des Kontos (durch einen Kunden-Administrator oder ConstructSecure) bzw. nach Vertragsende gelöscht. ConstructSecure möchte bei seinen Dienstleistungen sicherstellen, dass Daten nicht versehentlich oder in böswilliger Absicht gelöscht werden. Wenn ein Nutzer etwas löscht, kann es daher etwas dauern, bis Kopien in unserem aktiven System und unserem Sicherungssystem gelöscht werden.

Wie bereits erwähnt kann ein Kunden-Administrator ein im CS-System erstelltes spezifisches Nutzerkonto löschen. Nach Ende eines Kunden- oder Subunternehmervertrags entfernt der CTO alle Zugriffsrechte der damit verknüpften Endnutzerkonten. Er deaktiviert alle Anmeldedaten, entfernt ihre Profile im System und verifiziert, dass keine Zugriffmöglichkeit mehr besteht.

Aus dem Beteiligungsvertrag für Subunternehmer von ConstructSecure geht hervor, dass ConstructSecure von Subunternehmen übermittelte Daten anonymisieren und zusammenfassen kann und dass ConstructSecure alle zusammengefassten Daten ohne Verpflichtung gegenüber dem Subunternehmen besitzt, sie für alle Zwecke nutzen und Dritten mitteilen kann. Zusammengefasste Daten sind anonyme Informationen, für die keine Datenschutzgesetze oder -vorschriften gelten, weil es sich nicht mehr um personenbezogene Daten handelt.

10. Anforderungen der Datenschutzgrundverordnung und Datenschutzschild-Erklärung

Die Implementierung eines mit der Norm ISO 27001 konformen Managementsystems für Informationssicherheit (ISMS) ist ein bewährtes Verfahren. Darüber hinaus sehen Kunden, Subunternehmen und Dritte so, dass Datenschutzvorschriften eingehalten werden. Zudem konnte ConstructSecure durch die Implementierung von ISO 27001 eine solide Rahmenordnung schaffen, die sicherstellt, dass die seit 25.05.2018 geltende europäische Datenschutzgrundverordnung (DSGVO) eingehalten wird.

Um die Konformität mit der DSGVO zu gewährleisten, erfüllt ConstructSecure den Datenschutzschild zwischen der EU und den USA sowie zwischen der Schweiz und den USA wie vom US-Handelsministerium bezüglich der Erfassung, Nutzung und Speicherung der von der Europäischen Union in die Schweiz und die USA übermittelten personenbezogenen Daten dargelegt.
ConstructSecure hat dem US-Handelsministerium die Einhaltung der Grundsätze des

Datenschutzschilds bestätigt. Sollten die Bedingungen der Datenschutzrichtlinien von CS mit den Grundsätzen des Datenschutzschilds kollidieren, gelten die Grundsätze des Datenschutzschilds. Weitere Informationen zum Datenschutzschildprogramm und unserer Zertifizierung finden Sie unter: https://www.privacyshield.gov/.

Im Rahmen der Grundsätze des Datenschutzschilds bestätigt ConstructSecure Folgendes:

- Die Selbstzertifizierung von ConstructSecure unterliegt den Untersuchungs- und Durchsetzungsbefugnissen der Federal Trade Commission (USWettbewerbs- und Verbraucherschutzbehörde);
- ConstructSecure erfasst in begrenztem Umfang personenbezogene Daten wie vorstehend in Abschnitt 5 beschrieben und nutzt diese Informationen nur für die vorstehend in Abschnitt 6 beschriebenen Zwecke;
- Einzelne Nutzer der Anwendung von ConstructSecure sind dazu berechtigt, auf ihre personenbezogenen Daten zuzugreifen und sie zu prüfen, zu korrigieren, zu ändern, zu löschen oder die Nutzung und/oder Offenlegung ihrer personenbezogenen Daten einzuschränken. Nutzer aus der EU und der Schweiz können sich wie alle anderen Nutzer mit ihrem eindeutigen Benutzernamen und Passwort jederzeit sicher beim System von CS anmelden und auf ihre personenbezogenen Daten zugreifen und sie prüfen. Nutzer der Anwendung von ConstructSecure, die ihre personenbezogenen Daten ändern oder löschen oder deren Nutzung und/oder Offenlegung einschränken möchten, können sich unter support@constructsecure.com mit ConstructSecure in Verbindung setzen. In Abschnitt 13 wird näher hierauf eingegangen;
- ConstructSecure gibt Daten nicht an Dritte weiter, übermittelt Daten nicht an Dritte und nutzt keine dritten Werbeanbieter. ConstructSecure bestätigt dennoch, dass Körperschaften, einschliesslich ConstructSecure, die Daten an Dritte weitergeben oder Dritten übermitteln, dafür haften, wenn diese Dritten personenbezogene Daten in mit den Grundsätzen unvereinbarer Weise verarbeiten;
- In Übereinstimmung mit unseren rechtlichen Verpflichtungen und auf rechtmässige Anfrage kann ConstructSecure öffentlichen Behörden personenbezogene Daten zu Zwecken der Strafverfolgung oder der nationalen Sicherheit übermitteln.
- Nutzer aus der EU und der Schweiz sowie alle anderen Nutzer, die Fragen oder Beschwerden bezüglich unserer Verarbeitung personenbezogener Daten gemäss dem Datenschutzschild haben, werden dazu angehalten, sich wie in Abschnitt 13 beschrieben mit ConstructSecure in Verbindung zu setzen. ConstructSecure wird sich so schnell wie möglich und innerhalb von höchstens 30 Tagen nach Erhalt einer Frage oder Beschwerde um Ihre Anfragen kümmern.
- Wenn es ungeklärte Beschwerden zum Datenschutz oder zur Datennutzung gibt, denen wir nicht in zufriedenstellender Weise nachgegangen sind, können Sie sich unter https://www.adr.org/TechnologyServiceskostenlos an unsere externe Schlichtungsstelle American Arbitration Association wenden;

- Nutzer aus der EU oder der Schweiz, die Beschwerden in der oben genannten Weise nicht klären können, haben die Möglichkeit, unter https://www.privacyshield.gov/article?id=How- eine Beschwerde einzureichen und ein verbindliches Schiedsverfahren im Rahmen des Datenschutzschilds zu beantragen.

11. Anforderungen in Kalifornien und Brasilien

ConstructSecure ist konform mit dem seit 01.01.2020 geltenden kalifornischen Verbraucherdatenschutzgesetz (California Consumer Privacy Act, CCPA) und die Lei Geral de Protecão de Dados (LGPD), die am 01.02.20 in Brasilien in Kraft trat. Sollte das kalifornische Verbraucherdatenschutzgesetz (California Consumer Privacy Act, CCPA) oder die LGPD für die Daten eines Nutzers Anwendung finden, wird in Abschnitt 13 dieser Richtlinie beschrieben, welche Verfahren zur Verfügung stehen, damit ein Nutzer sein Recht auf Erhalt von Informationen zu den datenbezogenen Praktiken von ConstructSecure und/oder auf Beantragung der Löschung seiner Daten/seines Kontos ausüben kann.

Personenbezogene Daten eines Nutzers werden von ConstructSecure nicht weitergegeben, verkauft oder übermittelt. ConstructSecure nutzt und verarbeitet personenbezogene Daten nur zu den geschäftlichen Zwecken, die im Softwarelizenzvertrag und im Dienstleistungsvertrag für Kunden, im Beteiligungsvertrag für Subunternehmer und in dieser Richtlinie festgelegt sind.

12. Bekanntgabe von Änderungen dieser Datenschutzrichtlinien oder Datenpannen

ConstructSecure behält sich das Recht vor, die Datenschutzrichtlinie von CS jederzeit zu überarbeiten. Bei wesentlichen Änderungen dieser Datenschutzerklärung veröffentlicht ConstructSecure diese Änderungen auf dem „Blog von ConstructSecure". Dieser ist über unsere Website unter www.constructsecure.comabrufbar. Alle neuen Versionen dieser Richtlinie werden auch sofort erneut auf der Website von ConstructSecure veröffentlicht. Der Zugriff erfolgt direkt über den Link „Datenschutzrichtlinie" am Ende jeder Seite der Website von ConstructSecure.

Darüber hinaus benachrichtigt ConstructSecure Kunden umgehend per E-Mail über etwaige Datenpannen (innerhalb von höchstens 72 Stunden nach Bekanntwerden). Diese Benachrichtigung enthält alle erforderlichen Informationen, die Kunden benötigen, um die Panne ggf. der zuständigen Aufsichtsbehörde zu melden, darunter:

- die Art der Panne und eine Beschreibung der Panne, darunter die Anzahl der betroffenen Nutzer;
- Fehleranalysen und Hauptursachen;
- sofortige Abhilfemassnahmen zur Behebung der Panne und zur Eindämmung der Beeinträchtigungen; und
- weitere vorgeschlagene oder getroffene Abhilfemassnahmen, um zu vermeiden, dass derartige Pannen in Zukunft erneut auftreten.

13. Kontaktaufnahme mit ConstructSecure

Die Postanschrift von ConstructSecure lautet 450 Bedford Street, Suite 2200, Lexington, Massachusetts, 02420.

Fragen oder Beschwerden zu den datenbezogenen Praktiken von ConstructSecure oder Anfragen bezüglich einer Löschung ihrer Daten/Konten können Nutzer unter obenstehender Adresse an den Chief Technology Director oder den Vice President of Compliance richten. Nutzer können sich hierfür auch an die E-Mail-Adresse support@constructsecure.com oder die Telefonnummer 866-817-2210 wenden. Auf unserer öffentlichen Website und nach der Anmeldung von Nutzern im System von ConstructSecure gibt es ebenfalls direkte Links zur E-Mail-Adresse von ConstructSecure.

ConstructSecure beantwortet schriftliche Beschwerden, indem die Person kontaktiert wird, die sich beschwert hat. Im Einklang mit der Dienstgütevereinbarung (DGV) des Kunden- oder Subunternehmervertrags von ConstructSecure gehen wir dabei direkt und zügig auf die Anliegen ein. Im Einklang mit den Grundsätzen des Datenschutzschilds zwischen der EU und den USA und zwischen der Schweiz und den USA und wie aus Abschnitt 10 hervorgeht, arbeitet ConstructSecure bei der Klärung von Beschwerden zur Zufriedenheit von Nutzern und für diese kostenlos falls notwendig mit den zuständigen unabhängigen Behörden zusammen. Hierzu gehören u. a. das US-Handelsministerium, die Federal Trade Commission (US-Wettbewerbs- und Verbraucherschutzbehörde), die Datenschutzbehörden der EU und der Schweizer Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB).

14. Einhaltung der Richtlinie

a. Einhaltungskriterien

Um zu evaluieren, ob dieses Dokument wirksam und angemessen ist, müssen folgende Kriterien berücksichtigt werden:

- Anzahl der Pannen des Systems.
- Anzahl der Kontolöschungen.
- Anzahl der Anfragen bezüglich Informationen zur Datensicherheit und Bearbeitungszeiten.
- Anzahl der Beschwerden zur Datensicherheit und Bearbeitungszeiten.

b. Messung der Einhaltung

Die oben genannten spezifischen Kriterien werden im Rahmen der von ConstructSecure erstellten Comprehensive Compliance Measurement Table des Managementsystems für Informationssicherheit berücksichtigt. Sie ist in Anhang 1 der Richtlinie für Informationssicherheit von CS enthalten. Der technische Direktor (CTO) prüft vierteljährlich anhand der Comprehensive Compliance Measurement Table des Managementsystems für

Informationssicherheit, ob unsere allgemeinen Richtlinie für Informationssicherheit und alle anderen technischen Richtlinien eingehalten werden. Die Ergebnisse der vierteljährlichen Prüfung werden verfolgt, analysiert und im Rahmen der jährlichen Besprechung der Managementprüfung des Managementsystems für Informationssicherheit berücksichtigt.

Neben der förmlichen vierteljährlichen Prüfung wird die Einhaltung auch kontinuierlich gemessen. Hierfür werden verschiedene Methoden herangezogen, darunter u. .a. regelmässige Besichtigungen, Tool-Berichte des Unternehmens und Rückmeldungen an den für die Richtlinie verantwortlichen Mitarbeiter.

Im Rahmen der allgemeinen Mitarbeiterschulung, die im Mitarbeiterhandbuch von CS genauer beschrieben wird, führt ConstructSecure Schulungen zu dieser Richtlinie durch und schafft ein Bewusstsein dafür.

c. Ausnahmen

Der für die Richtlinie verantwortliche Mitarbeiter muss Ausnahmen von dieser Richtlinie vorher genehmigen.

d. Nicht-Einhaltung

Wenn sich herausstellt, dass ein Mitarbeiter vorsätzlich gegen diese Richtlinie verstossen hat, kann dies bis hin zu einer Kündigung geahndet werden.

15. Prüfung und Überarbeitung

Der Verfasser dieser Richtlinie gilt als für die Richtlinie verantwortlicher Mitarbeiter. Wenn die Arbeit dies erfordert, ist er dafür zuständig, sie zu aktualisieren. Zudem findet eine jährliche Prüfung dieser Richtlinie durch den technischen Direktor (CTO) statt. Dies soll sicherstellen, ob sie unter Berücksichtigung entsprechender gesetzlicher Änderungen, organisationsbezogener Richtlinien und/oder vertraglicher Verpflichtungen immer noch angemessen ist.

Alle Änderungen eines Dokuments des Managementsystems für Informationssicherheit gegenüber der letzten Version müssen gemäss den Bestimmungen im administrativen Leitfaden von CS im Dokument nachverfolgt und in roter Textfarbe oder ~~durchgestrichen~~angezeigt werden. Alle früheren Versionen eines Dokuments des Managementsystems für Informationssicherheit werden als Referenz zusätzlich auf der persönlichen Nutzerfestplatte des Vice President of Compliance von CS gespeichert. Die folgende Tabelle enthält den Versionsverlauf dieses Dokuments:

Versionsverlauf	Datum	Verfasser	Genehmiger	Klassifizierung
Version 5	6/8/20 (Datenschutzschild)	S. Kirilenko	D. Milinazzo, K. Sardone	Vertraulich

Version 4	1/13/20 (CCPA-Berücksichtigung)	S. Kirilenko	D. Milinazzo, K. Sardone	Vertraulich
Version 3	5/15/19	S. Kirilenko	D. Milinazzo, K. Sardone	Vertraulich
Version 2	5/15/18 (Cookie-Richtlinie)	S. Kirilenko	D. Milinazzo, K. Sardone	Vertraulich
Version 1	5/15/17	S. Kirilenko	D. Milinazzo, K. Sardone	Vertraulich
Diese Richtlinie wird jährlich vom technischen Direktor (CTO) geprüft.				