



1. Zweck und Anwendungsbereich

Zweck dieser Richtlinie ist es, die Datenschutzbedingungen zu bestimmen, unter denen ConstructSecure seine allgemeine Website betreibt und unter denen das Unternehmen die Daten verwendet, verarbeitet und speichert, die es von registrierten Kunden sammelt, die sich einloggen und die Anbieter-Präqualifizierungsanwendung von ConstructSecure nutzen.

Der Geltungsbereich dieser Richtlinie gilt für die öffentliche ConstructSecure-Website (www.constructsecure.com) sowie alle ConstructSecure-Netzwerke und IT-Systeme und alle Endbenutzerdaten, die von angemeldeten Kunden im Zusammenhang mit der Nutzung des CSSystems bereitgestellt werden. Zu den Endbenutzerdaten zählen unter anderem Namen, geschäftliche E-Mails und geschäftliche Telefonnummern. Benutzer des CS Inspect-Moduls können sich auch dafür entscheiden, ihre geschäftlichen Mobiltelefonnummern anzugeben, um Benachrichtigungen über Inspektionsergebnisse zu erhalten. Diese persönlichen Endbenutzerdaten sind im Rahmen der Interaktion eines angemeldeten Kunden und der Nutzung der CS-Anwendung erforderlich, damit die Benutzer sichere Konten einrichten und Nachrichten und Warnungen vom System empfangen können. Diese Richtlinie ist für die Laufzeit eines aktiven Kundenkontos in vollem Umfang wirksam.

Die CS-Datenschutzrichtlinie soll unsere Richtlinien zu Cookies, Datenerfassung, Datenverwendung, Datenverarbeitung, Datentransfer, Datenaufbewahrung und -löschung, Benachrichtigungen bei Datenschutzverletzungen und wie Sie ConstructSecure kontaktieren können, um Ihre Informationen/Account zu verwalten oder zu löschen, klar und gründlich erklären.

2. Besucher vs. Benutzer

Die ConstructSecure-Website ist frei zugänglich und **Besucher** auf der Website sind nicht erforderlich, um persönliche Informationen einzugeben, damit Sie auf unseren Seiten navigieren und sich über unsere Produkte informieren können. ConstructSecure benutzt jedoch Cookies, um das Besuchererlebnis zu verbessern, wie in Abschnitt 4 weiter unten beschrieben. Erstmalige Besucher der CS-Website werden über ein Pop-up-Banner sofort über unsere Verwendung von Cookies informiert, und es gibt auch einen Link zu dieser Richtlinie, der im Text des Pop-up-Banners und unten auf jeder Seite unserer Website zu finden ist.

Benutzer des ConstructSecure-Systems sind in dieser Richtlinie definiert als Personen, die in einem oder mehreren Softwareprodukten von CS eingeschrieben sind, einschließlich CS Safety, CS Financial, CS Tracker und/oder CS Inspect. Diese Politik erstreckt sich auf die gesamte Kundenseite. **Benutzer** die irgendeinen Aspekt des CS-Systems verwenden, sowie Mitarbeiter von ConstructSecure.



MANAGING YOUR RISK...SMARTER™

CS-Benutzer können mit 1 von 2 Arten des Zugriffes auf die webbasierte CS-Anwendung eingerichtet werden - entweder administrativ oder allgemein. Die einzige standardmäßige Unterscheidung zwischen den beiden Zugangsebenen besteht darin, dass administrative Benutzer zunächst von ConstructSecure im System eingerichtet werden und die Möglichkeit erhalten, allgemeine Benutzer anzulegen, so dass sie intern die Liste ihrer Mitarbeiter verwalten können, die die CS-Anwendung auf der Grundlage ihrer spezifischen Geschäftsanforderungen verwenden werden.

Wenn ein allgemeiner Benutzer von einem Client-Verwalter hinzugefügt wird, sind die einzigen identifizierbaren Daten, die vom Verwalter bereitgestellt werden, der Name, die geschäftliche EMail-Adresse und die Telefonnummer des allgemeinen Benutzers. Sobald ein Kundenadministrator ein Allgemeines Benutzerprofil erstellt hat, wird eine automatische E-Mail vom CS-System an den Allgemeinen Benutzer gesendet, die einen Link zur formellen Erstellung eines eindeutigen Allgemeinen Benutzerprofils enthält. Während dieses Aufbauprozesses verwenden wir einen CAPTCHA-Test (Completely Automated Public Turing test to tell Computers and Humans Apart), bei dem es sich um einen Challenge-Response-Systemtest handelt, der Menschen von automatisierten Programmen unterscheiden soll. Ein CAPTCHA unterscheidet zwischen Mensch und Bot, indem es die Erledigung einer Aufgabe verlangt, die für die meisten Menschen einfach auszuführen ist, für aktuelle Bots jedoch schwieriger und zeitaufwändiger ist. Außerdem müssen alle Benutzer während der Einrichtung ein striktes Passwortsystem erstellen und einhalten, das in der CS-Passwortrichtlinie ausführlich beschrieben ist.

Endbenutzerkonten sind für jeden Benutzer einzigartig und werden nie gemeinsam genutzt. Aufgrund des eindeutigen Benutzernamens und Passworts kann ein allgemeiner Benutzer nur auf die spezifischen Daten zugreifen, die er/sie eingibt. Darüber hinaus haben Endbenutzer nur Zugang zu den spezifischen Modulen der CS-Anwendung (z.B. CS Safety, CS Financial, CS Tracker, CS Inspect), die in ihrem Kundenvertrag definiert sind.

3. Referenzdokumente

Zu den spezifischen Regelungen und Rahmenbedingungen, die für diese Politik relevant sind, gehören unter anderem:

- ISO/IEC 27001 Standard. 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.
- Allgemeine Datenschutzverordnung (GDPR), 25.05.2018
- [EU-U.S. & Schweiz-U.S. Privacy Shield Frameworks, US-Handelsministerium/Europäische Kommission/Schweizer Verwaltung](#)
- [Kalifornisches Verbraucherschutzgesetz \(CCPA\), 01.01.2020](#)
- Allgemeines Datenschutzgesetz (LGPD) vom 01.02.2020



Die übergreifenden Richtlinien, die die Einhaltung der Informationssicherheit durch ConstructSecure beschreiben, sind diese CS-Datenschutzrichtlinie und die CS-Informationssicherheitsrichtlinie. Der Zweck der CS-Informationssicherheitsrichtlinie ist es, ein hochrangiges Verständnis der Prinzipien und der Praxis des Informationssicherheits-Managementsystems (ISMS) von ConstructSecure zu vermitteln. Während die Informationssicherheitspolitik der CS einen allgemeinen Ansatz zur Informationssicherheit bietet, wird sie durch sehr spezifische technische Richtlinien erweitert, die die Maßnahmen definieren, die wir ergreifen, um die Vertraulichkeit und Integrität unserer Daten sicherzustellen.

- CS Richtlinie zur akzeptablen Nutzung
- CS-Zugriffskontrollrichtlinie
- CS Änderungsmanagement & Secure Engineering-/Entwicklung-Richtlinie
- CS Clear Desk- und Clear-Screen-Richtlinie
- CS-Richtlinie zur Datensicherung
- CS Dokument- und Informationskontrollrichtlinie
- CS Verschlüsselungsrichtlinie
- CS Vorfallmanagement-Richtlinie
- CS Interne & Externe Revisionsrichtlinie
- CS Richtlinie zur Protokollierung und Beobachtung
- CS Passwort-Richtlinie

Außerdem gibt es mehrere interne CS-Handbücher, die organisatorische Informationen enthalten, die für unsere Informationssicherheit relevant sind und wie wir diese mit unseren Mitarbeitern und Kunden kommunizieren, inklusive:

- CS Verwaltungshandbuch
- CS Handbuch zur Kunden-/Lieferantenbindung und -unterstützung
- CS Handbuch zur Wiederherstellung im Katastrophenfall und Geschäftskontinuität
- CS ISMS Risikobewertung und Risikobehandlungsmethodik
- CS ISMS-Risikobewertung und Risikobehandlungsbericht
- CS-Mitarbeiterhandbuch
- CS-Handbuch zur Systemarchitektur

4. **Cookie-Richtlinie**

Damit die ConstructSecure-Website richtig funktioniert, werden manchmal kleine Datendateien, so genannte Cookies, auf dem Gerät eines Besuchers oder Benutzers platziert. Diese Cookies werden in Textdateien auf einem Gerät gespeichert, so dass die Präferenzen eines Besuchers oder Benutzers (wie Sprache, Schriftgröße, Anmeldung und andere Anzeigepräferenzen) "gespeichert" werden, wenn die CS-Website anschließend in einem



MANAGING YOUR RISK...SMARTER™

Browser geladen wird. Diese gängige Praxis verringert in keiner Weise das Engagement von ConstructSecure, die höchsten Standards für die Sicherheit und den Schutz der Informationen eines Kunden einzuhalten. Wie die meisten Websites verwendet ConstructSecure Cookies, um eine konsistente und effiziente Erfahrung für Besucher und Benutzer zu gewährleisten und um wesentliche Funktionen auszuführen, wie z.B. die Registrierung und Anmeldung angemeldeter Benutzer.

ConstructSecure kann auch Cookies verwenden, um zu analysieren, wie Besucher und Benutzer mit unseren Websites interagieren und durch sie navigieren, damit wir Verbesserungen vornehmen können. Cookie-bezogene Informationen werden auch dazu verwendet, die Aktionen der angemeldeten Benutzer zu speichern und zu protokollieren. Cookies werden für keinen anderen als den hier beschriebenen Zweck verwendet. Insbesondere ermöglicht die ConstructSecure-Website nicht die Sammlung von Daten durch Tracking-Mechanismen von Drittparteien im Laufe der Zeit und über nicht angeschlossene Websites hinweg zur Verwendung für interessenbezogene Werbung. Darüber hinaus kennzeichnet ConstructSecure alle Cookies mit einem speziellen HttpOnly-Flag, das dem Browser mitteilt, dass auf dieses spezielle Cookie nur der Browser zugreifen darf. Dieses HttpOnly-Flag stellt sicher, dass jeder Versuch eines Angreifers, mit böartigem JavaScript auf das Cookie zuzugreifen, strengstens verboten ist.

Besucher und Benutzer können über ihre Browsereinstellungen alle Cookies von jeder Website blockieren. Beachten Sie, dass die Verfahren zum Ändern von Einstellungen und Cookies von Browser zu Browser verschieden sind. Weitere Informationen zur Deaktivierung von Cookies für die Top-Browser finden Sie in den Anweisungen auf den jeweiligen Websites:

- 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/>)

Zusätzlich zur Änderung der Einstellungen eines Browsers, um das Setzen von Cookies zu verhindern, kann eine Person auch alle Cookies löschen, die bereits auf einem Gerät gespeichert sind. Wenn ein Besucher oder Benutzer diese Option wählt, kann es sein, dass er jedes Mal, wenn er die ConstructSecure-Website besucht, einige Präferenzen manuell anpassen muss und dass einige Dienste und Funktionalitäten überhaupt nicht funktionieren.

Erstmalige Besucher der ConstructSecure-Website werden über ein Pop-up-Banner sofort über die Verwendung von Cookies durch ConstructSecure informiert.



MANAGING YOUR RISK...SMARTER™

5. Datensammlung

Endbenutzerdaten, die als Teil der Registrierung in der ConstructSecure-Anwendung erfasst werden und als persönliche Daten oder persönlich identifizierbare Informationen (PII) kategorisiert werden, umfassen den vollständigen Namen des Benutzers, geschäftliche E-Mails und geschäftliche Telefonnummern. Benutzer des CS Inspect-Moduls können sich auch dafür entscheiden, ihre geschäftlichen Mobiltelefonnummern anzugeben, um Benachrichtigungen über Inspektionsergebnisse zu erhalten. Diese persönlichen Endbenutzerdaten sind im Rahmen der Interaktion eines angemeldeten Kunden und der Nutzung der CS-Anwendung erforderlich, damit die Benutzer sichere Konten einrichten und Nachrichten und Warnungen vom System empfangen können.

6. Verwendung von Daten

Das ISMS von ConstructSecure wird intern von unserem leitenden Technologie-Officer verwaltet, der als unser Leiter für Informationssicherheit (CISO) gemäß ISO 27001 und als unser Datenschutzbeauftragter gemäß Artikel 37 der GDPR fungiert. Wenn Kunden unsere Dienstleistungen und Systeme nutzen, legt der leitende Technologie-Officer klare Parameter fest, wie ihre Daten verwendet werden und wie die Privatsphäre eines Benutzers geschützt wird, einschließlich, aber nicht beschränkt auf die Art und Weise, wie diese Daten genutzt werden:

- Für Benutzer des CS-Systems verarbeitet ConstructSecure Daten ausschließlich für die Zwecke, die in der Client-Software-Lizenz- und Dienstleistungsvereinbarung und/oder der Subunternehmer-Beteiligungsvereinbarung definiert sind, und nutzt die Amazon Web Services für unser gesamtes Cloud Computing, wie in Abschnitt 7 unten beschrieben;
- ConstructSecure garantiert die Vertraulichkeit der persönlichen Daten, die wie in den Vertragsvereinbarungen und innerhalb dieses Dokuments definiert verarbeitet werden;
- ConstructSecure gibt keine Daten an Dritte weiter und verwendet keine Drittanbieter von Werbung;
- ConstructSecure stellt sicher, dass seine Mitarbeiter vollständig überprüft werden und die entsprechende Schulung zum Schutz persönlicher Daten erhalten, wie im CS-Verwaltungshandbuch und im CS-Mitarbeiterhandbuch definiert;
- Die Mitarbeiter von ConstructSecure erkennen die im CS-Mitarbeiterhandbuch dargelegten Geheimhaltungsanforderungen an und unterzeichnen sie;
- Jeder Datentransfer oder Download erfolgt über das SSL-Protokoll;
- Um auf die Daten zuzugreifen, muss sich der Benutzer mit einem Benutzernamen/Passwort anmelden, der vollständig in der CS-Passwortrichtlinie definiert ist;



MANAGING YOUR RISK...SMARTER™

- Während des Hochladens von Daten werden die Dateien verschlüsselt und so gespeichert, wie in der CS-Verschlüsselungsrichtlinie vollständig definiert, einschließlich der Anforderung, dass jede verschlüsselte Datei ihren eigenen Schlüssel hat;
- Gespeicherte Backups und Protokolle werden verschlüsselt, wie in der CS-Datensicherungsrichtlinie vollständig definiert, einschließlich der Anforderung, dass ConstructSecure keinen temporären Speicher verwendet.

7. Datenverarbeitung

Wie oben erwähnt, verwendet ConstructSecure persönliche Daten ausschließlich für die Zwecke, die in der Software-Lizenz- und Dienstleistungsvereinbarung des Kunden und/oder der Teilnahmevereinbarung des Subunternehmers definiert sind. Darüber hinaus, wie im CSVerwaltungshandbuch detailliert beschrieben, schließt ConstructSecure Verträge mit Amazon Web Services, einem führenden Anbieter von Cloud-Technologie, ab, um einen logisch isolierten Abschnitt von AWS zu erstellen, in dem wir eine Virtual Private Cloud (VPC) für unser System erstellen können. Sogleich AWS nicht in den Geltungsbereich des ISMS von ConstructSecure fällt, war einer der Gründe für die Wahl von AWS deren eigene Zertifizierung nach ISO/IEC 27001:2013. Konkret wurde AWS am 18.11.2010 die Bescheinigung Nr. 2013-009 ausgestellt, die zuletzt am 27.03.2020 aktualisiert und neu ausgestellt wurde.

Darüber hinaus sind wir im Rahmen unserer Vereinbarung mit der AWS Vertragspartei ihres Data Processing Addendum (DPA). Dies ist eine entscheidende Komponente unseres Engagements für Datensicherheit und Datenschutz, denn Amazons Datenschutzgesetz ist vollständig konform und erfüllt alle Anforderungen der Allgemeinen Datenschutzverordnung (GDPR), des EU-US- und des SCHWEIZ-US Privacy Shield Frameworks sowie des kalifornischen Verbraucherschutzgesetzes. Unser Datenschutzvertrag mit AWS gibt uns Sicherheit in Bezug auf wichtige Anforderungen an die Datensicherheit, einschließlich, aber nicht beschränkt auf:

- AWS bearbeitet Kundendaten nur in Übereinstimmung mit den Anweisungen des Kunden;
- AWS hat robuste technische und organisatorische Maßnahmen für das AWSNetzwerk eingeführt und wird diese beibehalten;
- AWS benachrichtigt ihre Kunden über einen Sicherheitsvorfall ohne unangemessene Verzögerung, nachdem sie von dem Sicherheitsvorfall Kenntnis erlangt hat.



MANAGING YOUR RISK...SMARTER™

8. Datentransfers

ConstructSecure gibt keine Daten an Dritte weiter oder übermittelt sie an Dritte und nutzt keine Drittanbieter von Werbung.

Die ConstructSecure-Anwendung ist eine SaaS-basierte, web gehostete Anwendung. Wie bereits in vorangegangenen Abschnitten erwähnt, schließt ConstructSecure Verträge mit Amazon Web Services für Cloud-Dienste ab. Als Teil dieses Vertrags unterhält AWS Server für ConstructSecure sowohl in den Vereinigten Staaten als auch in Europa (Frankfurt, Deutschland), um zu garantieren, dass Daten aus Ländern der Europäischen Union (EU) (einschließlich Island, Liechtenstein, Norwegen und der Schweiz) in einem EU-Land aufbewahrt werden. **AWS hält sich sowohl an das EU-US Privacy Shield Framework als auch an das SWISS-US Privacy Shield Framework und beide Zertifizierungen werden als "aktiv" klassifiziert, wobei die nächsten Zertifizierungen am 16.01.2021 fällig sind.**

9. Datenaufbewahrung und -löschung

ConstructSecure behält alle Endbenutzerdaten nur so lange, wie wir einen anhaltenden legitimen Bedarf dazu haben und im Rahmen eines Kunden- oder Subunternehmervertrags arbeiten. Spezifische Benutzerkonten und persönlich identifizierbare Informationen werden sofort nach der Kontolöschung (durch einen administrativen Kundenbenutzer oder durch ConstructSecure) oder bei Vertragskündigung gelöscht. ConstructSecure versucht sicherzustellen, dass unsere Dienste Informationen vor versehentlicher oder mutwilliger Löschung schützen. Daher kann es zu Verzögerungen zwischen dem Zeitpunkt kommen, an dem ein Benutzer etwas löscht, und dem Zeitpunkt, an dem Kopien aus unseren aktiven und Sicherungssystemen gelöscht werden.

Wie bereits oben erwähnt, hat ein administrativer Kundenbenutzer zum Löschen bestimmter Benutzerkonten die Funktion, ein von ihm erstelltes Konto aus dem CS-System zu löschen. Außerdem wird der leitende Technologie-Officer bei Beendigung eines Kunden- oder Untervertragsvertrags die Zugriffsrechte der zugehörigen Endbenutzerkonten entfernen, indem er ihre Anmeldungen deaktiviert, ihre Profile aus dem System entfernt und überprüft, ob der Zugriff beendet wurde.

Wie in der Vereinbarung zur Teilnahme von Subunternehmern von ConstructSecure ausführlich beschrieben, kann ConstructSecure die von den Subunternehmern eingereichten Informationen de-identifizieren und ansammeln, und ConstructSecure ist Eigentümer aller angesammelten Informationen und kann diese für jeden beliebigen Zweck verwenden und sie ohne Verpflichtung gegenüber einem Subunternehmer an Dritte weiterleiten. Gesammelte Informationen sind anonyme Informationen und unterstehen nicht mehr den Datenschutzgesetzen oder -bestimmungen.



MANAGING YOUR RISK...SMARTER™

10. GDPR-Anforderungen und Erklärung zum Privacy Shield

Die Implementierung eines ISO 27001-konformen Informationssicherheits-Managementsystems (ISMS) ist nicht nur eine bewährte Praxis, sondern auch ein wesentlicher Bestandteil des Nachweises der Einhaltung des Datenschutzes gegenüber Kunden, Unterauftragnehmern und Dritten. Zudem hat ConstructSecure durch die Implementierung von ISO 27001 einen starken Rahmen geschaffen, um die Einhaltung der allgemeinen Datenschutzverordnung der Europäischen Union (DSGVO) sicherzustellen, die am 25.05.2018 in Kraft getreten ist.

Um die DSGVO-Einhaltung sicherzustellen, erfüllt ConstructSecure die Anforderungen des EU-USA Privacy Shield Framework und des Schweiz-USA Privacy Shield Frameworks, wie es vom Handelsministerium der Vereinigten Staaten bezüglich der Sammlung, Verwendung und Aufbewahrung von persönlichen Daten, die von der Europäischen Union und der Schweiz in die Vereinigten Staaten transferiert werden, festgelegt wurde.

ConstructSecure hat dem US-Handelsministerium bescheinigt, dass es sich an die Prinzipien des Privacy Shields hält. Bei einem Konflikt zwischen den Bedingungen in der CS-Datenschutzrichtlinie und den Prinzipien des Privacy Shields walten die Prinzipien des Privacy Shields. Um mehr über das Privacy Shield Programm zu erfahren und um unsere Zertifizierung einzusehen, gehen Sie bitte auf: <https://www.privacyshield.gov/>.

Als Teil des Privacy Shield Framework und der Prinzipien zertifiziert ConstructSecure das Folgende:

- Die Selbstzertifizierung von ConstructSecure untersteht der Untersuchungs- und Vollzugsbehörde der Bundeshandelskommission;
- ConstructSecure sammelt limitierte persönliche Daten, wie zuvor in Abschnitt 5 beschrieben, und wir verwenden diese Informationen nur für die zuvor in Abschnitt 6 beschriebenen Zwecke;
- Einzelne Benutzer der ConstructSecure-Anwendung haben das Recht, auf ihre persönlichen Daten zuzugreifen und ihre persönlichen Daten zu überprüfen, zu korrigieren, zu ergänzen, zu löschen oder die Verwendung und/oder Veröffentlichung ihrer persönlichen Daten einzuschränken. Benutzer aus der EU und der Schweiz können sich, wie alle anderen Benutzer auch, jederzeit mit ihrem eindeutigen Benutzernamen und Passwort sicher in das CS-System einloggen, um auf ihre persönlichen Daten zuzugreifen und sie zu überprüfen. Wenn ein Benutzer der ConstructSecure-Anwendung die Verwendung und/oder Veröffentlichung seiner persönlichen Daten ändern, löschen oder einschränken möchte, kann er sich mit ConstructSecure in Verbindung setzen auf support@constructsecure.com wie in Abschnitt 13 ausführlicher beschrieben;
- ConstructSecure gibt keine Daten an Dritte weiter oder übermittelt sie an Dritte und nutzt keine Drittanbieter von Werbung. Jedoch erkennt ConstructSecure an, dass jede Entität, einschließlich ConstructSecure, die Daten an Dritte weitergibt oder überträgt,



MANAGING YOUR RISK...SMARTER™

- haftbar bleibt, wenn diese Dritten persönliche Daten in einer Weise verarbeiten, die nicht mit den Prinzipien;
- ConstructSecure kann, in Übereinstimmung mit unseren gesetzlichen Verpflichtungen und vorbehaltlich einer rechtmäßigen Anfrage, persönliche Daten an öffentliche Behörden für Zwecke der Strafverfolgung oder der nationalen Sicherheit weitergeben;
 - ConstructSecure ermutigt Benutzer aus der EU und der Schweiz sowie alle Benutzer, die Fragen oder Beschwerden darüber haben, wie wir ihre persönlichen Daten unter dem Privacy Shield verarbeiten, uns wie in Abschnitt 13 beschrieben zu kontaktieren. ConstructSecure wird sich bemühen, Ihre Probleme so schnell wie möglich zu lösen, aber nicht später als 30 Tage nach Erhalt einer Frage oder Beschwerde;
 - Wenn Sie ungelöste Beschwerden über den Datenschutz oder die Datennutzung haben, auf die wir nicht zufriedenstellend eingegangen sind, wenden Sie sich bitte kostenlos an unseren in den USA ansässigen Drittanbieter für die Streitschlichtung, die Amerikanische Vereinigung für Schiedsgerichtsbarkeit, unter <https://www.adr.org/TechnologyServices>;
 - Wenn Sie ein Nutzer aus der EU oder der Schweiz sind und nicht in der Lage sind, Beschwerden durch eine der oben genannten Methoden zu lösen, können Sie sich auf ein verbindliches Schiedsgerichtsverfahren in Übereinstimmung mit dem Privacy Shield Framework berufen unter <https://www.privacyshield.gov/article?id=How-to-Submit-aComplaint>.

11. Anforderungen für Kalifornien und Brasilien

ConstructSecure hält sich auch an den California Consumer Privacy Act (CCPA), der am 01.01.2020 in Kraft getreten ist und die Lei Geral de Proteção de Dados (LGPD), die am 01.02.20 in Brasilien in Kraft trat. Wenn der California Consumer Privacy Act (CCPA) or the LGPD auf die Informationen eines Benutzers anwendbar ist, beschreibt Abschnitt 13 dieser Richtlinie den Prozess, der einem Benutzer zur Verfügung steht, um sein Recht wahrzunehmen, Informationen über die Datenpraktiken von ConstructSecure zu erhalten und/oder die Löschung seiner Informationen/seines Kontos zu beantragen.

ConstructSecure teilt, verkauft oder gibt die persönlichen Daten eines Benutzers nicht weiter. ConstructSecure verwendet und verarbeitet persönliche Daten nur für geschäftliche Zwecke, wie in der Softwarelizenz- und Dienstleistungsvereinbarung des Kunden, der Unterauftragnehmer-Beteiligungsvereinbarung und dieser Richtlinie festgelegt.

12. Benachrichtigung über Änderungen an der Datenschutzrichtlinie oder Verstöße bei persönlichen Daten

ConstructSecure behält sich das Recht vor, die CS-Datenschutzrichtlinie jederzeit zu revidieren.



MANAGING YOUR RISK...SMARTER™

Wenn wesentliche Änderungen an diesem Datenschutzhinweis vorgenommen werden, wird ConstructSecure eine Benachrichtigung über solche Änderungen im "ConstructSecure Blog" veröffentlichen, der von unserer Website aus verlinkt ist unter www.constructsecure.com. Außerdem werden alle neuen Versionen dieser Richtlinie sofort auf der Website von ConstructSecure gepostet, auf die über den direkten Link "Datenschutzrichtlinie" zugegriffen werden kann, der sich unten auf jeder Seite der Website von ConstructSecure befindet.

Außerdem benachrichtigt ConstructSecure seine Kunden sofort per E-Mail über jede Verletzung von persönlichen Daten (und niemals später als 72 Stunden, nachdem sie davon Kenntnis erhalten haben). Diese Benachrichtigung wird alle notwendigen Unterlagen beinhalten, damit die Kunden diese Verletzung bei Bedarf der zuständigen Aufsichtsbehörde melden können, einschließlich:

- die Art und Beschreibung der Verletzung einschließlich der Anzahl der betroffenen Benutzer;
- Analyse und Grundursache des Versagens;
- Sofortige Korrekturmaßnahmen, um den Verstoß zu beheben und die negativen Auswirkungen zu lindern; und,
- Andere Korrekturmaßnahmen, die vorgeschlagen oder ergriffen wurden, um zukünftige Verstöße derselben Art und Weise zu vermeiden.

13. ConstructSecure kontaktieren

ConstructSecure befindet sich auf der 450 Bedford Street, Suite 2200, Lexington, Massachusetts, 02420, USA.

Wenn Benutzer Fragen oder Beschwerden zu den Datenpraktiken von ConstructSecure haben oder wenn sie die Löschung ihrer Informationen/ihres Kontos beantragen möchten, können sie sich an den leitenden Technologie-Officer oder den Vizepräsidenten für Einhaltung unter der oben genannten Adresse wenden, per E-Mail unter support@constructsecure.com, oder telefonisch unter 866-817-2210. Direkte Links zur E-Mail-Adresse von ConstructSecure sind auch auf unserer öffentlichen Website und nach dem Einloggen der Benutzer in das ConstructSecureSystem erhältlich.

ConstructSecure reagiert auf schriftliche Beschwerden, indem es sich mit der Person, die die Beschwerde erhoben hat, in Verbindung setzt, um jedes Problem direkt und schnell in Einklang mit der Dienstgütevereinbarung (SLA), das in der Kunden- oder Subunternehmervereinbarung von ConstructSecure dargelegt ist, zu lösen. **Außerdem wird ConstructSecure in Einklang mit den Prinzipien des EU-US- und Schweiz-US Privacy Shield Frameworks und wie in Abschnitt 10 ausführlich dargestellt, mit den entsprechenden unabhängigen Ressourcen-Behörden zusammenarbeiten, einschließlich, aber nicht beschränkt auf, das US-Handelsministerium, die US-Bundeshandelskommission, die EU-Datenschutzbehörden (DPAs) und den Schweizerischen Eidgenössischen Datenschutz- und Informationsbeauftragten (FDPIC), soweit dies notwendig ist,**



MANAGING YOUR RISK...SMARTER™

um alle Beschwerden zur Zufriedenstellung des Benutzers und ohne Kosten für den Benutzer zu lösen.

14. Einhaltung von Richtlinien

a. Kriterien für die Einhaltung

Bei der Bewertung der Effektivität und Adäquatheit dieses Dokuments müssen die folgenden Kriterien berücksichtigt werden:

- Anzahl der Systemverstöße.
- Anzahl der Kontolöschungen.
- Anzahl der Anfragen nach Informationen zur Datensicherheit und Häufigkeit von Lösungen.
- Anzahl der Datensicherheitsbeschwerden und Häufigkeit von Lösungen.

b. Messung der Einhaltung

Die oben aufgezählten spezifischen Einhaltungskriterien sind als Teil einer ISMS Comprehensive Compliance Measurement Table enthalten, die von ConstructSecure erstellt wurde und in der CS Richtlinie zu Informationssicherheit, Anhang 1, enthalten ist. Der leitende Technologie-Officer wird die Einhaltung unserer allgemeinen Richtlinie zu Informationssicherheit und aller anderen technischen Richtlinien durch eine vierteljährliche Überprüfung anhand des ISMS Comprehensive Compliance Measurement Table überprüfen. Die Resultate der vierteljährlichen Überprüfung werden verfolgt, analysiert und als Teil des jährlichen ISMS Management Review Meetings einbezogen.

Zusätzlich zu der formellen vierteljährlichen Überprüfung wird die Einhaltung der Vorschriften auch kontinuierlich mit verschiedenen Methoden gemessen, u.a. durch regelmäßige Besichtigungen, Berichte über Geschäftsinstrumente und Feedback an den Richtlinieninhaber.

Das Training und die Sensibilisierung für diese Richtlinie wird als Teil des gesamten Mitarbeitertrainingsprogramms von ConstructSecure vorgenommen, wie im CSMitarbeiterhandbuch ausführlich beschrieben.

c. Ausnahmen

Jede Ausnahme von der Richtlinie muss im Vorfeld vom Eigentümer der Richtlinie anerkannt werden.

d. Nichteinhaltung



MANAGING YOUR RISK...SMARTER™

Ein Mitarbeiter, bei dem ein mutwilliger Verstoß gegen diese Richtlinie festgestellt wird, kann disziplinarischen Maßnahmen bis hin zur Kündigung des Arbeitsverhältnisses erleiden.

15. Überprüfung und Entwicklung

Der Verfasser dieser Richtlinie wird als Eigentümer angesehen und trägt die Verantwortung für deren Aktualisierung, wenn Änderungen durch das Werk vorgeschrieben werden. Zudem wird der leitende Technologie-Officer eine jährliche Überprüfung dieser Richtlinie vornehmen, um sicherzustellen, dass sie unter Berücksichtigung aller relevanten Änderungen des Gesetzes, der Organisationsrichtlinien und/oder der vertraglichen Verpflichtungen angemessen bleibt.

Wie im CS-Verwaltungshandbuch festgelegt, müssen alle Änderungen an einem ISMSDokument unter Verwendung von "Änderungen nachverfolgen" vorgenommen werden, wobei nur die Überarbeitungen der vorherigen Version sichtbar gemacht werden, indem diese entweder in roter Schrift angezeigt werden oder ~~durch Streichen~~. Außerdem werden zur Referenz alle früheren Versionen eines ISMS-Dokuments auf dem persönlichen Benutzerlaufwerk des CS Vizepräsidenten für Einhaltung aufbewahrt. Die Versionierungsgeschichte für dieses Dokument ist in der folgenden Tabelle festgelegt:

Versionsgeschichte	Datum	Verfasser	Befürworter	Klassifikation
Version 5	6/8/20 (Privacy Shield)	S. Kirilenko	D. Milinazzo, K. Sardone	Vertraulich
Version 4	1/13/20 (CCPA Inklusion)	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 leitenden Technologie-Officer überprüft.				