Datenschutzgesetz

Reiseführer

Version: 1.0

Überarbeitet: Januar 2024

Inhalt

Zusammenfassung

Die Datenschutzgesetze nehmen weltweit rasant zu. Da die Zahl der Datenschutzverletzungen in die Höhe geschnellt ist und die Verbraucher immer bewusster und versierter geworden sind, haben die Regierungen reagiert und neue, strenge Vorschriften erlassen, die regeln, wie Online-Daten erfasst, verarbeitet, gespeichert und verkauft werden.

Es ist unwahrscheinlich, dass dieser Trend nachlässt. Der Erfolg bahnbrechender Gesetze wie der Datenschutz-Grundverordnung (GDPR) in Europa und anderer neuerer Gesetze hat einen Schneeballeffekt ausgelöst, bei dem die Rechtsordnungen zunehmend auf den Fortschritten anderer aufbauen, was zu einer beschleunigten Bewegung hin zu breiten, weitreichenden Datenschutzstandards führt. Prognosen zufolge werden bis 2025 75 % der Weltbevölkerung von modernen Datenschutzvorschriften erfasst sein.

Für Hoteliers bedeuten der zunehmende Umfang und die Strenge der Datenschutzgesetze eine noch nie dagewesene Komplexität in einem ohnehin schon sehr anspruchsvollen Spiel um die Einhaltung von Vorschriften. Unternehmen, die versuchen, die potenziell enormen finanziellen Kosten und den verheerenden Imageschaden einer Nichteinhaltung zu vermeiden, müssen sich nun mit mehreren sich überschneidenden (und potenziell widersprüchlichen) Rechtsvorschriften auseinandersetzen.

Angesichts dieser Situation sollten vorausschauende Hoteliers der Aufklärung und Sensibilisierung Vorrang einräumen. Obwohl es ratsam ist, sich bei bestimmten rechtlichen Fragen auf einen qualifizierten Anwalt zu verlassen, obliegt es auch den Führungskräften des Unternehmens, ein grundlegendes Verständnis der Datenschutzgesetze zu haben, sich des rechtlichen Umfelds, in dem sie tätig sind, bewusst zu sein und entsprechend zu handeln, um in ihren Teams eine starke Datenschutz- und Sicherheitskultur zu schaffen.

Zu diesem Zweck werden in diesem Leitfaden die wichtigsten Konzepte, Anforderungen und Gesetze im Zusammenhang mit dem Datenschutz vorgestellt und erörtert.

Grundlagen

Für Neulinge auf diesem Gebiet kann das Datenschutzrecht unzugänglich und überwältigend erscheinen. Aufgrund seiner weitreichenden Auswirkungen und der juristischen Terminologie wird es oft ausgeklammert oder nur Spezialisten und Anwälten überlassen.

Dies muss nicht der Fall sein.

Die Datenschutzgesetze unterliegen im Grunde genommen logischen und einfachen Grundsätzen.

Um sie zu verstehen, muss man jedoch mit einer Reihe grundlegender, fundamentaler Kenntnisse arbeiten. Die folgenden Begriffe sind wesentlich, um die Bedeutung dieser Gesetze zu erfassen.

Geschützte Daten

Im Mittelpunkt des Datenschutzrechts steht der Schutz bestimmter Arten von Daten, die dazu verwendet werden können, eine Person direkt oder indirekt zu identifizieren, zu kontaktieren, ausfindig zu machen oder Informationen über sie abzuleiten, um das Recht des Einzelnen auf Privatsphäre und Autonomie in Bezug auf seine persönlichen Daten zu schützen.

Diese Art von Daten gehört in der Regel zu einer Kategorie von Informationen, die als *personenbezogene Daten* bezeichnet werden.

Gemäß der Definition in der Datenschutz-Grundverordnung umfassen "personenbezogene Daten" alle Informationen, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen. Beispiele hierfür sind die folgenden:

Identifikatoren Namen, ID-Nummern, SSN, etc.	**Kontaktinformationen** Adressen oder Telefonnummern.	**Demografische Daten** Alter, Geschlecht, ethnische Zugehörigkeit, usw.
Finanzielle Informationen Kreditkartennummern, Bankkonten, Einkommen usw.	**Gesundheitsdaten** Krankenakten, Versicherungsinformationen, genetische Daten.	**Beschäftigungsdaten** Arbeitsgeschichte oder Bewertungen.

Pädagogische Informationen Akademische Zeugnisse, Zertifizierungen oder Ausbildungsnachweise.	**Online-Kennungen** IP-Adressen, Cookies oder RFID-Etiketten.	**Standortdaten** GPS-Daten oder andere geografische Standortinformationen.

In den Vereinigten Staaten wurde in der Vergangenheit häufig der engere Begriff "persönlich identifizierbare Informationen" (PII) verwendet. Mit dem zunehmenden Einfluss des GDPR-Standards haben die modernen Gesetze der Bundesstaaten jedoch häufig den Begriff "personenbezogene Daten" übernommen.

Obwohl die Terminologie in den Datenschutzgesetzen auf der ganzen Welt sehr unterschiedlich sein kann, ist das Kernkonzept häufig gleich - sie beziehen sich alle auf Informationen, die sich auf eine Person beziehen und sie identifizieren können, entweder allein oder in Verbindung mit anderen Daten.

Diese Übereinstimmung spiegelt eine globale Konvergenz hin zu einem breiteren, umfassenderen Verständnis dessen wider, was identifizierbare Informationen im digitalen Zeitalter ausmacht.

Die wichtigsten Akteure

Das Datenschutzrecht betrifft verschiedene Akteure mit unterschiedlichen Rollen, Rechten und Pflichten. Jeder von ihnen hat eine andere Funktion und ist in unterschiedlicher Weise vom Gesetz betroffen.

In der nachstehenden Tabelle sind die üblichen Kategorien von Akteuren und die typische Art und Weise, wie sie vom Datenschutzrecht betroffen sind, aufgeführt.

Kategorie	Definition	Rechtliche Wirkung
Gegenstand der Daten	Identifizierte oder identifizierbare natürliche Person, deren personenbezogene Daten von einem Verantwortlichen oder einem Auftragsverarbeiter verarbeitet werden. Formale Bezeichnung für einen Verbraucher oder Nutzer.	*Rechte*

Datenkontrolleur	Stelle, die die Zwecke und Mittel der Verarbeitung personenbezogener Daten festlegt. Formale Bezeichnung für das Unternehmen oder die sammelnde Einrichtung.	*Zuständigkeiten*
Datenverarbeiter	Stelle, die personenbezogene Daten im Auftrag des für die Datenverarbeitung Verantwortlichen verarbeitet. Der Auftragsverarbeiter handelt nach den Anweisungen des für die Verarbeitung Verantwortlichen. Zum Beispiel ein Cloud-Service-Anbieter oder ein CRM-Anbieter.	*Zuständigkeiten*
Regulierungsbehörde	Durch Datenschutzgesetze eingerichtete Behörden, die die Einhaltung und Durchsetzung überwachen. Im Rahmen der DSGVO hat zum Beispiel jedes EU-Mitglied eine Datenschutzbehörde, die für die Überwachung und Durchsetzung der Verordnung in ihrem Zuständigkeitsbereich verantwortlich ist.	*Keine*

Elemente des Rechts

Jedes Datenschutzgesetz enthält bestimmte gemeinsame Elemente, die seine Funktionsweise bestimmen. Wenn Sie diese kennen, können Sie die Relevanz und die Auswirkungen neuer Gesetze für Ihre Organisation schnell beurteilen.

In der nachstehenden Tabelle sind diese Elemente aufgelistet und die Definitionen für jedes Element angegeben.

Element	Definition
Zeitleiste	Spezifische Daten und Meilensteine innerhalb des Gesetzes. Beachten Sie, dass das Datum des *Inkrafttretens* und das Datum des *Inkrafttretens* unterschiedlich sind.

Rechte	Rechte oder Privilegien, die den betroffenen Personen nach dem Gesetz zustehen.
Anforderungen	Gesetzliche Verpflichtungen für Einrichtungen, die personenbezogene Daten verarbeiten.
Mechanismus zur Durchsetzung der Vorschriften	Verfahren, um gegen Verstöße vorzugehen und die Einhaltung der Vorschriften zu gewährleisten. In der Regel handelt es sich dabei um eine staatliche Durchsetzung durch die Regulierungsbehörden, doch kann auch ein privates Klagerecht vorgesehen sein.
Sanktionen	Sanktionen oder Geldstrafen bei Nichteinhaltung. Dies kann Disziplinarmaßnahmen einschließlich Unterlassungsklagen oder sogar Strafanzeigen umfassen.

Anforderungen

Die Datenschutzgesetze schreiben eine Reihe von Anforderungen vor, die die Art und Weise, wie personenbezogene Daten erhoben, verarbeitet und gespeichert werden, verändern.

Diese Vorschriften stellen sicher, dass Daten in einer Weise behandelt werden, die die Autonomie des Einzelnen respektiert und vor Missbrauch schützt. Der Zweck dieser Gesetze besteht nicht darin, Innovationen zu ersticken oder den Informationsfluss zu behindern, sondern eine Kultur des Datenschutzes zu schaffen, die mit der ethischen Nutzung und den gesellschaftlichen Erwartungen in Einklang steht.

Daten Subjekte
Einzelpersonen/Verbraucher

Datenkontrolleure
Organisationen / Unternehmen

Die in diesen Verordnungen enthaltenen Anforderungen lassen sich in der Regel in zwei Hauptkategorien einteilen. Die erste Kategorie umfasst die Rechte, die den *betroffenen Personen* gewährt werden - den Personen, auf die sich die Daten beziehen. Die zweite Kategorie beschreibt die Pflichten der *für die Datenverarbeitung Verantwortlichen*, d. h. der

Stellen, die den Zweck und die Mittel der Verarbeitung personenbezogener Daten bestimmen.

Zusammen bilden diese Rechte und Pflichten die beiden Säulen, auf denen das Gebäude des Datenschutzrechts steht.

Dieser Abschnitt enthält eine detaillierte Beschreibung der einzelnen Arten.

Rechte der Verbraucher

Viele Datenschutzgesetze räumen den Verbrauchern zusätzliche Rechte ein, die ihre Möglichkeiten zur Kontrolle der Erhebung und Verwendung ihrer Daten verbessern. In diesem Abschnitt werden einige der gebräuchlichsten und wichtigsten Rechte aus den jüngsten Rechtsvorschriften hervorgehoben.

Opt-Out

Opt-out-Rechte für betroffene Personen beziehen sich auf Bestimmungen in Datenschutzgesetzen, die es Einzelpersonen ermöglichen, sich gegen die Erhebung, Verwendung oder Weitergabe ihrer personenbezogenen Daten für bestimmte Zwecke zu entscheiden.

Dieses Recht ist besonders in Bereichen wie dem Direktmarketing von Bedeutung, wo die betroffenen Personen die Möglichkeit haben, zu verhindern, dass Organisationen ihre personenbezogenen Daten für die Zusendung von Werbematerial verwenden.

Das Widerspruchsrecht kann auch für andere Datenverarbeitungstätigkeiten gelten, wie den Verkauf personenbezogener Daten an Dritte oder die Weitergabe zu Forschungszwecken.

Machen betroffene Personen von ihrem Opt-out-Recht Gebrauch, muss der für die Verarbeitung Verantwortliche der Aufforderung innerhalb eines angemessenen Zeitraums nachkommen und die spezifischen Datenverarbeitungsaktivitäten, für die das Opt-out beantragt wurde, einstellen.

Die Datenschutzgesetze können vorschreiben, dass Organisationen klare und einfache Mechanismen für die betroffenen Personen bereitstellen, damit sie ihre Opt-out-Rechte ausüben können, wobei oft verlangt wird, dass die Opt-out-Option ebenso zugänglich und unkompliziert sein muss wie das Verfahren zur Erteilung der Einwilligung.

Verwendung und Änderung von Daten

Nutzungs- und Änderungsrechte sind in vielen Datenschutzgesetzen enthalten, um sicherzustellen, dass der Einzelne die Kontrolle über seine persönlichen Daten behält.

Diese Bestimmungen - zu denen Rechte wie Zugang, Berichtigung und Löschung und mehr gehören - stellen die zentralen Möglichkeiten dar, mit denen Betroffene die Hoheit über ihre Daten ausüben können.

Die Umsetzung dieser Rechte bedeutet einen Wandel hin zu mehr Transparenz und mehr Mitspracherecht des Einzelnen bei der Verwaltung seiner personenbezogenen Daten.

Sie unterstreicht den Einfluss der weltweiten Bewegung zur Anerkennung der Bedeutung persönlicher Daten als Erweiterung der persönlichen Autonomie.

In der folgenden Tabelle sind die üblichen Rechte zur Nutzung und Änderung von Daten, ihre Definitionen und ihre Verbreitung in modernen Datenschutzgesetzen aufgeführt.

Rechts	Definition	Prävalenz
Zugang	Das Recht einer betroffenen Person, von dem für die Verarbeitung Verantwortlichen eine Bestätigung darüber zu erhalten, ob sie betreffende personenbezogene Daten verarbeitet werden, und, falls dies der Fall ist, Zugang zu den personenbezogenen Daten und Informationen über ihre Verarbeitung zu erhalten.	*Weit verbreitet*
Berichtigung	Das Recht einer betroffenen Person, unrichtige personenbezogene Daten berichtigen oder vervollständigen zu lassen, wenn sie unvollständig sind.	*Weit verbreitet*

Löschung	Das Recht einer betroffenen Person, ihre personenbezogenen Daten unter bestimmten Umständen von dem für die Verarbeitung Verantwortlichen löschen zu lassen, z. B. wenn die Daten für den Zweck, für den sie erhoben wurden, nicht mehr erforderlich sind oder wenn die betroffene Person ihre Einwilligung widerruft. Auch bekannt als das "Recht auf Vergessenwerden".	*Weit verbreitet*
Einspruch gegen die automatisierte Verarbeitung	Recht auf Widerspruch gegen Entscheidungen, die ausschließlich auf einer automatisierten Verarbeitung, einschließlich Profiling, beruhen.	*Weniger häufig*
Tragbarkeit	Das Recht, personenbezogene Daten von einem für die Verarbeitung Verantwortlichen an einen anderen in einem strukturierten, allgemein gebräuchlichen und maschinenlesbaren Format zu übermitteln.	*Erhöhung der*

Verpflichtungen des Controllers

Im Rahmen des Datenschutzrechts sind die Verpflichtungen des für die Verarbeitung Verantwortlichen ( ) eine umfassende Reihe von rechtlichen und ethischen Pflichten, die die als für die Verarbeitung Verantwortlichen benannten Stellen übernehmen, wenn sie die Zwecke und Mittel der Verarbeitung personenbezogener Daten festlegen.

Diese Verantwortlichkeiten sollen die Rechenschaftspflicht durchsetzen und sicherstellen, dass die für die Datenverarbeitung Verantwortlichen nicht nur im Rahmen der Legalität,

sondern auch unter Wahrung der Privatsphäre und der Autonomie der betroffenen Personen handeln.

In diesem Abschnitt werden die häufigsten und folgenreichsten Arten von Verpflichtungen erläutert.

Datenschutz-Hinweise

Datenschutzhinweise sind formelle Mitteilungen, die Einzelpersonen darüber informieren, wie ihre personenbezogenen Daten von einer Einrichtung erfasst, verarbeitet und verwaltet werden.

Sie dienen dazu, die Transparenz der Datenverarbeitungstätigkeiten zu gewährleisten und die Datenschutzpraktiken des für die Datenverarbeitung Verantwortlichen klar und deutlich darzulegen. Sie stellen sicher, dass Einzelpersonen über die Verarbeitung ihrer personenbezogenen Daten informiert sind und ihre Rechte in Bezug auf diese Daten kennen.

Bekanntmachungen können sich auf verschiedene Arten von Tätigkeiten beziehen. In der nachstehenden Tabelle sind die üblichen Formen aufgeführt, und es wird angegeben, ob sie in modernen Datenschutzvorschriften häufig vorkommen.

Typ	Definition	Gemeinsames Erfordernis
Benachrichtigung über Datenschutzverletzungen	Übermittlung an Einzelpersonen und Behörden im Falle einer Datenschutzverletzung, die ein Risiko für die betroffenen Personen darstellt.	✓
Ableitender Hinweis	Hinweise auf Daten, die aus der Analyse der gesammelten Daten abgeleitet oder abgeleitet wurden.	✗

Erste Bekanntmachung	Sie werden zum Zeitpunkt der Erhebung personenbezogener Daten bereitgestellt und geben an, wie und warum die Daten verarbeitet werden.	✓
Interner Hinweis	Mitteilungen innerhalb einer Organisation über allgemeine Datenverarbeitungspraktiken, die sich nicht speziell an die betroffenen Personen richten.	✗
Aktualisierte Mitteilung zur Politik	Wird bei wesentlichen Änderungen der Datenverarbeitungstätigkeiten oder -richtlinien herausgegeben.	✓
Hinweis zur Vermarktung durch Dritte	Spezifische Offenlegungen gegenüber Einzelpersonen bezüglich der Verwendung ihrer Daten für die Vermarktung durch Dritte, wenn die Daten nicht mit dem Vermarkter geteilt wurden.	✗

Zustimmung der Verbraucher

Das Erfordernis der Zustimmung des Verbrauchers ist ein zentrales Element in den meisten Datenschutzgesetzen und dient als Eckpfeiler der Autonomie des Nutzers über seine persönlichen Daten.

Die Einwilligung ist definiert als eine frei gegebene, spezifische, informierte und unzweideutige Angabe der Zustimmung der betroffenen Person zur Verarbeitung ihrer personenbezogenen Daten.

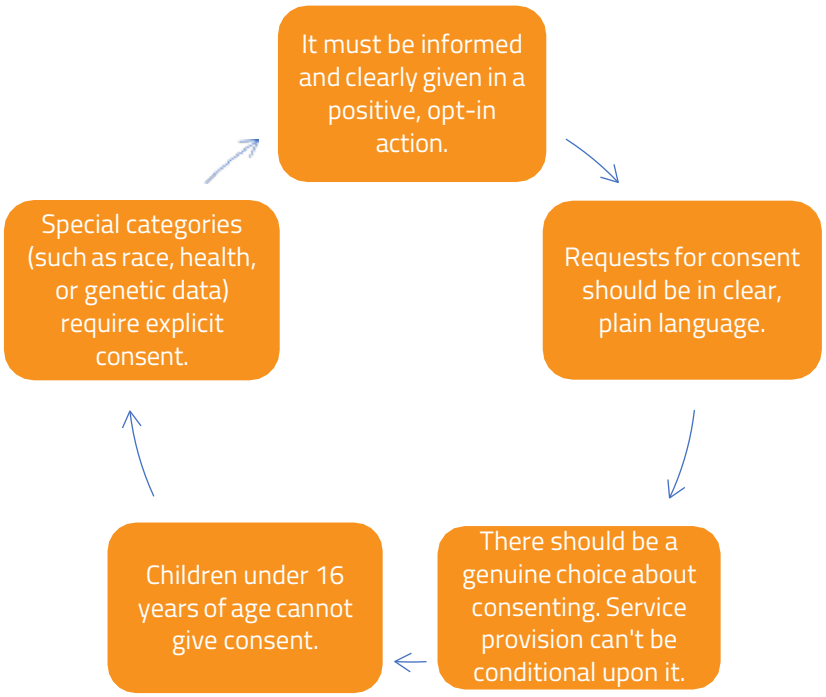
Das bedeutet, dass der Einzelne eine klare Entscheidung darüber treffen können muss, ob und für welche Zwecke seine Daten verwendet werden, ohne dass er in irgendeiner Form gezwungen, unter unzulässigen Druck gesetzt oder getäuscht wird.

Damit die Einwilligung gültig ist, muss sie durch eine bestätigende Handlung gegeben werden, die Zustimmung bedeutet, wie z. B. das Ankreuzen eines Kästchens auf einer Website, die Auswahl technischer Einstellungen oder eine andere Erklärung, die eindeutig die Zustimmung zur vorgeschlagenen Verarbeitung personenbezogener Daten signalisiert. Schweigen, angekreuzte Kästchen oder Inaktivität stellen nach strengen Datenschutzregelungen wie der DSGVO im Allgemeinen keine gültige Einwilligung dar.

Die betroffenen Personen müssen in angemessener und transparenter Weise über den Umfang und die Folgen der Datenverarbeitung, in die sie einwilligen, informiert werden. Dazu gehört, wer die Daten sammelt, welche Daten gesammelt werden, wie sie verwendet werden und ob sie an Dritte weitergegeben werden.

Bei sensiblen Datenkategorien, zu denen Informationen über Gesundheit, Rasse, sexuelle Orientierung, religiöse Überzeugungen usw. gehören, sind die Anforderungen an die Zustimmung in der Regel strenger und erfordern eine ausdrückliche Zustimmung.

Das Erfordernis der Zustimmung spiegelt das übergreifende Ziel der Datenschutzgesetze wider, dem Einzelnen die Kontrolle über seine personenbezogenen Daten zu geben und sicherzustellen, dass Einrichtungen, die Daten erheben und verarbeiten, dies mit der ausdrücklichen Zustimmung des Einzelnen tun.



Schlüsselkriterien für die Zustimmung der Verbraucher

Zweck Beschränkungen

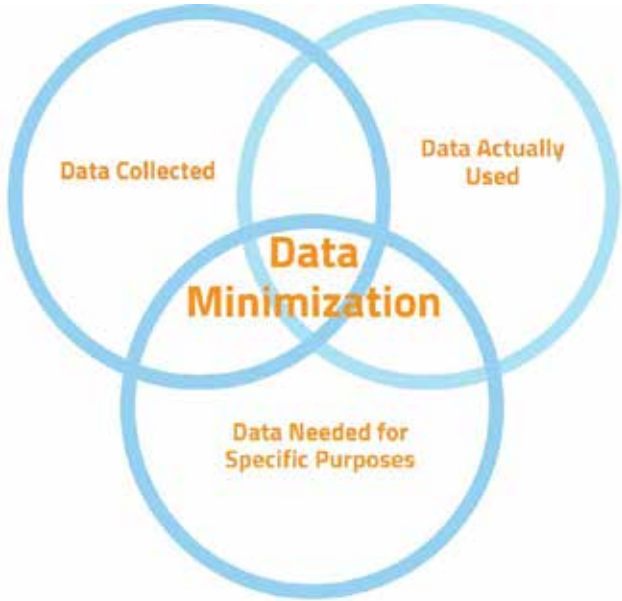
Zusätzlich zu den genauen Anforderungen enthalten viele Datenschutzgesetze Grundsätze, die als übergreifende Leitlinien für ethisches und rechtliches Verhalten dienen. Ein solches Beispiel ist der Grundsatz der "Zweckbindung", der erstmals in der Datenschutz-Grundverordnung festgelegt wurde (Artikel 5 Absatz 1 Buchstabe b)).

Vereinfacht ausgedrückt, besagt dieser Grundsatz Folgendes:

> *"Personenbezogene Daten sollten nur für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und nicht in einer Weise weiterverarbeitet werden, die mit diesen Zwecken unvereinbar ist."*

Dieser Grundsatz stellt sicher, dass Organisationen die Gründe für die Verarbeitung von Daten transparent machen und sie daran hindern, die Daten für neue, nicht damit zusammenhängende oder unrechtmäßige Zwecke zu verwenden, ohne die Einwilligung der betroffenen Person einzuholen oder eine andere legitime Grundlage nach dem geltenden Recht zu schaffen.

Die Zweckbindung trägt dazu bei, das Vertrauen der betroffenen Personen zu erhalten und die Integrität der Datenverarbeitungsaktivitäten zu bewahren.



Datenminimierung visualisiert

DPIA

Eine Datenschutz-Folgenabschätzung (Data Protection Impact Assessment, DPIA) ist eine systematische und umfassende Analyse, wie sich ein bestimmtes Projekt oder System auf die Privatsphäre der betroffenen Personen auswirken wird.

Datenschutzfolgenabschätzungen sind häufig in den Datenschutzgesetzen vorgeschrieben, um die Datenschutzrisiken eines Projekts zu ermitteln und zu minimieren.

So können Gesetze DPIAs verpflichtend vorschreiben, wenn bestimmte Auslöser auftreten, wie z. B. eine Verarbeitung, die eine systematische und umfassende Bewertung persönlicher Aspekte auf der Grundlage automatisierter Entscheidungsfindung beinhaltet, eine groß angelegte Verarbeitung sensibler Daten, eine umfassende Überwachung öffentlicher Bereiche oder andere risikoreiche Ereignisse.

Umweltverträglichkeitsprüfungen laufen als standardisierte Prozesse ab. Ihre genaue Durchführung kann variieren, aber es ist hilfreich, sie als vier Phasen zu verstehen:

Prozess der Datenschutz-Folgenabschätzung

- **Phase 1 - Vorbereitung und Planung**

In der Anfangsphase wird festgestellt, ob eine Datenschutz-Folgenabschätzung notwendig ist, ihr Umfang festgelegt und geplant, wie sie durchgeführt werden soll. Sie umfasst die Ermittlung der Datenverarbeitungstätigkeiten und der Zwecke, für die personenbezogene Daten verarbeitet werden.

- **Phase 2 - Risikobewertung**

In der zweiten Phase werden die potenziellen Risiken für die Rechte und Freiheiten der betroffenen Personen, die sich aus den Tätigkeiten des Unternehmens ergeben könnten, ermittelt und bewertet. Dabei werden die Art, der Umfang, der Kontext und die Zwecke der Verarbeitung sowie die Wahrscheinlichkeit und Schwere der Risiken berücksichtigt.

- **Phase 3 - Entwicklung einer Minderungsstrategie**

Auf der Grundlage der Risikobewertung werden in der dritten Phase Maßnahmen zur Risikominderung festgelegt. Dazu gehört die Entscheidung über Maßnahmen zur Vermeidung oder Verringerung der Auswirkungen der ermittelten Risiken, die Gewährleistung des Datenschutzes und die Einhaltung der geltenden Gesetze.

- **Phase 4 - Dokumentation und Integration**

In der letzten Phase werden der DPIA-Prozess und seine Ergebnisse dokumentiert. Im DPIA-Bericht werden die Risiken und Maßnahmen zur Risikominderung aufgeführt. Falls erforderlich, kann die DPIA an eine Aufsichtsbehörde gemeldet werden.

Gesetze

Das Interesse am Datenschutz hat weltweit zugenommen.

Seit der Verabschiedung des bahnbrechenden GDPR-Gesetzes in Europa haben Länder auf der ganzen Welt zunehmend die Bedeutung des Schutzes von Verbraucherdaten erkannt und Maßnahmen ergriffen, um Unternehmen zu einem ordnungsgemäßen Umgang mit diesen Informationen zu verpflichten.

Wie unten dargestellt, verfügen die meisten Länder inzwischen über nationale Datenschutzgesetze:

Datenschutzgesetz auf Länderebene, 2024

GDPR

Die Datenschutz-Grundverordnung (DSGVO) ist eine Verordnung der Europäischen Union (EU), die die Privatsphäre und die personenbezogenen Daten von EU-Bürgern schützt, indem sie Richtlinien für die Erhebung, Verarbeitung und Speicherung personenbezogener Daten durch Organisationen und Unternehmen festlegt.

Zum Zeitpunkt ihrer Verabschiedung war sie eine bahnbrechende Errungenschaft. Sie setzte neue ehrgeizige Standards für den Datenschutz (z. B. Zustimmungserfordernisse für die Datenverarbeitung, Anforderungen an den Datenschutzbeauftragten und Vorschriften zur Datenminimierung) und nutzte das geopolitische und wirtschaftliche Gewicht der EU, um die Debatte über Verbraucherrechte und den Schutz der Privatsphäre für immer zu prägen.

Seine Auswirkungen sind global. Mit einer Reichweite, die sich auf Unternehmen auswirkt, die vollständig außerhalb der EU tätig sind (bekannt als "Extraterritorialität"), sind Unternehmen auf der ganzen Welt von dem Gesetz betroffen. In den Jahren nach ihrer Verabschiedung hat die GDPR die letzten Gesetze in anderen Ländern stark beeinflusst, wie z. B. das CPRA in Kalifornien und PIPEDA in Kanada.

Die Bedeutung der Datenschutzgrundverordnung kann gar nicht hoch genug eingeschätzt werden.

Zu den wichtigsten Anforderungen der GDPR gehören:

1. **Rechtmäßigkeit, Fairness und Transparenz**

Personenbezogene Daten müssen rechtmäßig, nach Treu und Glauben und in einer transparenten Weise gegenüber der betroffenen Person verarbeitet werden. Organisationen müssen eine rechtmäßige Grundlage für die Verarbeitung von Daten haben, wie z. B. die Einwilligung, und sie müssen Personen klar darüber informieren, wie ihre Daten verwendet werden.

2. **Zweck Einschränkung**

Die erhobenen Daten müssen für festgelegte, eindeutige und rechtmäßige Zwecke bestimmt sein und dürfen nicht in einer Weise weiterverarbeitet werden, die mit diesen Zwecken unvereinbar ist.

3. **Minimierung von Daten**

Organisationen sollten nur die personenbezogenen Daten verarbeiten, die zur Erreichung des Verarbeitungszwecks erforderlich sind. Das bedeutet, dass die erhobenen Daten auf das beschränkt werden, was für den angegebenen Zweck unmittelbar relevant und notwendig ist.

4. **Rechte der betroffenen Personen**

Einzelpersonen haben Rechte in Bezug auf ihre Daten, darunter das Recht auf Zugang, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruch gegen die Verarbeitung und das Recht auf Datenübertragbarkeit.

5. **Rechenschaftspflicht und Datenschutz durch Design und Standard**

Organisationen müssen die Einhaltung der Vorschriften nachweisen, indem sie die Datenschutzgrundsätze umsetzen und die erforderlichen Garantien von Anfang an in ihre Datenverarbeitungstätigkeiten integrieren (by design) und sicherstellen, dass standardmäßig nur personenbezogene Daten verarbeitet werden, die für den jeweiligen Zweck der Verarbeitung erforderlich sind.

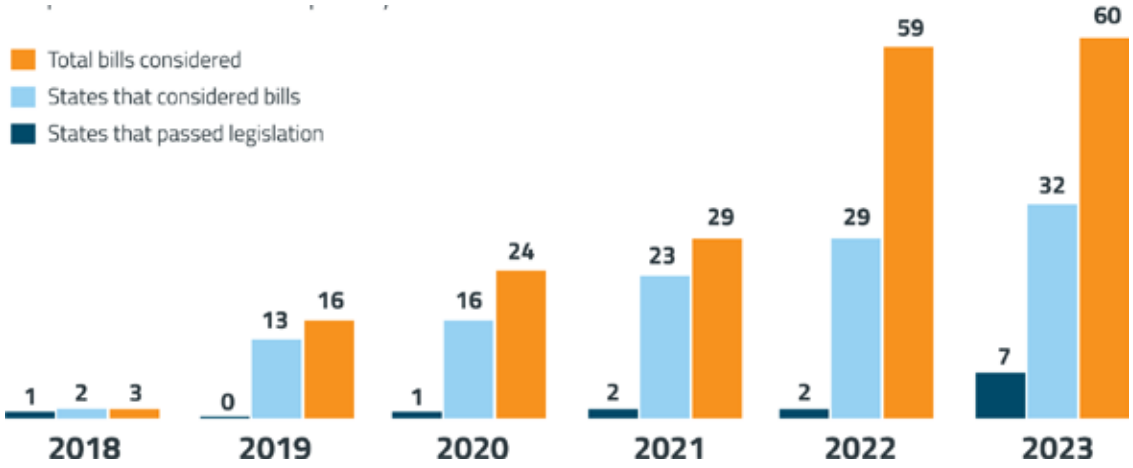
Vereinigte Staaten

Das Datenschutzrecht in den Vereinigten Staaten unterscheidet sich erheblich von dem in der EU.

Die Vereinigten Staaten sind eines der wenigen Länder, in denen es kein übergreifendes Bundesgesetz zum Datenschutz gibt. Im Jahr 2022 wurde zwar ein neues Gesetz - der American Data Privacy and Protection Act (ADPPA) - eingeführt und im Kongress auf den Weg gebracht, doch scheint es ohne Unterstützung im Senat ins Stocken geraten zu sein, und Analysten sagen voraus, dass es in naher Zukunft auf der Strecke bleiben wird.

Aufgrund der Untätigkeit der Bundesbehörden wird das US-Datenschutzrecht in erster Linie auf Ebene der Bundesstaaten geregelt.

Wie wir weltweit gesehen haben, ist das Interesse an staatlichen Datenschutzgesetzen exponentiell gestiegen. Die Zahl der erwogenen und verabschiedeten Gesetzesentwürfe hat in den letzten fünf Jahren deutlich zugenommen.



2023 war in vielerlei Hinsicht ein bahnbrechendes Jahr für die Verabschiedung von Gesetzen. In sieben Staaten wurden neue Gesetze verabschiedet, darunter die folgenden:

Delaware Delaware-Gesetz zum Schutz persönlicher Daten (DPDPA)	**Florida** Florida Digital Bill of Rights (FDBR)	**Indiana** Indiana Verbraucherdatenschutzgesetz (ICDPA)

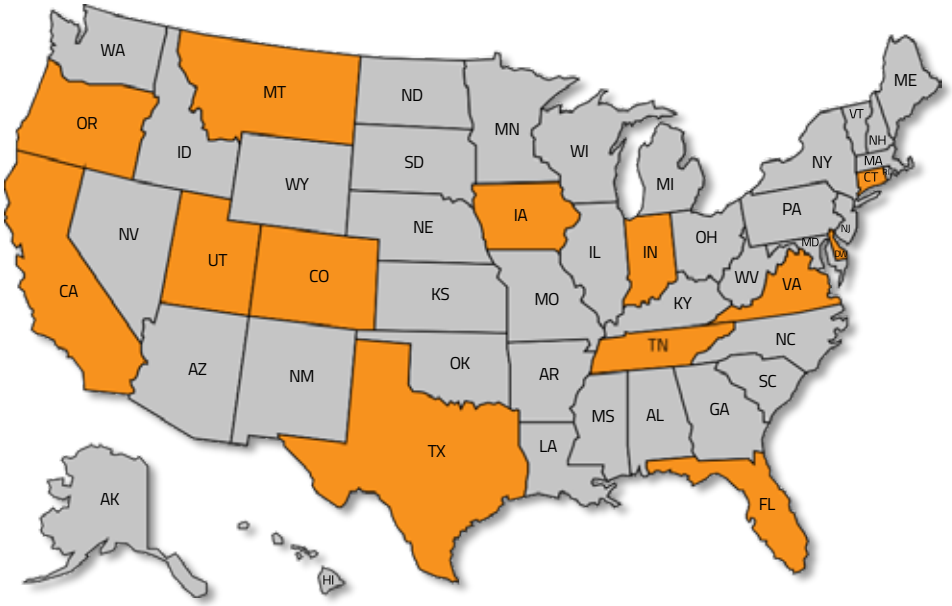
Montana Montana Verbraucherdatenschutzgesetz (MCDPA)	**Oregon** Oregon Consumer Privacy Act (OCPA)	**Tennessee** Tennessee-Informationsschutzgesetz (TIPA)	**Texas** Gesetz zum Datenschutz und zur Datensicherheit in Texas (TDPSA)

Die Gesetzgebungsmaßnahmen in den oben genannten Rechtsordnungen kommen zu den bereits bestehenden Rechtsvorschriften in den folgenden Staaten hinzu:

Kalifornien Kalifornisches Gesetz zum Schutz der Privatsphäre (CPRA)	**Colorado** Colorado Datenschutzgesetz (CPA)	**Connecticut** Connecticut-Datenschutzgesetz (CDPA)

Iowa Gesetz von Iowa (Gesetz über den Schutz von Verbraucherdaten)	**Utah** Gesetz zum Schutz der Privatsphäre der Verbraucher in Utah (UCPA)	**Virginia** Virginia Verbraucherdatenschutzgesetz (VCDPA)

Infolgedessen stellt sich die derzeitige Gesamtlandschaft des US-Datenschutzrechts wie folgt dar:



Datenschutzgesetze auf Staatsebene, 2024

Obwohl die Gesetze der einzelnen Bundesstaaten einige Gemeinsamkeiten aufweisen (sie zielen alle darauf ab, die Rechte der Verbraucher zu stärken, und im Moment müssen Unternehmen, die die Vorschriften einhalten wollen, den höchsten anwendbaren Standard der einzelnen Bundesstaaten erfüllen), gibt es genügend Unterschiede, so dass Rechtskommentatoren das US-Datenschutzrecht als "Flickwerk" bezeichnen. So unterscheiden sich beispielsweise die Opt-out- und Opt-in-Rechte für digitale Werbung erheblich, und es besteht weiteres Potenzial für künftige Änderungen, wenn die einzelnen Bundesstaaten ihre Regelungen abschließen.

Angesichts dessen könnten die kommenden Jahre ein "entscheidender Meilenstein" im Streben nach regulatorischer Konvergenz sein. Halten Sie Ausschau nach künftigen Schritten zur Angleichung der Gesetze der einzelnen Staaten oder nach Möglichkeiten zur Vermeidung von Überregulierung. Es gibt Anzeichen dafür, dass in diesem Jahr ein bedeutender Fortschritt in Richtung Harmonisierung erzielt werden könnte.

Andere

Kanada

Der derzeitige kanadische Datenschutzrahmen wird in erster Linie durch den Personal Information Protection and Electronic Documents Act (PIPEDA) geregelt.

Das im Jahr 2000 in Kraft getretene PIPEDA regelt die Erfassung, Verwendung und Weitergabe personenbezogener Daten im Rahmen kommerzieller Aktivitäten in allen Provinzen, mit Ausnahme derjenigen, die über eigene, gleichwertige Datenschutzgesetze verfügen. Es gilt für privatwirtschaftliche Organisationen und wird vom Office of the Privacy Commissioner of Canada überwacht.

PIPEDA basiert auf dem Prinzip der Einholung der Zustimmung für die Sammlung, Verwendung und Weitergabe von persönlichen Daten. Es unterstreicht die Notwendigkeit für Organisationen, Informationen nur für vernünftige Zwecke zu sammeln und verlangt von ihnen, genaue, vollständige und aktuelle Daten zu führen. Einzelpersonen haben das Recht, auf ihre persönlichen Daten in einer Organisation zuzugreifen und deren Richtigkeit anzufechten. Das Gesetz schreibt auch angemessene Sicherheitsmaßnahmen zum Schutz personenbezogener Daten vor.

Im Laufe der Jahre wurde das PIPEDA-Gesetz geändert, um neuen Datenschutzbedenken Rechnung zu tragen, insbesondere in Bezug auf digitale Informationen und grenzüberschreitende Datenströme. Derzeit sind größere Aktualisierungen der nationalen Gesetze Kanadas vorgeschlagen, aber noch nicht in Kraft gesetzt worden.

Indien

Die indischen Datenschutzgesetze werden derzeit durch den Digital Personal Data Protection Act (DPDP Act) geregelt, der im Jahr 2023 in Kraft tritt. Die indische Regierung hat noch keine effektiven Daten festgelegt und wird wahrscheinlich Folgegesetze verabschieden, die bestimmen, wie das Gesetz umgesetzt wird.

The Das Datenschutzgesetz verpflichtet Datentreuhänder unter anderem dazu, vor der Datenverarbeitung die Zustimmung der Nutzer einzuholen und Schutzmaßnahmen zur Vermeidung von Verstößen zu ergreifen. Den Verbrauchern werden Rechte eingeräumt,

darunter das Recht, eine Zusammenfassung ihrer gesammelten Daten anzufordern und sie zu korrigieren, zu aktualisieren oder zu löschen.

Mit dem Gesetz wird auch eine Datenschutzbehörde in Indien geschaffen, die über weitreichende Befugnisse verfügt, um potenzielle Verstöße gegen das Gesetz zu untersuchen und ihre Mandate durchzusetzen.

Das DPDP-Gesetz hat einen extraterritorialen Anwendungsbereich. Es gilt für die Datenverarbeitung außerhalb Indiens, wenn sie in Verbindung mit einer Tätigkeit steht, bei der Waren oder Dienstleistungen für Personen innerhalb Indiens angeboten werden. Das bedeutet, dass internationale Unternehmen bei der Verarbeitung von Daten indischer Nutzer das Gesetz einhalten müssen.

Mexiko

Das Bundesgesetz über den Schutz personenbezogener Daten im Besitz von Privatpersonen in Mexiko ist der Eckpfeiler des mexikanischen Rechtsrahmens für den Datenschutz im privaten Sektor.

Die 2010 in Kraft getretene Verordnung war ein bedeutender Schritt zur Angleichung an die weltweiten Datenschutzstandards und spiegelt Grundsätze wie die der Datenschutz-Grundverordnung der Europäischen Union wider.

Das Gesetz zielt in erster Linie darauf ab, die rechtmäßige, informierte und faire Verarbeitung personenbezogener Daten durch private Einrichtungen zu regeln und den Schutz der Privatsphäre und der Grundrechte des Einzelnen zu gewährleisten.

Sie verpflichtet die für die Datenverarbeitung Verantwortlichen, die ausdrückliche Zustimmung zur Verarbeitung personenbezogener Daten einzuholen, außer in bestimmten, gesetzlich vorgesehenen Ausnahmefällen. Außerdem wird die Transparenz betont, indem die für die Verarbeitung Verantwortlichen verpflichtet werden, den Zweck und die Mittel der Datenverarbeitung offenzulegen.

Darüber hinaus werden dem Einzelnen ARCO-Rechte eingeräumt, die ihm die Kontrolle über seine persönlichen Daten ermöglichen.

Ressourcen

Für Fachleute, Organisationen und Einzelpersonen, die mit personenbezogenen Daten umgehen, ist eine kontinuierliche Weiterbildung zu aktuellen Entwicklungen unerlässlich.

Um diesen Bedarf an ständigem Lernen und der Einhaltung von Gesetzen zu unterstützen, wird im folgenden Abschnitt eine ausgewählte Liste externer Ressourcen vorgestellt.

Diese Ressourcen, die kostenlos zugänglich sind, bieten eine Fülle von Wissen, das von einführenden Materialien bis hin zu eingehenden Analysen und praktischen Anleitungen zu verschiedenen Aspekten des Datenschutzes reicht.

Internationaler Verband der Datenschutzbeauftragten (IAPP)

Als größte und umfassendste globale Gemeinschaft und Ressource für den Datenschutz bietet die IAPP umfangreiche Schulungen, Richtlinien und Ressourcen für Datenschutzbeauftragte. Lesen Sie hier mehr.

Baker McKenzie Global Data Privacy & Security Handbook

Diese von der Anwaltskanzlei Baker McKenzie eingerichtete Ressourcendrehscheibe bietet Unternehmen einen Leitfaden für den Umgang mit Datenschutz-, Privatsphäre- und Cybersicherheitsgesetzen in verschiedenen Rechtsordnungen. Lesen Sie hier mehr.

Privatsphäre ist wichtig

Die Global Privacy and Data Protection Resource von DLA Piper enthält Berichte und juristische Expertenanalysen zu Datenschutztrends. Lesen Sie hier mehr.

Ressourcen zur Verantwortung für Google Business-Daten

Google bietet Schulungen sowie Zugang zu kostenlosen Analysetools und Open-Source-Datenschutztechnologien an, die Unternehmen dabei helfen, ihre Daten besser zu verstehen und verantwortungsvoller zu verwalten. Lesen Sie hier mehr.

JD Supra

Diese Ressource enthält aktuelle Informationen zum Datenschutzrecht, Nachrichten und juristische Kommentare von führenden Anwälten und Kanzleien. Lesen Sie hier mehr.

Glossar

Begriff	Definition
Biometrische Daten	Personenbezogene Daten, die sich aus spezifischen technischen Verarbeitungen ergeben und sich auf physische Merkmale beziehen, die eine Person identifizieren können.
Zustimmung	Eine aus freien Stücken, für den konkreten Fall, in Kenntnis der Sachlage und unmissverständlich abgegebene Willensbekundung der betroffenen Person, mit der sie der Verarbeitung personenbezogener Daten zustimmt.
Datenpanne	Ein Sicherheitsvorfall, bei dem unbefugt auf Informationen zugegriffen wird.
Datenkontrolleur	Die Stelle, die die Zwecke und Mittel der Verarbeitung personenbezogener Daten festlegt.
Minimierung von Daten	Der Grundsatz, dass die erhobenen personenbezogenen Daten auf das beschränkt werden sollten, was in Bezug auf die Zwecke, für die sie verarbeitet werden, notwendig ist.

Übertragbarkeit von Daten	Das Recht einer betroffenen Person, ihre personenbezogenen Daten in einem strukturierten, allgemein gebräuchlichen und maschinenlesbaren Format zu erhalten.
Datenverarbeiter	Eine Stelle, die personenbezogene Daten im Auftrag des für die Datenverarbeitung Verantwortlichen verarbeitet.
Datenschutzbehörde (DPA)	Eine öffentliche Behörde, die für die Überwachung und Durchsetzung der Datenschutzgesetze zuständig ist.
Gegenstand der Daten	Die Person, zu der die personenbezogenen Daten gehören.
De-identifizierte Daten	Informationen, aus denen Identifikatoren entfernt wurden, um eine direkte Verbindung zu Einzelpersonen zu verhindern.
Verschlüsselte Daten	Personenbezogene Daten, die durch technische Mittel umgewandelt wurden, um sie vor unbefugtem Zugriff zu schützen.
Allgemeine Datenschutzverordnung (GDPR)	Eine Verordnung im EU-Recht über den Datenschutz und den Schutz der Privatsphäre in der Europäischen Union und dem Europäischen Wirtschaftsraum.
Büro des Informationsbeauftragten (ICO)	Die unabhängige Behörde des Vereinigten Königreichs, die zur Wahrung der Informationsrechte im öffentlichen Interesse eingerichtet wurde.
Legitimes Interesse	Ein berechtigtes Interesse, das ein für die Verarbeitung Verantwortlicher an der Verarbeitung personenbezogener Daten hat und das mit den Interessen oder Grundrechten der betroffenen Person abgewogen wird.
Persönliche Daten	Informationen, die sich auf eine identifizierbare Person beziehen, wie Namen, ID-Nummern und Standortdaten.
Datenschutz-Folgenabschätzung (PIA)	Ein Tool zur Ermittlung und Verringerung der Datenschutzrisiken von Unternehmen durch Analyse des Umgangs mit personenbezogenen Daten.
Datenschutz durch Design	Ein Prinzip, das die Berücksichtigung der Privatsphäre während des gesamten Entwicklungsprozesses eines Produkts oder einer Dienstleistung fordert.

Verarbeitung	Jeder Vorgang, der mit personenbezogenen Daten durchgeführt wird, von der Erhebung bis zur Vernichtung.
Profilierung	Jede Form der automatisierten Verarbeitung personenbezogener Daten zur Bewertung bestimmter persönlicher Aspekte in Bezug auf eine natürliche Person.
Pseudonymisierung	Verarbeitung personenbezogener Daten in einer Weise, dass sie ohne die Verwendung zusätzlicher Informationen nicht mehr einer bestimmten betroffenen Person zugeordnet werden können.
Recht auf Vergessenwerden	Das Recht des Einzelnen, seine personenbezogenen Daten unter bestimmten Umständen löschen zu lassen.
Sensible persönliche Daten	Personenbezogene Daten, die genetische Daten, biometrische Daten, Daten über Gesundheit, rassische oder ethnische Herkunft, politische Meinungen oder sexuelle Orientierung umfassen.
Antrag auf Zugang zum Thema (SAR)	Ein Antrag einer betroffenen Person, eine Kopie der personenbezogenen Daten zu erhalten, die eine Organisation über sie gespeichert hat.
Dritte Partei	Jede Stelle, die nicht die betroffene Person, der für die Verarbeitung Verantwortliche, der Auftragsverarbeiter oder die Personen ist, die befugt sind, personenbezogene Daten unter der direkten Aufsicht des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters zu verarbeiten.
Transparenz	Der Grundsatz, dass Informationen über die Verarbeitung personenbezogener Daten für die betroffene Person leicht zugänglich und verständlich sein sollten.
Zwei-Faktoren-Authentifizierung (2FA)	Ein Sicherheitsverfahren, bei dem der Benutzer zwei verschiedene Authentifizierungsfaktoren angibt, um sich zu verifizieren.
Unstrukturierte Daten	Informationen, die sich nicht in einer herkömmlichen zeilen- und spaltenbasierten Datenbank befinden und oft sehr textlastig sind.
Benutzerdaten	Daten, die sich auf das Verhalten und die Interaktion von Nutzern mit Diensten oder Produkten beziehen und häufig durch Online-Aktivitäten erhoben werden.
Verstöße	Nichteinhaltung der Datenschutzgesetze, was zu Durchsetzungsmaßnahmen und Strafen führen kann.

Über VENZA

Venza ist der führende Anbieter von Datenschutz und Einhaltung gesetzlicher Vorschriften für das Gastgewerbe. Basierend auf jahrzehntelanger Erfahrung bietet VENZA eine 360-Grad-Transparenz, die ein proaktives Risikomanagement ermöglicht, um Schwachstellen zu minimieren und Ihre Gäste und deren Daten zu schützen. Kennen Sie Ihre Risiken und schützen Sie Ihr Unternehmen mit Venza...

Besuchen Sie www.venza.io für weitere Informationen.

Kontakt

Verkäufe: sales@venzagroup.com

Kundenerfolg: success@venza.io