# Der ultimative Leitfaden für das Datenschutz-management

OneTrust

PRIVACY, SECURITY & GOVERNANCE

E-BOOK | JANUAR 2022

# INHALTSVERZEICHNIS



## HAFTUNGSAUSSCHLUSS



OneTrust

PRIVACY, SECURITY & GOVERNANCE

# ÜBER DIESEN LEITFADEN

Heutzutage müssen Unternehmen eine Vielzahl lokaler und internationaler Gesetze zum Schutz individueller Datenrechte einhalten. Die dabei unterstützenden Prozesse und Aktivitäten sind in einem Fachbereich zusammengefasst, der als **Datenschutzmanagement** bezeichnet wird.

Mit der Weiterentwicklung der Datenschutzlandschaft haben sich auch die wichtigsten Bereiche, die in ein Datenschutzmanagement-Programm aufgenommen werden müssen, verändert. Da dieser Bereich für Unternehmen, die ihre Kunden besser ansprechen und sich rechtlich schützen möchten, so entscheidend ist, ist es wichtig, die Hauptfaktoren zu verstehen, die zu einem soliden Datenschutzmanagement-Programm beitragen.

Dieser ultimative Leitfaden zum Datenschutzmanagement tut genau das. Sie erfahren, welche Bereiche Sie einbeziehen müssen, warum sie wichtig sind und wie Sie spezifische Taktiken zur Unterstützung umsetzen können.

OneTrust
PRIVACY, SECURITY & GOVERNANCE

# RECHTMÄSSIGKEIT, FAIRNESS UND NICHTDISKRIMINIERUNG

Ein grundlegender Standard für das Datenschutzmanagement ist es, durch Aufzeichnungen nachzuweisen, dass Sie eine rechtliche Grundlage für die Erhebung und Verarbeitung personenbezogener Daten haben. Dies wird als Rechtsgrundlage bezeichnet und gehört zu den wichtigsten Aspekten der weithin bekannten Datenschutzgesetze, einschließlich der DSGVO und des LGPD.

Um die Rechtsgrundlage zu schaffen, müssen Sie mindestens **einen von sechs Parametern** befolgen:

1. Erfüllung eines Vertrags: Sie verarbeiten Daten, um einen Vertrag zu unterzeichnen oder seine Bedingungen zu bestätigen.
2. Einhaltung einer gesetzlichen Verpflichtung: Sie verarbeiten Daten zu rechtlichen Zwecken, z. B. zur Überprüfung der Bewerbung und der Hintergrundinformationen eines neuen Mitarbeiters.
3. Schutz lebenswichtiger Interessen (Sicherheit) von Personen: Sie verarbeiten Daten, um jemandem in einer Notfallsituation, in der Regel bei einem medizinischen Notfall, zu helfen.
4. Erfüllung einer Aufgabe, die im öffentlichen Interesse ausgeführt wird: Sie verarbeiten Daten als Regierungsorganisation oder als Unterstützer einer solchen Stelle.
5. Berechtigte Interessen: Sie verarbeiten Daten, ohne dass Nutzer ihre Einwilligung aus einem Grund erteilen, den Sie für diese Nutzer als wertvoll erachten. Führen Sie eine Bewertung des berechtigten Interesses durch, um nachzuweisen, dass Sie berechtigt sind, sich auf diesen Grund zu stützen.
6. Einwilligung: Sie verarbeiten Daten, weil Nutzer ihre ausdrückliche Einwilligung gegeben haben. Um diese als Rechtsgrundlage heranzuziehen, stellen Sie sicher, dass die Einwilligung freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegeben wird.

Neben der Rechtsgrundlage gibt es **vier weitere Kriterien**, die in Bezug auf Rechtmäßigkeit, Fairness und Nichtdiskriminierung zu befolgen sind.

1. Fairness: Personenbezogene Daten müssen auf dem konservativsten Niveau der Fairness verarbeitet werden. Ein Beispiel dafür ist, dass Datenschutzeinstellungen leicht zugänglich und verständlich sind und standardmäßig auf den höchsten Schutz eingestellt sind.
2. Schutz von Minderjährigen: Stellen Sie sicher, dass Mechanismen und Prozesse zum Schutz der Daten von Minderjährigen vorhanden sind. Ein Beispiel, das durch einige Datenschutzgesetze gefördert wird, ist die vorherige Einwilligung der Eltern.
3. Verarbeitung sensibler Daten: Richten Sie Maßnahmen und angemessene Stufen der Sonderbehandlung ein, um sensible Daten sicher zu verarbeiten, z. B. rassische oder ethnische Herkunft, Gesundheitsdaten und Religionszugehörigkeit.
4. Nichtdiskriminierung: Sie können Nutzer nicht aufgrund ihrer Datenschutzpräferenzen diskriminieren.


OneTrust
PRIVACY, SECURITY & GOVERNANCE

# TRANSPARENZ UND FREIER ZUGRIFF

Ein modernes Datenschutzmanagement-Programm sollte nichts vor den Nutzern verbergen - nicht nur aus datenschutzrechtlichen Gründen, sondern auch aus geschäftlichem Interesse. Der sichtbarste Weg, Transparenz zu schaffen, ist eine Datenschutzrichtlinie.

Eine solche Datenschutzrichtlinie sollte dauerhaft auf Ihrer Website vorhanden sein, damit Besucher leicht darauf zugreifen können. Sie sollte aber auch im Intranet oder auf einem Cloud-basierten System gespeichert und für Ihre Mitarbeiter zugänglich sein. Erstellen Sie unterstützende Materialien,
die Ihrem Team helfen, die Datenschutzrichtlinie wirksamer zu erfüllen:

- Verfassen Sie Verfahren und Konzepte, um sie für Schulungen und zu Referenzzwecken zu verwenden.
- Dokumentieren Sie die Aktivitäten und führen Sie Audits durch, um ihre interne Einhaltung sicherzustellen.
- Weisen Sie eine Person und/oder Abteilung zu, die für die Dokumentation und Kommunikation von Richtlinienänderungen verantwortlich ist.

Der Übermittlungsprozess, mit dem ein Nutzer individuelles Feedback zu einer Statusänderung seines Feedbacks einreichen kann, sollte ebenfalls Teil Ihrer Datenschutzrichtlinie sein.

Und schließlich müssen Sie freien Zugriff ermöglichen und Informationen über Form und Dauer Ihrer Datenverarbeitung und deren Integrität bereitstellen. Dies sollte geschehen, indem den Nutzern zu dem Zeitpunkt, zu dem Sie ihre Daten erheben, eine Nachricht angezeigt wird: Welche Daten Sie erheben, nutzen, speichern und übermitteln.

OneTrust
PRIVACY, SECURITY & GOVERNANCE

# ZWECKBESTIMMUNG, NUTZUNGSBESCHRÄNKUNG UND EIGNUNG

Es reicht nicht aus, dass Sie einen guten Grund und ein gültiges Mittel zur Erhebung personenbezogener Daten angeben. Das Datenschutzmanagement erfordert eine Zweckbestimmung: Sie verwenden die erfassten Daten – nur und genau – dafür, wie Sie es angegeben haben.

**Beachten Sie dabei bitte Folgendes:**

- Dokumentieren Sie den Zweck der Datenerhebung, bevor Sie damit beginnen.
- Erheben Sie keine Daten für den Fall, dass Sie sie in der Zukunft benötigen. Erheben Sie sie nur für den/die angegebenen Zweck(e).

Außerdem sollten Sie nicht mehr mit den Daten tun, als Sie angegeben haben. Der Grundsatz der Nutzungsbeschränkung macht Sie unter anderem dafür verantwortlich, keine Daten zwischen Abteilungen auszutauschen, die Anfälligkeit für Hackerangriffe zu minimieren und eine sichere ID-Authentifizierung zu etablieren.

Sie sind außerdem verpflichtet, eine angemessene Nutzung zu gewährleisten. Sie dürfen die Zwecke, die Sie gegenüber den betroffenen Personen über die Verarbeitung ihrer Daten mitgeteilt haben, nicht überschreiten.

OneTrust
PRIVACY, SECURITY & GOVERNANCE

# DATENMINIMIERUNG, SPEICHERBEGRENZUNG UND GENAUIGKEIT

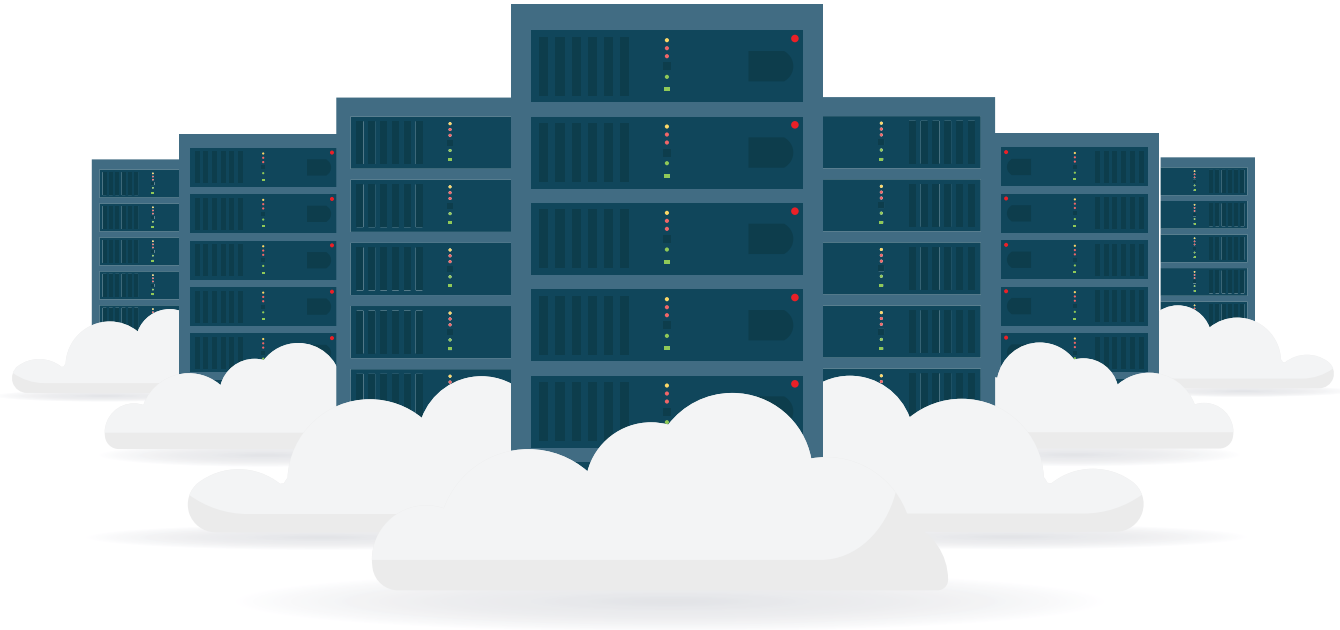
Ein Datenschutzmanagement-Programm sollte sich nicht nur auf die Vorbereitung und spätere Erhebung personenbezogener Daten konzentrieren. Sie müssen außerdem sicherstellen, dass Daten nach der Erhebung sicher gespeichert und aufbewahrt werden. Die Integrität der Daten einer Person muss während des gesamten Lebenszyklus bei Ihrem Unternehmen erhalten bleiben.

Datenminimierung stellt sicher, dass die Verarbeitung personenbezogener Daten angemessen, relevant und auf das notwendige beschränkt ist. Setzen Sie die Datenminimierung wie folgt um:

- Richten Sie eine Benutzeroberfläche ein, die zwischen optionalen und erforderlichen Formularfeldern unterscheiden kann.
- Verwenden Sie festgelegte Felder in einem Formular anstelle von offenen Textfeldern.
- Überprüfen Sie Daten auf Angemessenheit und Relevanz für einen bestimmten Zweck – vor der Verarbeitung.
- Erheben Sie nur die Daten, die zur Erreichung eines bestimmten Zweck erforderlich sind.
- Begrenzen Sie die Menge der übermittelten Daten auf das Mindeste.

Außerdem müssen Sie die bewährten Methoden für die Speicherbeschränkung befolgen. Personenbezogene Daten müssen so aufbewahrt werden, dass Sie sie leicht löschen können, wenn sie nicht mehr für Ihre Zwecke gespeichert werden müssen. Überprüfen Sie regelmäßig Ihren Datenbestand. Richten Sie Auslöser zum Löschen von Daten ein. Und löschen Sie personenbezogene Daten sofort und sicher, wenn Nutzer ihre Konten deaktivieren oder löschen.

Um die personenbezogenen Daten, die Sie speichern, genau und auf dem neuesten Stand zu halten, richten Sie Prüfverfahren speziell für diese Aufgabe ein. Temporäre Dateien, die beim Speichern personenbezogener Daten erstellt werden, müssen vollständig und sicher gelöscht werden.



OneTrust
PRIVACY, SECURITY & GOVERNANCE

# MANAGEMENTSYSTEM UND SICHERHEIT

Die Durchführung eines langfristigen Datenschutzmanagement-Programms beginnt damit, den rechtlichen Kontext hinter allem, was Sie tun, zu verstehen. Weltweit erlassen Regierungen Datenschutzgesetze. Sie müssen mit diesen rechtlichen, regulatorischen und vertraglichen Anforderungen vertraut sein, um sie umsetzen zu können.

Beginnen Sie mit der Bestandsaufnahme und Zuordnung. Untersuchen Sie Ihre gespeicherten Daten und wie sie verarbeitet werden sorgfältig. Dazu gehören Verarbeitungstätigkeiten, Datenaktionen, Datenelemente, die Kategorie der Personen und die Datenumgebung.

So können Sie besser verstehen, welches Datenschutzrahmenwerk zu befolgen ist, wie z. B. das **NIST-Datenschutzrahmenwerk**, und wie Sie die damit verbundenen Datenschutzrisiken handhaben können. Das Management dieser Risiken ist wichtig. Erstellen Sie Berichtsfunktionen und Datenschutzkontrollen, um sie im Auge zu behalten.

**Dokumentieren Sie alles, was geschieht:**

- Die internen und externen Faktoren, die sich auf den Datenschutz Ihres Unternehmens auswirken – oder ihn potenziell beeinträchtigen.
- Die Bedürfnisse und Erwartungen betroffener Parteien.
- Den Umfang, den Ihr Datenschutzprogramm abdecken muss.

Eine zuverlässige und leistungsfähige **Plattform für das Datenschutzmanagement** ist entscheidend für den Erfolg in diesem Bereich. Führen Sie ein formales und dokumentiertes Datenschutz- und/oder Sicherheitssystem ein, das sich der kontinuierlichen Überprüfung und Verbesserung verpflichtet.

## Sicherheit

Datenschutz und Sicherheit sind unterschiedliche, aber miteinander zusammenhängende Disziplinen. Sie sind aufeinander angewiesen, um wirksam zu funktionieren. Damit Ihr Datenschutzmanagement-Programm erfolgreich ist, sollten Sie sicherstellen, dass Sie die bewährten Methoden für die Sicherheit befolgen:

- Führen Sie Aufzeichnungen über die Medien, die personenbezogene Daten enthalten.
- Schützen Sie biometrische Daten, indem Sie sie außerhalb von Informationssystemen für personenbezogene Daten und in physischen Datenträgern speichern.
- Ernennen Sie einen Informationssicherheitsbeauftragten.
- Führen Sie Penetrationstests und Schwachstellenbewertungen für Informationssysteme durch.
- Beschränken Sie die Nutzerzugriffsrechte gemäß dem „Need-to-know"-Grundsatz.
- Verwenden Sie Multi-Faktor-Authentifizierung und -Verschlüsselung, um unbefugten Zugriff auf Daten zu verhindern.
- Installieren Sie Firewalls, Systempatches, Malware- und Virenschutzsoftware.
- Setzen Sie technische und organisatorische Maßnahmen ein, um die kontinuierliche Integrität, Verfügbarkeit und Belastbarkeit von Systemen, Diensten und Daten zur Verarbeitung zu gewährleisten.

Sicherheit ist für die Eignung Ihres Datenschutzmanagement-Programms von entscheidender Bedeutung. Sie müssen es richtig machen. Um Ihre Sicherheitsprozesse und -kontrollen noch einmal zu überprüfen, können Sie **diese Checkliste** mit folgenden Fragen durchgehen:

- Haben Sie bei der Auswahl Ihrer Sicherheitskontrollen rechtliche und regulatorische Faktoren überprüft?
- Haben Sie bei der Auswahl Ihrer Sicherheitskontrollen die vertraglichen Faktoren überprüft?
- Haben Sie bei der Auswahl Ihrer Sicherheitskontrollen die Geschäftsfaktoren überprüft?
- Würden Sie sagen, dass Ihr Unternehmen über angemessene Sicherheitskontrollen verfügt, die dem Risiko und der Sensibilität der verarbeiteten Daten entsprechen?

OneTrust
PRIVACY, SECURITY & GOVERNANCE

# RECHENSCHAFTSPFLICHT UND DOKUMENTATION

Rechenschaftspflicht spielt eine wichtige Rolle beim Datenschutzmanagement. Sie müssen strenge Verfahren bei der Erhebung, Speicherung und Verwendung von Daten befolgen. Sie müssen sie aber auch beweisen können, wenn eine Regulierungsbehörde danach fragt.

Aufzeichnungen über die Verarbeitung sind die beste Möglichkeit, ihrer Rechenschaftspflicht nachzukommen. Führen Sie detaillierte Aufzeichnungen über die Verarbeitungstätigkeiten Ihres Unternehmens, die Datenflüsse und die Kategorien der betroffenen Personen. Wenn Sie noch keine haben, erstellen Sie ein Verarbeitungsverzeichnis:

- Integrierte Bestände personenbezogener Daten
- Verarbeitungstätigkeiten
- Informationsbestände
- Aufzeichnungen über Weitergabe an Dritte

Beraten Sie sich außerdem mit Ihren B2B-Kunden, bevor Sie rechtsverbindlich personenbezogene Daten an Dritte weitergeben.

Außerdem müssen Sie nachweisen können, dass Sie bei den zuständigen Behörden bezüglich der Verarbeitungstätigkeiten registriert sind oder eine Genehmigung für bestimmte Verarbeitungstätigkeiten erhalten haben. Und Sie müssen genau aufzeigen, wer der Tätigkeit nachgeht – für externe und interne Zwecke.

Für die externe Überprüfung müssen Sie festlegen, wer für die Verarbeitung personenbezogener Daten verantwortlich ist, wenn es einen gemeinsamen Verantwortlichen gibt. Unterauftragnehmer vertreten ebenfalls eine externe Stelle, die von Kunden zur Verarbeitung von Daten autorisiert werden muss.

Eine fortlaufende und genaue Führung von Aufzeichnungen ist die einzige Möglichkeit, mit ausreichenden Beweisen ausgestattet zu sein, wenn Sie jemals zur Rechenschaft gezogen werden. Eine Kombination aus automatisierten und manuellen internen **Berichterstellungs- und Auditmechanismen** ist unerlässlich. **Achten Sie auf neue Gesetze und Vorschriften**, um Ihre Richtlinien und Verfahren zu aktualisieren.

Stellen Sie sicher, dass Sie über offene Kommunikationswege zwischen dem Datenschutzbeauftragten und anderen Abteilungen innerhalb des Unternehmens verfügen.

OneTrust
PRIVACY, SECURITY & GOVERNANCE

# DSB UND DATENSCHUTZ DURCH TECHNIKGESTALTUNG

Eine der Hauptaufgaben des DSB besteht darin, durchgängig teamweite Kommunikationskanäle zu Datenschutzrichtlinien und -verfahren zu erstellen und zu pflegen. Datenschutzbeauftragte aus jeder Abteilung fungieren als Kontaktpersonen zwischen dem DSB und ihren jeweiligen Teams:

- Informationssicherheit
- Internes Audit
- HR
- Lieferantenmanagement
- Kommunikation
- Geschäftsführung
- Produktentwicklung
- Analytik
- Marketing

Die andere Hauptaufgabe des DSB besteht darin, Strategien zu entwickeln – und sicherzustellen, dass sie ordnungsgemäß ausgeführt werden –, wenn es um die **sieben Grundsätze des Datenschutzes durch Technikgestaltung** geht.

**Diese Grundsätze sind:**

- Proaktiv, nicht reaktiv – als Vorbeugung und nicht als Abhilfe
- Datenschutz als Standardeinstellung
- Der Datenschutz ist in das Design eingebettet
- Volle Funktionalität trotz Datenschutz – eine Positivsumme, keine Nullsumme
- Durchgängige Sicherheit – Schutz während des gesamten Lebenszyklus
- Sichtbarkeit und Transparenz – für Offenheit sorgen
- Die Wahrung der Privatsphäre der Nutzer – für eine nutzerzentrierte Gestaltung sorgen


OneTrust
PRIVACY, SECURITY & GOVERNANCE

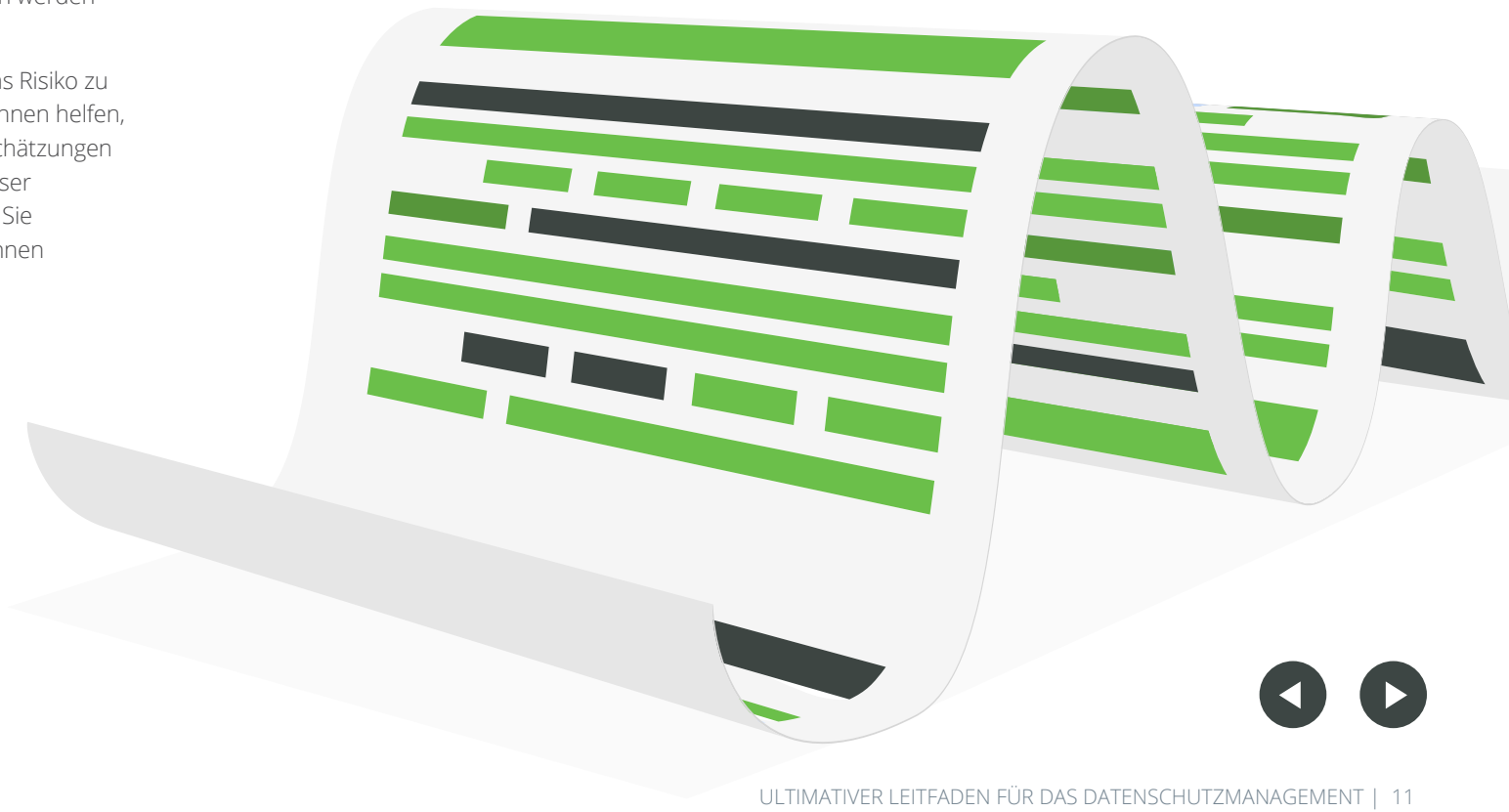
# DATENSCHUTZ-FOLGENABSCHÄTZUNGEN

Einige Datenschutzgesetze verlangen Datenschutz-Folgenabschätzungen: Ihr Unternehmen ist für die Erkennung von Risiken im Zusammenhang mit Verarbeitungstätigkeiten verantwortlich. Andere Datenschutzstandards erfordern, dass Datenschutz-Folgenabschätzungen unterschiedliche Inhalte umfassen. **Zu den allgemein unverzichtbaren Aspekten gehören:**

- Die zu erhebenden Informationen (Art und Quelle)
- Warum diese Daten erfasst werden
- Verwendungszweck der Informationen
- An wen die Informationen weitergegeben werden

Nach der Erstellung einer Datenschutz-Folgenabschätzung besteht das Ziel darin, das Risiko zu verstehen. Ein Risikobehandlungsplan kann Ihnen helfen, die Ergebnisse Ihrer Datenschutz-Folgenabschätzungen zu beurteilen und zu dokumentieren. Auf dieser Grundlage können Sie besser verstehen, wie Sie Maßnahmen ergreifen können, um die von Ihnen ermittelten Risiken zu verringern.

Wenn Sie hohe Restrisiken entdeckt haben, ist es in Ihrem besten Interesse, Rat und Genehmigung von Datenschutzbehörden einzuholen, bevor Sie mit der Verarbeitung von Daten fortfahren. Einige Datenschutzgesetze verlangen dies sogar. Wenn es um den Schutz personenbezogener Daten geht, ist es immer besser, sich zu schützen, als sich zu entschuldigen.



OneTrust
PRIVACY, SECURITY & GOVERNANCE

# RECHTE BETROFFENER PERSONEN

Die Bereitstellung von Datenrechten für Nutzer steht im Mittelpunkt fast aller internationalen Datenschutzgesetze. Mit anderen Worten: Sie müssen über Prozess- und Unterstützungsmechanismen verfügen, um Anfragen von Personen zu ihren Daten zu bearbeiten.

Es beginnt damit, dass betroffene Personen klar und unmissverständlich darauf hingewiesen werden, welche Rechte sie haben und wie sie diese ausüben können. Es muss eine einfache Möglichkeit für sie bestehen, Anfragen einzureichen. Und Ihr Team sollte darauf vorbereitet sein, mit ihnen umzugehen. Interne Richtlinien, Verfahren und Schulungen zum Umgang mit Anfragen von betroffenen Personen sind ein Muss.

**Die Rechte der betroffenen Personen fallen in 10 Bereiche:**

- Recht auf Unterrichtung
- Recht auf Widerruf oder Änderung
- Recht auf Auskunft
- Recht auf Berichtigung
- Recht auf „Vergessenwerden“/Recht auf Löschung
- Recht auf Einschränkung
- Recht auf Sicherheitsstopp
- Recht auf Datenübertragbarkeit
- Recht auf Widerspruch
- Recht auf Ablehnung des Verkaufs von Daten

Wenn Ihr Unternehmen einige Entscheidungen über Nutzerdaten automatisiert, müssen Sie eine Möglichkeit für Nutzer bereitstellen, eine manuelle Überprüfung dieser Automatisierungen anzufordern. Ebenso müssen alle Änderungen an Nutzerdaten, die auf Anfrage der betroffenen Person vorgenommen werden, auch von Dritten geändert werden, an die sie weitergegeben wurden.

Schaffen Sie offene Kommunikationswege, um diese Stellen über Änderungen, Widerruf oder Einwände gegen personenbezogene Daten zu informieren.

OneTrust
PRIVACY, SECURITY & GOVERNANCE

# LIEFERANTENMANAGEMENT

Es ist nicht ungewöhnlich, dass Unternehmen verschiedene Dienste an Dritte auslagern. Wenn Sie Lieferanten nutzen, liegt es jedoch in Ihrer Verantwortung, dafür zu sorgen, dass diese Ihre Datenschutzrichtlinien einhalten. Sie müssen Prozesse und unterstützende Technologien einrichten, um ihren Verpflichtungen vollumfänglich nachzukommen.

Verträge sind der Schlüssel für ein wirksames Lieferantenmanagement. Sie sollten Ihre eigenen Datenschutzstandards genau widerspiegeln. Hier kann eine Checkliste zur Einhaltung hilfreich sein. Sie enthält eine Liste allgemeiner Erfordernisse im Datenschutz, z. B. eine Bewertung der Auswirkungen auf den Datenschutz von Lieferanten, die mit speziellen Richtlinien Ihres Unternehmens verknüpft sind. Sie müssen jedes Kästchen auf dieser Checkliste abhaken, um einen neuen Lieferanten einzubinden.

Lieferantenbewertungen sind für **die Überwachung der laufenden Einhaltung** unerlässlich. Überprüfen Sie alle Prozesse, um sicherzustellen, dass sie technische und organisatorische Maßnahmen ausreichend abdecken – und dass die Lieferanten sie befolgen.

**Grenzüberschreitende Datenübermittlung und Datenlokalisierung**

Unabhängig davon, ob Sie personenbezogene Daten außerhalb des Landes, in dem Sie geschäftlich tätig sind, empfangen oder senden, erfordert das Datenschutzmanagement, dass Sie diese Tätigkeiten nachverfolgen. Diese grenzüberschreitenden Datenübermittlungen müssen über rechtmäßige Mechanismen wie verbindliche interne Datenschutzvorschriften, Standardvertragsklauseln oder die Einwilligung der betroffenen Person erfolgen.

Es ist wichtig zu verstehen, dass die **Entscheidung "Schrems II"** den seit langem bestehenden EU-US-Datenschutzschild abgeschafft hat. Und obwohl Standardvertragsklauseln als Mechanismus zur Datenübermittlung zulässig sind, werden sie lediglich von Fall zu Fall akzeptiert.

Neben der Verantwortung für die grenzüberschreitende Datenübermittlung sehen einige Gesetze vor, dass personenbezogene Daten von Bürgern oder Einwohnern des vom Gesetz abgedeckten geografischen Gebiets innerhalb eines bestimmten Landes verarbeitet oder gespeichert werden müssen. Halten Sie sich genau an diese Anforderungen zur Datenlokalisierung.

OneTrust
PRIVACY, SECURITY & GOVERNANCE

# VORFÄLLE UND DATENSCHUTZVERLETZUNGEN

Kein Unternehmen möchte in die Situation kommen, in der die von ihm gespeicherten personenbezogenen Daten kompromittiert werden. Ein Teil des Datenschutzmanagements besteht darin, sich gründlich auf Vorfälle und Verstöße vorzubereiten, falls diese auftreten.

- Etablieren Sie Berichtsverfahren, um Vorfälle oder Schwachstellen schnell und vollständig nachzuverfolgen, sobald sie erkannt wurden.
- Dokumentieren Sie diese Schritte, um genau herauszufinden, was das Ereignis verursacht hat.
- Ermitteln, erheben und schützen Sie die Informationen im Zusammenhang mit dem Vorfall und bewahren Sie sie als Beweismittel auf.
- Erstellen Sie eine Checkliste mit Abhilfemaßnahmen zur Behebung der Auswirkungen des Vorfalls.

Viele Datenschutzvorschriften verlangen von Unternehmen, Vorfälle und Verstöße zu verfolgen. Sie sollten dies zu einer Best Practice machen, um sich rechtlich abzusichern.

Wenn Sie Ihr Team in den Prozessen und Verfahren zur Reaktion auf Vorfälle schulen, fühlen Sie sich besser auf solche Ereignisse vorbereitet. Weisen Sie Managern und ihren Teams Verantwortlichkeiten zu. Wenn jeder weiß, was seine Aufgaben sind, werden die Reaktionen auf Verstöße und Vorfälle schneller stattfinden.

Die Benachrichtigung der betroffenen Parteien ist eine wesentliche Tätigkeit nach einem Verstoß. Bereiten Sie im Voraus Benachrichtigungen vor, um sie schnell und klar an die betroffenen Personen, Behörden und Verantwortlichen zu übermitteln.

Führen Sie eine eingehende Überprüfung durch. Diese Analyse nach dem Sicherheitsvorfall sollte Folgendes umfassen: Was das Team gelernt hat, welche Aktualisierungen oder wiederkehrenden negativen Muster Sie ansprechen müssen und alle anderen Mitteilungen, die Sie ggf. versenden müssen.

OneTrust
PRIVACY, SECURITY & GOVERNANCE

# OneTrust

## PRIVACY, SECURITY & GOVERNANCE

### Informationen zu OneTrust

OneTrust ist das am schnellsten wachsende Unternehmen auf Inc. 500 und die kategoriedefinierende Unternehmensplattform zur Operationalisierung von Vertrauen. Mehr als 11.000 Kunden, darunter die Hälfte der Fortune-500-Unternehmen, nutzen OneTrust, um Vertrauen zu einem Wettbewerbsvorteil zu machen, indem sie zentrale, agile Workflows in den Bereichen Datenschutz, Sicherheit, Data Governance, GRC, Risikomanagement von Drittanbietern, Ethik und Compliance sowie ESG-Programme implementieren.

Die OneTrust Plattform wird von 150 Patenten gestützt und arbeitet mit der KI- und roboterbasierten Automatisierungs-Engine OneTrust Athena™. Zu unseren Angeboten gehören: OneTrust Datenschutzmanagement-Software, OneTrust DataDiscovery™ – KI-gestützte Erkennung und Klassifizierung, OneTrust DataGovernance™ – Data Intelligence Software, OneTrust Vendorpedia™ – Datenbank der Drittparteirisiken, OneTrust GRC – integriertes Risikomanagement, OneTrust Ethics – Ethik- und Compliance-Software, OneTrust PreferenceChoice™ – Einwilligungs- und Präferenzmanagement, OneTrust ESG-Software (Umwelt, Soziales und Governance) sowie das OneTrust DataGuidance™ Datenschutzportal.

Im IDC Worldwide Data Privacy Management Software Market Shares Report, 2020 heißt es: „OneTrust ist klarer Marktführer und zeigt keinerlei Anzeichen von Abschwächung oder Stillstand."

OneTrust hat von Insight Partners, Coatue, TCV, SoftBank Vision Fund 2 und Franklin Templeton insgesamt 920 Mio. US-Dollar aufgebracht und wurde mit 5,3 Mrd. US-Dollar bewertet.

Das Team von 2.000 Mitarbeitern von OneTrust hat seinen gemeinsamen Hauptsitz in Atlanta und London, weitere Büros befinden sich in Bangalore, Melbourne, Seattle, San Francisco, New York, São Paulo, München, Paris, Hongkong und Bangkok.

Weitere Informationen finden Sie auf OneTrust.de oder auf LinkedIn, Twitter und YouTube.