Datenschutzrichtlinie für Dashlane

Nachstehend finden Sie unsere Datenschutzrichtlinie. Sie müssen sie akzeptieren, um unsere Software verwenden zu können. Wir wissen aber, wie schwer es sein kann, die Inhalte zu verstehen. Damit Sie besser verstehen, womit Sie Ihr Einverständnis erklären, beginnt jeder Abschnitt mit einer kurzen Zusammenfassung in „nicht-juristischer" Sprache. Die Zusammenfassungen sind technisch betrachtet nicht Bestandteil der Richtlinie.

LETZTE AKTUALISIERUNG: 15. März 2024

1. EINFÜHRUNG

Zusammenfassung:
Diese Richtlinie beschreibt, wie wir personenbezogene Daten (die zur Identifizierung einer bestimmten Person verwendet werden können) und anonyme Daten (die dazu nicht verwendet werden können) über unsere Benutzer erfassen und verwenden. Bestimmte Teile der Richtlinie gelten nur für bestimmte Benutzer, wie z. B. Personen, die Dashlane mit einem vom Arbeitgeber bereitgestellten Tarif verwenden. Wir dürfen diese Richtlinie jederzeit ändern, indem wir die überarbeitete Richtlinie an dieser Stelle veröffentlichen. Wir werden aktuelle Benutzer außerdem per E-Mail oder In-App-Nachrichten über wichtige Änderungen informieren. Die Erfassung bestimmter personenbezogener Daten ist zur Bereitstellung der Dienste erforderlich. Wir bemühen uns jedoch, nur Daten zu erfassen, die wir tatsächlich benötigen. Auf Anfrage entfernen wir alle personenbezogenen Daten zu Kindern, die keine autorisierten Benutzer sind (z. B. nicht Mitglied eines Familientarifs). ***Aufgrund unserer Zero-Knowledge-Architektur wissen wir nicht, welche Daten Sie in den Diensten speichern.***

a. *Allgemeines*. Die vorliegende Datenschutzrichtlinie (die „**Richtlinie**") beschreibt, wie Dashlane Inc. und verbundene Unternehmen („**Dashlane**" oder „**wir**") Daten über Besucher unserer Website unter www.dashlane.com (zusammen mit den Subdomains wie dem Dashlane-Blog die „**Website**") sowie über Benutzer unserer Web-Erweiterungen und Mobile- und Web-Anwendungen (je eine „**App**" und gemeinsam die „**Apps**") sammeln, verwenden und weitergeben. Die Apps und die Website werden zusammen als die „**Dienste**" bezeichnet. „**Sie**" oder „**Benutzer**" stehen für alle Personen, die die Dienste nutzen oder die Website besuchen. Großgeschriebene Wörter, die in dieser Richtlinie verwendet, aber nicht definiert werden, haben die in unseren Nutzungsbedingungen (die „**Bedingungen**") angegebenen Bedeutungen.

b. *Personenbezogene und anonyme Daten*. „**Personenbezogenen Daten**" sind Daten, die entweder allein oder in Verbindung mit anderen Daten, die sich im Besitz des Halters befinden, die Identifizierung einer natürlichen Person ermöglichen (z. B. Name, Postadresse, E-Mail-Adresse, IP-Adresse oder Telefonnummer). „**Anonyme Daten**" sind Daten, die nicht zur Identifizierung einer Person verwendet werden können. Wir erfassen und verwenden sowohl personenbezogene als auch anonyme Daten wie nachfolgend beschrieben.

c. *Datenschutzgesetze*. Immer mehr Gesetze wie das California Privacy Rights Act („**CPRA**") und die Datenschutzgrundverordnung der Europäischen Union („**DSGVO**") regeln die Erfassung, Speicherung und Verwendung personenbezogener Daten durch Unternehmen (gemeinsam „**Datenschutzgesetze**"). Datenschutzgesetze gewähren Personen definierte Rechte, die es ihnen erlauben, zu wissen und zu kontrollieren, wie Unternehmen ihre personenbezogenen Daten verwenden. So weit wie möglich gestalten wir unsere Richtlinien so, dass sie den Datenschutzgesetzen entsprechen, die am meisten schützen, und wenden diese Richtlinien dann auf alle Benutzer an. In Abschnitt 8 der vorliegenden Richtlinie geht es um Rechte, die Benutzer hinsichtlich personenbezogener Daten haben können und die im Zentrum der meisten Datenschutzgesetze stehen.

d. *Geschäftsbenutzer.* Bestimmte klar gekennzeichnete Abschnitte der Richtlinie gelten nur für Benutzer, die über ein Konto ihres Arbeitgebers oder einer ähnlichen Einheit auf die Dienste zugreifen (jeweils ein „**Geschäftsbenutzer**" und die Konten jeweils ein „B2B-Konto").

e. *Änderungen*. Wir können die vorliegende Richtlinie jederzeit ändern. Wenn wir es tun, werden wir die aktualisierte Richtlinie auf dieser Seite veröffentlichen und Benutzer per E-Mail oder In-App-Benachrichtigung informieren, falls die Änderungen wesentlicher Art sind.

f. *Kinder*. Die Dienste richten sich nicht an Kinder. Kinder dürfen die Dienste aber im Rahmen eines Familientarifs nutzen. Wenn Sie erfahren, dass ein Kind (basierend auf dem Land, in dem das Kind lebt; in den Vereinigten Staaten bedeutet das eine Person unter 13 Jahren) personenbezogene Daten ohne Zustimmung der Eltern bereitgestellt hat, kontaktieren Sie legal@dashlane.com. Wir werden die entsprechenden Daten dann umgehend aus unseren Systemen entfernen.

g. *Wozu benötigen wir Ihre personenbezogenen Daten*? Wir brauchen bestimmte personenbezogene Daten für die Bereitstellung der Dienste. Sie werden dazu aufgefordert, die Angaben zu machen, um die Apps herunterladen und verwenden zu können. Diese Einwilligung, die Sie jederzeit widerrufen können, dient als Rechtsgrundlage, die wir für die Verarbeitung der personenbezogenen Daten von Nicht-Geschäftsbenutzern benötigen. Sie sind nicht dazu verpflichtet, personenbezogene Daten anzugeben. Möglicherweise können wir die Dienste aber nicht richtig bereitstellen bzw. nicht auf Ihre Anfragen reagieren, wenn Sie keine Angaben machen.

h. *Geschützte Daten*. Diese Richtlinie bezieht sich in erster Linie auf Daten, die Dashlane zur Verarbeitung von Zahlungen, zur Fehlerbehebung, zur Verwaltung von Konten usw. verwendet. Das unterscheidet sich von den Daten, die unsere Benutzer in unseren Diensten speichern („**Geschützte Daten**"). Dashlane kann nicht auf geschützte Daten zugreifen; sie sind mit Schlüsseln verschlüsselt, die für jeden Benutzer eindeutig sind und die wir nicht kennen. Es gibt auch keine „Hintertür" oder einen ähnlichen Mechanismus, mit dem wir auf geschützte Daten zugreifen könnten. Genauere Informationen finden Sie in unserem Whitepaper zum Thema Sicherheit.

2. WELCHE PERSONENBEZOGENEN DATEN ERHEBT DASHLANE (UND WELCHE NICHT)?

Zusammenfassung:
Kalifornische Datenschutzgesetze schreiben vor, dass wir die Arten von personenbezogenen Daten, die wir erfassen, offenlegen müssen. Wir erfassen nicht bei jedem Benutzer alle Daten – zum Beispiel benötigen wir bei Dashlane Free-Benutzern oder Geschäftsbenutzern keine Abrechnungsdaten. In den folgenden Abschnitten finden Sie genauere Informationen zu der Frage, welche Daten wir sammeln und wie wir sie verwenden.

Der Bundesstaat Kalifornien schreibt vor, dass wir offenlegen müssen, ob wir in den folgenden Kategorien personenbezogene Daten erfassen. Dies ist eine allgemeine Übersicht über die Arten von personenbezogenen Daten, die wir erfassen. *Wir erfassen nicht bei jedem Benutzer alle Daten.* In den folgenden Abschnitten der Richtlinie finden Sie Informationen dazu, wie wir diese Daten beziehen und verwenden.

- *Kennungen* umfassen Name, E-Mail-Adresse und Postadresse sowie staatliche Ausweise wie z. B. Führerschein oder Sozialversicherungsnummer. Wir benötigen von jedem Benutzer, der ein Konto erstellen möchte, eine E-Mail-Adresse. Außer in seltenen Fällen (wenn wir Ihre Identität im Zusammenhang mit einer Kontowiederherstellung prüfen müssen) fragen wir Benutzer nie nach staatlichen Ausweisen oder ähnlichen Kennungen. Wenn wir das tun, nutzen wir einen Drittanbieter, um solche Daten zu validieren. Der Anbieter informiert uns nur darüber, ob der Benutzer die Identitätsprüfung bestanden hat oder nicht.
- *Kundendatensätze* überschneiden sich mit Kennungen (Name, Adresse, Ausweise), beinhalten aber auch Elemente wie Zahlungs-, medizinische und Versicherungsdaten. Selbstverständlich verarbeiten wir Zahlungsdaten (z. B. Kreditkartendaten) wie für kostenpflichtige Konten angegeben (bewahren sie jedoch nach der Verarbeitung nicht auf). Intern weisen wir jedem Benutzer eine eindeutige ID zu, die nur in Dashlane-Systemen verwendet wird.

- *Merkmale geschützter Klassifizierungen* wie ethnische Herkunft, Abstammung, sexuelle Orientierung, Familienstand usw. **Wir erfassen solche Daten nicht**.
- *Geschäftliche Daten* wie Datensätze zum Kauf von privatem Eigentum, Produkten oder Dienstleistungen bzw. Kauf- oder Konsumhistorien. Wir erfassen Daten über den Zahlungsverlauf (so zutreffend) und die Frage, welcher Dashlane-Tarif mit einem Benutzer oder Konto verknüpft ist.
- *Biometrische Daten*. **Wir erfassen solche Daten nicht.** Wenn Sie biometrische Daten verwenden, um sich beim Dienst anzumelden, werden diese Daten nur auf dem entsprechenden Gerät genutzt.
- *Internet- oder andere Daten zur Aktivität in elektronischen Netzwerken* wie Browserverlauf, Suchverlauf oder Daten bezüglich der Interaktion eines Verbrauchers mit einer Website, Anwendung oder Anzeige. Wir erfassen IP-Adressen wie nachfolgend beschrieben. Wir erfassen Daten darüber, mit welchen Seiten auf unserer Website Besucher interagieren und welche unserer Anzeigen sie vor dem Besuch der Website ggf. gesehen haben. Anwendungen müssen Websites oder Dienste erkennen können, die Sie besuchen, um Felder korrekt auszufüllen. Das geschieht jedoch lokal auf dem Benutzergerät. Diese Daten sind für Dashlane nur auf aggregierter und anonymer Basis verfügbar. Je nach Kontokonfiguration können Administratoren von Dashlane B2B-Konten bestimmte Daten zu Websites anzeigen, auf die Geschäftsbenutzer in ihrem Konto zugreifen (z. B. Daten dazu, ob Anmeldedaten gefährdet sind).
- *Geolokalisierungsdaten*. Wir erfassen die Ursprungs-IP für alle Benutzer und zudem, mit welchen IP-Adressen ein Benutzer auf die Dienste zugreift. Wir bewahren bei Privatanwendern die IP-Aktivitäten der letzten 45 Tage, bei B2B-Benutzern maximal der letzten 365 Tage auf.
- *Auditive, elektronische, visuelle, thermische, olfaktorische oder ähnliche Daten*. Wir zeichnen Vertriebs-, Support- und Anwenderforschungsanrufe auf, die nur Audio bzw. Audio und Video umfassen können, wenn eine entsprechende Einwilligung vorliegt. Wir speichern solche Daten ggf. bis zu 2 Jahre.
- *Berufliche oder beschäftigungsbezogene Daten*. Wir erfassen diese Daten ggf. für Administratoren von B2B-Konten und potenzielle B2B-Kunden.
- *Ausbildungsdaten, die nicht als öffentlich verfügbar betrachtet werden*. **Wir erfassen solche Daten nicht**.
- Inferenzen, mit denen sich das Profil eines Verbrauchers erstellen lässt, das Vorlieben, Eigenschaften, psychologische Trends, Präferenzen, Veranlagungen, Verhaltensweisen, Einstellungen, Intelligenz, Fähigkeiten oder Eignungen des Verbrauchers widerspiegelt. **Wir erfassen diese Daten nicht bei B2C-Benutzern**.
- *Vertrauliche personenbezogene Daten*. Das beinhaltet viele Elemente, die in den oben genannten Kategorien erfasst werden, wie z. B. Finanz- oder medizinische Daten, Ausweisdaten, Daten zu Rasse und anderen „geschützten" demografischen Aspekten sowie biometrische Daten. Mit Ausnahme von Zahlungsdaten und wenn dies zur Wiederherstellung des Zugriffs auf ein Konto (wie oben beschrieben) erforderlich ist, **erfassen wir solche Daten nicht**.

3. Auf welche Weise erfasst Dashlane personenbezogene Daten?

Zusammenfassung:
Wir erhalten Daten von Ihnen (z. B. beim Erstellen eines Kontos oder Bezahlen eines Abonnements), von anderen (z. B. wenn Sie Ihr Arbeitgeber zu Dashlane einlädt), automatisch von den Apps oder über Cookies (z. B. Region, aus der Sie auf die Apps zugreifen) und von Dritten (z. B. Tools, die die Leistung der Dienste analysieren). Personenbezogene Daten, die wir erfassen, enthalten Ihre E-Mail-Adresse und (bei Abonnments) Zahlungsdaten. Vollständige Zahlungsdaten werden jedoch nur von unseren

Zahlungsabwicklern gespeichert. Wir nutzen technologische Mittel, einschließlich Cookies zur Erfassung von Nutzungsdaten. Weitere Informationen finden Sie in unserer Cookie-Richtlinie.

Wir erfassen Daten wie nachstehend beschrieben:

a. *Von Ihnen bereitgestellte Angaben.*

- Registrierungsdaten. Sie müssen ein Konto erstellen, um eine Anwendung nutzen zu können. Dafür müssen Sie eine gültige E-Mail-Adresse angeben, die als Benutzername für die Dienste dient (es sei denn, Sie sind B2B-Benutzer, der sich per Single Sign-On bzw. **SSO** anmeldet). Möglicherweise geben Sie auch eine Telefonnummer an (zur Einrichtung von Zwei-Faktor-Authentifizierung) und/oder eine zusätzliche E-Mail-Adresse (z. B. für den Fall, dass Sie den Zugriff auf die E-Mail-Adresse verlieren, die Sie zur Anmeldung bei Ihrem Konto verwenden). *Die einzige personenbezogene Angabe, die Sie bei der Eröffnung eines Dashlane Free-Kontos machen müssen, besteht aus Ihrer E-Mail Adresse*. Bei kostenpflichtigen Konten müssen Benutzer Abrechnungsdaten bereitstellen (wie nachfolgend beschrieben). Bei B2B-Konten umfassen Registrierungsdaten den Firmennamen, die Postanschrift (wenn per Rechnung bezahlt wird) und Kontaktdaten des Administrators. **Es ist wichtig, Registrierungsdaten aktuell zu halten**. Wir müssen dazu in der Lage sein, den Kontobesitzer zu prüfen, um auf Support-Anfragen von Benutzern reagieren zu können. Wenn Sie den Zugriff auf die als Kontakt genutzte E-Mail-Adresse oder Telefonnummer verlieren, die mit Ihrem Konto verknüpft ist (so zutreffend), können Sie sich ggf. nicht mehr bei Ihrem Konto anmelden. Möglicherweise können wir Ihnen dann auch nicht weiterhelfen. Wir speichern Registrierungsdaten bis zu 30 Tage nach der Löschung eines Kontos.
- Abrechnungsdaten. Wir greifen auf Dritte zurück, um Zahlungen, die über die Website vorgenommen werden, verarbeiten zu lassen. Wir speichern ggf. partielle Zahlungsdaten (z. B. das Gültigkeitsdatum und die letzten vier Ziffern einer Kreditkarte), um Steuervorschriften einzuhalten und Benutzer zu unterstützen. Ggf. können wir auf den Namen, die Adresse und die Telefonnummer zugreifen, die beim Dienst eines Zahlungsabwicklers mit einer Zahlungsmethode verknüpft sind. Diese Daten werden aber ausschließlich vom Zahlungsabwickler gespeichert. Wir verfügen bei Konten niemals über komplette Zahlungsdaten und empfangen oder speichern auch keine Abrechnungsdaten, wenn Sie für ein Abonnement per Google Play oder Apple App Stores („***App Stores***") bezahlen. Abrechnungsdaten werden nach dem Löschen eines Kontos bis zu 30 Tage gespeichert.
- Master-Passwort. Mit Ausnahme von Benutzern von B2B-Konten, die für SSO-Login konfiguriert sind, und von Benutzern, die ihre Konten für passwortlose Anmeldung konfiguriert haben, muss jeder Benutzer ein „**Master-Passwort**" erstellen, das für den Zugriff auf sein Konto und die Generierung der Verschlüsselungsschlüssel, die ihre geschützten Daten schützen, dient. Je sicherer ein Master-Passwort ist, desto sicherer sind auch die geschützten Daten. Apps speichern Master-Passwörter nicht lokal, es sei denn, sie werden vom Benutzer dazu angewiesen. Wenn Sie Ihr Master-Passwort lokal speichern und Ihr Gerät gestohlen oder kompromittiert wird, können Ihre geschützten Daten offengelegt werden. Dashlane hat niemals Zugriff auf Master-Passwörter.
- Geschützte Daten. Mit unseren Apps können Sie digitale Identitätsdaten verwalten, einschließlich vertraulicher Daten wie Kreditkartennummern und Anmeldedaten für Websites oder Anwendungen. Das und alles, was Sie in den Apps speichern, sind geschützte Daten. Geschützte Daten werden beim Übertragen und Speichern stets verschlüsselt und können ausschließlich lokal auf autorisierten Geräten entschlüsselt werden. **Dashlane kann auf seinen Servern nicht auf geschützte Daten zugreifen, da das Unternehmen keine entsprechenden Entschlüsselungsschlüssel hat (wie oben beschrieben**). Konsultieren Sie unser Whitepaper zum Thema Sicherheit, um mehr zu erfahren.
- Support und Korrespondenz. Es kann sein, dass Sie personenbezogene Daten in Verbindung mit Kundensupport-Anfragen und Anfragen über unsere Website angeben müssen. Kundensupport-Verläufe werden nach dem Löschen eines Kontos bis zu 30 Tage lang gespeichert.

- Feedback. Wenn Sie Feedback geben (zum Beispiel Bewertungen in sozialen Medien, App Stores oder Websites wie Trustpilot bzw. Vorschläge, die im Zusammenhang mit Marktforschung gemacht werden), können wir mit dem Feedback bereitgestellte personenbezogene Daten verwenden, um Ihnen zu antworten. Wir können Feedback wie in den Bedingungen beschrieben unbegrenzt nutzen.
- Anforderung von Produktinformationen. Bestimmte Informationen, die Interessenten („**potenzielle Kunden**“) mit den kommerziellen Angeboten von Dashlane vertraut machen sollen, können erst nach Angabe und Verifizierung einer E-Mail-Adresse über unsere Website angefordert werden.
- Andere Daten. Wir können beim Sammeln von Informationen auch andere Arten von Daten so erfassen, wie von uns beschrieben.

b. *Daten, die Sie über andere angeben.* Mit den Diensten können Sie andere dazu einladen, die Apps zu testen oder Teil Ihres Konto zu werden. Wenn Sie andere einladen (oder auf diese Weise eingeladen werden), wird Dashlane die E-Mail-Adresse des Eingeladenen und die Nachricht speichern, die zum Nachfassen an sie übermittelt wird (und dem Empfehlenden ggf. einen Empfehlungsbonus gutschreiben). Wir werden die eingeladene Person darüber informieren, wer sie empfohlen hat, und ihr die Möglichkeit bieten, ihre Daten auf Anforderung aus unseren Systemen löschen zu lassen. Der Empfehlungsgeber bzw. der Eingeladene kann das Support-Center kontaktieren, um die Löschung seiner Daten zu beantragen.

c. *Technologische Erfassung von Daten.*

- IP-Adresse. Wir erfassen die IP-Adresse, die zur Erstellung eines neuen Kontos verwendet wird, sowie die IP-Adressen, mit denen Benutzer auf die Dienste zugreifen (wie oben beschrieben). Diese Daten werden zur Erbringung und Verbesserung der Dienste und für Compliance-Zwecke genutzt (z. B. Verwendung der Region, die mit einer IP-Adresse verbunden ist, zur Anzeige von lokalen behördlichen Mitteilungen). Die ursprüngliche IP-Adresse wird nach dem Löschen des Kontos bis zu 30 Tage gespeichert. Für den Zugang genutzte IP-Adressen werden bei B2C-Konten 45 Tage lang, bei B2B-Konten bis zu ein Jahr lang gespeichert.
- Geräte- und Browserdaten. Beim Zugriff auf die Dienste oder beim Besuch der Website protokollieren wir automatisch folgende Daten (so zutreffend): Name und Version des Betriebssystems, Gerätekennung, Browsertyp sowie Sprache des Browsers oder Geräts. Manche dieser Daten werden mithilfe von Cookies erfasst, wie in der Cookie-Richtlinie erläutert. Die Daten dienen dazu, Ihr Konto zu schützen, sicherzustellen, dass die Website und Dienste in der richtigen Sprache angezeigt und für Ihr Gerät optimiert werden, und den Kundensupport zu vereinfachen. Diese Daten werden nicht gelöscht, sondern innerhalb von 30 Tagen nach dem Löschen des Kontos anonymisiert.
- Nutzungsdaten. Wir verwenden Protokolle, um Daten über die Nutzung der Dienste („**Nutzungsdaten**“) zu erfassen. Wir pflegen zwei Arten von Nutzungsdaten:
    - „**Ereignisdaten**“ zeichnen die internen Funktionen der Apps auf (z. B. welche Funktionen sind aktiviert, wie viele Anmeldedaten sind in geschützten Daten gespeichert) und dienen dazu, dem Benutzer relevante Informationen und Support zu bieten sowie die Dienste bereitzustellen, zu analysieren und zu verbessern. Ereignisdaten beinhalten keine Informationen dazu, wie die Dienste mit Dritten interagieren (z. B. wissen wir zwar, wie viele Passwörter ein Benutzer hat, wissen aber nicht, welchen Websites oder Diensten die Passwörter zugeordnet sind). Nach dem Löschen eines Kontos werden Ereignisdaten gespeichert, aber vollständig anonymisiert (selbst wenn der gleiche Benutzer ein neues Konto erstellt, können Ereignisdaten aus dem alten Konto nicht mit dem neuen Konto verknüpft werden). Die Speicherung anonymisierter Ereignisdaten ist notwendig, um genaue historische Aufzeichnungen über die Nutzung der Dienste zu erhalten.

- „**Verhaltensdaten**“ sind Daten dazu, was Benutzer abseits der Dienste tun (z. B. Websites, bei denen Autovervollständigen zum Anmelden verwendet wird; für welche Websites oder Apps Benutzer über Anmeldedaten in ihren geschützten Daten verfügen). Verhaltensdaten sind für den ordnungsgemäßen Betrieb der Dienste entscheidend – beispielsweise müssen Apps die Website erkennen, bei der sich ein Benutzer anmeldet, um Anmeldedaten auszufüllen. Bestimmte Verhaltensdaten stehen autorisierten Administratoren von B2B-Konten (jeweils ein „**B2B-Administrator**“) auf individueller Basis zur Verfügung, damit Client-Administratoren die Client-Sicherheit verbessern können (z. B. können B2B-Administratoren sehen, ob die Anmeldedaten eines bestimmten Benutzers kompromittiert wurden). Die Daten sind für Dashlane aber nur vollständig anonymisiert verfügbar (z. B. kann Dashlane sehen, wie viel Prozent aller Benutzer über Anmeldedaten für eine bestimmte Website verfügen, aber nicht, ob einzelne Benutzer Anmeldedaten für diese Website besitzen).

Bestimmte Mitarbeiter von Dashlane haben zwecks Analysen der Nutzung der Dienste Zugriff auf Ereignisdaten und leisten Benutzer- und technischen Support. Sowohl Ereignis- als auch Verhaltensdaten werden von den Diensten genutzt, um automatisch kontextabhängige Warnungen (z. B. Benachrichtigungen zur Kontoeinrichtung) und aggregierte Daten zu generieren.

- Aggregierte Daten. Wir leiten zusätzliche Informationen über die Nutzung der Dienste ab, indem wir Nutzungsdaten aggregieren (z. B. Anzahl der Benutzer in einem bestimmten Land, beliebteste Funktionen). Aggregierte Daten sind anonyme Daten, die Dashlane gehören und in erster Linie dazu dienen, die Dienste zu analysieren und zu verbessern.
- Cookies. Wie in unserer Cookie-Richtlinie beschrieben, verwenden wir Cookies und ähnliche Technologien, um Sie bzw. Ihre Geräte zu erkennen und eine möglichst persönliche und nahtlose Erfahrung bei Interaktionen mit der Website und den Diensten zu ermöglichen. Cookies, die für den Betrieb der Dienste nicht notwendig sind, können hier jederzeit deaktiviert werden.

d. *Von Drittanbietern erhaltene Daten.*

- Geschäftsbenutzer. Wenn Sie B2B-Benutzer sind, kann Ihr B2B-Administrator bei der Kontoerstellung Ihre E-Mail- oder SSO-Daten bereitstellen.
- Dienstanbieter. Wir erhalten von unseren Dienstanbietern Daten über Benutzer (z. B. bei der Validierung eines Kontos durch einen Zahlungsabwickler oder beim Überwachen der Anwendungsleistung mit Analysediensten). Wir können außerdem Benutzerdaten aus öffentlich zugänglichen Quellen wie Social-Media-Konten, Bewertungssites und Foren abrufen. Wir erhalten Informationen über potenzielle Kunden mithilfe von Datenanreicherungsdiensten. Wir prüfen sorgfältig die rechtlichen Bedingungen sowie Geschäfts- und Sicherheitspraktiken aller Dienstanbieter, von denen wir solche Daten erhalten, um sicherzustellen, dass sie geltende Gesetze und die vorliegende Richtlinie einhalten.

4. Wie verwendet Dashlane personenbezogene Daten?

Zusammenfassung:
Wir verwenden personenbezogene Daten zur Validierung Ihres Kontos, zur Bereitstellung der Dienste und dazugehörigen Support-Leistungen, zur Kommunikationen mit Ihnen sowie zur Koordinierung von Marketingmaßnahmen. Wir verwenden personenbezogene Daten nicht für automatisierte Entscheidungen oder die Erstellung von Profilen.

a. *Allgemeines.* Dashlane nutzt personenbezogene Daten, um die Dienste bereitzustellen und zu bewerben und auf Ihre Anfragen zu reagieren, unter anderem für folgende Zwecke:

- Einrichtung, Verwaltung und Sicherung Ihres Kontos.
- Identifizierung von Benutzern und Bereitstellung der jeweils angeforderten Dienste.

- Betrugserkennung und Authentifizierung.
- Messung von Nutzungsdaten zur Verbesserung der Dienste und Ihrer Interaktionen mit den Diensten.
- Versand administrativer Benachrichtigungen, z. B. Zahlungserinnerungen oder Support- und Wartungshinweise. Sie erhalten solche Benachrichtigungen, auch wenn Sie den Erhalt von Marketing-Mitteilungen abgelehnt haben.
- Bereitstellung der Benutzeroberflächen und von Ihnen angefragten Optionen bzw. der gesetzlich vorgeschriebenen Optionen für das Land, von dem aus Sie auf die Dienste zugreifen.
- Bereitstellung von personalisierten Informationen, indem wir feststellen, ob Sie bestimmte Funktionen innerhalb der Dienste verwendet, Seiten auf unserer Website besucht oder eine unserer Werbeanzeigen gesehen haben.
- Beantwortung von Support- und anderen Anfragen.
- Versand von Dashlane-Marketinginformationen, einschließlich Ankündigungen zu Angeboten ausgewählter Dashlane-Partner. Wenn es lokale Gesetze vorschreiben, müssen Benutzer dem Erhalt von Marketing-Mitteilungen zustimmen. Andernfalls werden Marketing-Mitteilungen standardmäßig aktiviert; Benutzer können sie aber jederzeit deaktivieren. Beachten Sie, dass die Abmeldung von Marketing-Mitteilungen keinen Einfluss auf die Bereitstellung von oben beschriebenen administrativen Benachrichtigungen hat.
- Verwaltung von Werbemaßnahmen auf Websites und Plattformen von Drittanbietern, wie nachstehend beschrieben.

b. *Automatisierte Entscheidungsfindung und Erstellung von Profilen.* Wir verwenden keine personenbezogenen Daten für automatisierte Entscheidungen.

5. WIE GIBT DASHLANE PERSONENBEZOGENE DATEN WEITER?

Zusammenfassung:
Wir verkaufen niemals die personenbezogenen Daten unserer Benutzer. Wir teilen personenbezogene Daten mit Dienstleistern, die vertraglich dazu verpflichtet sind, Datenschutzbestimmungen einzuhalten, und nur Zugriff auf jene Daten haben, die sie für die Erbringung der relevanten Dienste benötigen. Sie haben die Möglichkeit, geschützte Daten (einschließlich personenbezogene Daten) auf Ihre ausdrückliche Anweisung über die Dienste an andere weiterzugeben. Wir geben gehashte E-Mail-Adressen und Gerätekennungen von Benutzern an Publisher weiter, um Werbemaßnahmen zu optimieren (z. B. damit aktive Benutzer keine Anzeigen von Dashlane sehen). Wir dürfen personenbezogene Daten an unsere verbundenen Unternehmen weitergeben, die alle an diese Richtlinie gebunden sind, sowie an einen Erwerber im Falle eines Verkaufs oder einer Fusion von Dashlane. Dashlane B2B-Administratoren haben Zugriff auf bestimmte Nutzungsdaten von Benutzern in ihrem Konto. Schließlich können wir personenbezogene Daten offenlegen, wenn dies gesetzlich vorgeschrieben ist oder wenn wir der Überzeugung sind, dass die Offenlegung zum Schutz unserer Rechte oder der Dienste erforderlich ist.

Dashlane wird Ihre personenbezogenen Daten niemals verkaufen (wie „Verkaufen“ normalerweise definiert wird – siehe Abschnitt 8 mit Informationen dazu, wie „Verkaufen“ in Kalifornien definiert wird) oder anders nutzen, als es in der vorliegenden Richtlinie beschrieben ist. Wir geben Ihre personenbezogenen Daten unter den im Folgenden beschriebenen Umständen weiter:

- Von Ihnen benannte Dritte. In den Diensten ist eine Funktion zum Teilen inbegriffen, mit der Sie bestimmte geschützte Daten an andere weitergeben können. Solche Daten werden zwar über unsere Server übertragen, wir haben jedoch – wie in dieser Richtlinie an anderer Stelle dargelegt – keinen Zugriff darauf.
- Dienstanbieter. Wir geben personenbezogene Daten nur an Dienstanbieter weiter, wenn dies für die Bereitstellung der Dienste erforderlich ist, zum Beispiel um Konten zu

erstellen, Kunden-Support zu leisten, Zahlungen abzuwickeln oder die Kommunikation zwischen Ihnen und Dashlane zu ermöglichen (beispielsweise stehen unseren Beauftragten in Zendesk personenbezogene Daten in Bezug auf Kundensupport-Anfragen zur Verfügung). Wir überprüfen die Sicherheits- und Datenschutzpraktiken aller Dienstanbieter, um sicherzustellen, dass sie die geltenden Gesetze und die vorliegende Richtlinie einhalten. Geschützte Daten, die von unserem Datenhosting-Anbieter (AWS) gespeichert werden, werden wie oben beschrieben stets verschlüsselt. Die Liste der beauftragten Datenverarbeiter enthält Informationen darüber, welche Dienstanbieter im Zusammenhang mit unserer Erbringung der Dienste Zugriff auf personenbezogene Daten haben.

- Marketing. Wir stellen Dienstanbietern gehashte E-Mail-Adressen und/oder Gerätekennungen zur Verfügung, um unsere Werbemaßnahmen zu optimieren (z. B. um sicherzustellen, dass aktuellen Benutzern keine Anzeigen für Dashlane auf anderen Websites angezeigt werden). Unsere Vereinbarungen mit diesen Anbietern verhindern, dass diese die von uns bereitgestellten Informationen für andere Zwecke verwenden, einschließlich der Erweiterung der von ihnen gepflegten Profile. Zur Verbesserung von Marketing-Aktivitäten stellen wir Anbietern für Datenanreicherungsleistungen gehashte E-Mail-Adressen potenzieller Kunden zur Verfügung.
- Verbundene Unternehmen. Diese Richtlinie gilt für alle Unternehmen, die Eigentum von Dashlane, Inc. sind oder unter der gemeinsamen Kontrolle von Dashlane, Inc. stehen („**verbundene Unternehmen**"). Wir geben personenbezogene Daten an verbundene Unternehmen weiter, wenn dies zur Bereitstellung der Dienste und zur Beantwortung von Anfragen erforderlich ist. Bestimmte verbundene Unternehmen befinden sich in den USA, wo die datenschutzrelevanten Bestimmungen nach Ansicht der europäischen Aufsichtsbehörden den Schutz von personenbezogenen Daten, die der DSGVO unterliegen, nicht im ausreichenden Umfang gewährleisten. Um das nach europäischem Recht erforderliche Schutzniveau zu bieten, haben wir zusätzlich zu den nachstehend aufgeführten Maßnahmen DSGVO-konforme Zusatzvereinbarungen zur Datenverarbeitung zwischen unseren verbundenen Unternehmen in der EU und den USA abgeschossen.
- Dashlane B2B-Administratoren. Bestimmte B2B-Benutzer haben Zugriff auf zwei „Bereiche" in ihren Anwendungen: einen „Geschäftsbereich", in dem geschützte Daten im Zusammenhang mit ihrer Arbeit gespeichert werden, und einen „privaten Bereich" für alle anderen Daten, die sie in den Diensten speichern möchten. Die Dienste ermöglichen es B2B-Administratoren, Daten über die Nutzung der Dienste durch die mit ihrem Konto verknüpften B2B-Benutzer anzuzeigen, einschließlich Ereignisdaten sowie bestimmter Verhaltensdaten auf individueller Basis. Beispielsweise können B2B-Administratoren die Passwortintegritätsbewertungen für sämtliche Benutzer des betreffenden Unternehmenskontos sowie Informationen zu den Websites bzw. Diensten einsehen, für die der jeweilige Benutzer in seinem Geschäftsbereich Anmeldedaten gespeichert hat, und etwaige Gefährdungen dieser Anmeldedaten erkennen.
- Umstrukturierung des Unternehmens. Wenn Dashlane bzw. der Geschäftsbetrieb oder die Wirtschaftsgüter von Dashlane von einem anderen Unternehmen erworben oder in ein anderes Unternehmen eingegliedert werden, gehen sämtliche personenbezogenen Daten, die wir zu diesem Zeitpunkt besitzen, in den Besitz dieses Unternehmens über, das damit unsere Rechte und Pflichten aus dieser Richtlinie übernimmt. Dementsprechend dürfen wir personenbezogene Daten im Zusammenhang mit einer solchen Transaktion weitergeben. Personenbezogene und andere Daten können auch im Falle der Insolvenz, des Konkurses oder der Zwangsverwaltung von Dashlane als Wirtschaftsgut übertragen werden.
- Sonstige Offenlegungen. Wir werden Sie über alle sonstigen Offenlegungen Ihrer personenbezogenen Daten informieren und vor einer solchen Offenlegung Ihre Zustimmung einholen. Allerdings darf Dashlane Ihre personenbezogenen Daten

unabhängig von den Präferenzen, die Sie für den Umgang mit personenbezogenen Daten angegeben haben, offenlegen, wenn (a) dies zur Einhaltung von Richtlinien zum Gesetzesvollzug, geltenden Gesetzen oder behördlichen Anordnungen erforderlich ist; oder (b) wir nach Treu und Glauben überzeugt sind, dass dies zum Schutz unserer Rechte, der Rechte anderer Benutzer oder der Dienste erforderlich ist. Aufgrund unserer Zero-Knowledge-Architektur ist es uns jedoch nicht möglich, Benutzerinformationen bereitzustellen, bei denen es sich nicht um Anmeldedaten und Ereignisdaten handelt, selbst wenn eine gültige Anordnung dafür vorliegt. Sofern es gesetzlich zulässig ist, informieren wir die jeweils betroffenen Benutzer über gesetzlich angeordnete Offenlegungen personenbezogener Daten.

6. Datensicherheit und internationale Übermittlung

Zusammenfassung:
Wir bemühen uns, die Sicherheit aller in unserem Besitz befindlichen Daten, insbesondere personenbezogener Daten, durch verschiedene Maßnahmen zu gewährleisten und arbeiten kontinuierlich an der Verbesserung und Aktualisierung dieser Praktiken. Wir können jedoch die Sicherheit der von uns verarbeiteten personenbezogenen Daten nicht garantieren. Personenbezogene Daten dürfen in Rechtsordnungen übertragen werden, in denen weniger strenge Datenschutzgesetze gelten als in Ihrem Heimatland, darunter in die USA. Zum Schutz personenbezogener Daten bei der Verarbeitung in den USA wenden wir jedoch technische und sonstige Maßnahmen an, die den jeweils geltenden Vorschriften entsprechen.

a. Wir setzen solide physische, organisatorische, technische und administrative Maßnahmen zum Schutz personenbezogener Daten ein und überprüfen und überarbeiten unsere Richtlinien und Praktiken regelmäßig, um die Sicherheit zu verbessern. Trotz unserer Bemühungen zum Schutz Ihrer personenbezogenen Daten ist keine Methode zur Datenübertragung oder -speicherung absolut sicher. Daher können wir die Sicherheit personenbezogener Daten unter unserer Kontrolle nicht garantieren. Wenn Sie der Meinung sind, dass die Sicherheit Ihrer personenbezogenen Daten von uns oder durch die Nutzung der Dienste gefährdet wurde, wenden Sie sich bitte umgehend an unser Support-Center.
b. Ihre Daten, einschließlich personenbezogener Daten, die wir über Sie erfassen, dürfen von uns, unseren verbundenen Unternehmen und Dienstleistern in Länder außerhalb Ihres Heimatlandes, einschließlich der USA, übertragen, dort gespeichert und verarbeitet werden, wo Datenschutzvorschriften möglicherweise nicht den in anderen Regionen üblichen Schutz bieten. Wenn wir das tun, ergreifen wir alle gesetzlich vorgeschriebenen Maßnahmen, um sicherzustellen, dass alle personenbezogenen Daten, die wir oder unsere Dienstanbieter verarbeiten (unabhängig von ihrem Ursprung), ordnungsgemäß geschützt werden. Durch die Nutzung der Dienste stimmen Sie der Übertragung, Speicherung oder Verarbeitung Ihrer Daten gemäß dieser Richtlinie zu.

7. Wie können Sie Ihre Daten kontrollieren?

Zusammenfassung:
Sie können Ihre personenbezogenen Daten bearbeiten und Ihre Privatsphäre- und Datenschutzeinstellungen in den Bereichen „Konto“ oder „Einstellungen“ der Apps anpassen. Wenn Sie derzeit Marketing-E-Mails erhalten und diese abbestellen möchten, können Sie sich in jeder E-Mail über den entsprechenden Link abmelden. In diesem Fall erhalten Sie weiterhin operative und transaktionsbezogene E-Mails (z. B. zur Verlängerung Ihres Abos). Wenn Sie Apps von Ihren Geräten deinstallieren, werden alle mit den Apps verknüpften Daten entfernt. Durch das Entfernen der Apps wird Ihr Konto nicht gelöscht. Sehen Sie dazu die Anleitung hier. Selbst wenn Sie keinen Datenschutzbestimmungen unterliegen, können Sie die in Abschnitt 8 beschriebenen Verfahren trotzdem zur Kontrolle Ihrer personenbezogenen Daten verwenden.

a. *Ändern Ihrer Daten- und Datenschutzeinstellungen*. Über die Bereiche „Einstellungen“ oder „Konto“ der Apps können Sie auf mit Ihrem Konto verknüpfte personenbezogene Daten

zugreifen und diese ändern sowie Ihre Privatsphäre- und Datenschutzeinstellungen ändern. Wenden Sie sich an unser Support-Center, wenn Sie Unterstützung benötigen.

b. *E-Mail-Kommunikation*. Mit Ihrer Zustimmung senden wir Ihnen regelmäßig E-Mails mit Hinweisen zur Nutzung der Dienste, einschließlich Tipps zur Verwendung der Apps, und Informationen zu Angeboten von ausgewählten Partnern von Dashlane. Sie können diese E-Mails abbestellen, indem Sie den Anweisungen zum Abbestellen in einer beliebigen E-Mail folgen oder Ihre Privatsphäre- und Datenschutzeinstellungen in den Diensten ändern. Sie können die Abbestellung auch über unser Support-Center anfordern. Beachten Sie, dass das Abbestellen von Marketing-Mitteilungen keine Auswirkungen auf operative und transaktionsbezogene Mitteilungen hat, einschließlich Meldungen zur Verletzung der Datensicherheit und anderen Warnungen in den Apps, E-Mails zur Abo-Verlängerung usw.

c. *Anwendungen*. Sie können die Erfassung von Daten durch eine App verhindern, indem Sie diese App deinstallieren. Dazu können Sie das Standardverfahren verwenden, das Ihnen auf Ihrem Gerät oder der entsprechenden Plattform zur Verfügung steht. Durch das Deinstallieren einer App wird Ihr Konto nicht gelöscht. Sehen Sie dazu die Anleitung hier.

8. Rechte aus Datenschutzgesetzen

Zusammenfassung:
Benutzer, die Datenschutzbestimmungen unterliegen, haben bestimmte Rechte bezüglich ihrer personenbezogenen Daten, einschließlich des Rechts auf Zugriff und Änderung personenbezogener Daten, über die Anbieter (wie wir) verfügen, und des Rechts auf „Vergessen" personenbezogener Daten durch Anbieter, wenn die Daten nicht mehr relevant sind. Die meisten dieser Rechte müssen in den Diensten über die Privatsphäre- und Datenschutzeinstellungen aufgerufen werden. Sie können uns jedoch jederzeit um Hilfe bitten. Wir werden ***niemandem*** *schlechtere Dienste bereitstellen oder Personen in irgendeiner Weise bestrafen, die sich für die Ausübung ihrer Rechte entscheiden. Wir unterstützen die Absicht hinter diesen Gesetzen nachdrücklich und werden unser Bestes tun, um Anfragen zur Ausübung der Rechte zu erfüllen, auch wenn sie technisch für Sie nicht gelten.*

a. *Datenverantwortlicher*. Für die Zwecke der DSGVO ist, wenn wir als Datenverantwortlicher handeln, der Verantwortliche Dashlane SAS, 21 Rue Pierre Picard, 75018 Paris, Frankreich. Anfragen zur Verarbeitung der Daten betroffener Personen gemäß der DSGVO können an unseren Datenschutzbeauftragten gesendet werden unter dpo@dashlane.com.

b. *Verkauf und Weitergabe von personenbezogenen Daten*. Wir tauschen personenbezogenen Daten niemals gegen Geld oder sonstige Leistungen (z. B. Tausch gegen kostenlose Dienstleistungen). Wenn Sie aber auf eine Anzeige klicken, die Sie zur Website weiterleitet, senden wir eine eindeutige Kennung an die weiterleitende Website, damit diese eine Gutschrift für die Weiterleitung erhalten kann. Dies gilt gemäß den Datenschutzgesetzen von Kalifornien als „Teilen". Sie können diese Einstellung deaktivieren, indem Sie die Seite Meine personenbezogenen Daten weder teilen noch verkaufen aufrufen.

c. Personen, die Datenschutzgesetzen unterliegen, haben einige oder alle der folgenden Rechte bezüglich ihrer personenbezogenen Daten, die wir verarbeiten. Wie bereits erwähnt, werden wir diese Anfragen durch beliebige Benutzer unter Beachtung der Anforderungen der relevanten Datenschutzgesetze (so zutreffend) ausführen. Beispielsweise kann ein B2B-Benutzer, der der DSGVO unterliegt, von uns verlangen, dass wir seine Daten löschen. In dem Fall ist das Unternehmen, mit dessen Konto der Benutzer verknüpft ist, der „Verantwortliche" dieser personenbezogenen Daten, sodass wir den zuständigen B2B-Administrator informieren und seinen Anweisungen folgen müssen.

- Widerruf der Einwilligung: Sie können Ihre Einwilligung zur Verarbeitung Ihrer personenbezogenen Daten durch uns (z. B. zu Marketing-Zwecken) ganz oder teilweise widerrufen. Manche Dienste können nach einem solchen Widerruf unwirksam werden.

- Zugriff auf/Anforderung von Daten: Sie dürfen auf die von uns gespeicherten personenbezogenen Daten jederzeit über Ihr Konto oder durch direkte Kontaktaufnahme mit uns zugreifen.
- Änderung: Sie dürfen die über Sie gespeicherten personenbezogenen Daten jederzeit über Ihr Konto oder durch direkte Kontaktaufnahme mit uns ändern, wenn diese falsch oder nicht mehr aktuell sind.
- Löschen und Vergessen. In bestimmten Situationen, z.B. wenn Registrierungsdaten, die wir über Sie gespeichert haben, nicht mehr relevant oder korrekt sind, können Sie verlangen, dass wir diese löschen. Wenn Sie Ihr Konto löschen, werden alle personenbezogenen Daten innerhalb von 30 Tagen nach dem Datum der Löschung automatisch gelöscht. **Aufgrund der vertraulichen Natur von geschützten Daten werden wir das Konto eines Benutzers niemals selbst löschen: Konten MÜSSEN vom Benutzer oder dem „Verantwortlichen" oder einer gleichwertigen Person gelöscht werden.**
- Übertragbarkeit: Sie haben das Recht, eine Kopie Ihrer personenbezogenen Daten anzufordern und diese auf Wunsch jederzeit an andere Entitäten zu übertragen. Die Dienste ermöglichen es Ihnen, geschützte Daten jederzeit zu exportieren.

d. Wenn Sie eines dieser Rechte ausüben möchten, senden Sie die Anfrage bitte über die Seite „Privatsphäre- und Datenschutzeinstellungen" in den Bereichen „Konto" oder „Einstellungen" der Anwendungen (wenn Sie das nicht direkt in den Bereichen erledigen können). Wenn Sie Hilfe benötigen, besuchen Sie bitte unser Support-Center oder schreiben Sie uns an die unten stehende Adresse. In Ihrer Anfrage machen Sie bitte klar: (i) **um welche** personenbezogenen Daten es geht und (ii) **welche Rechte** Sie wahrnehmen möchten. Zu Ihrem Schutz dürfen wir Anfragen bezüglich personenbezogener Daten nur in Verbindung mit der E-Mail-Adresse erfüllen, von der Sie Ihre Anfrage senden. Möglicherweise müssen wir Ihre Identität vor der Ausführung überprüfen. Wir werden Ihre Anfrage umgehend erfüllen, aber in jedem Fall innerhalb der gesetzlich vorgeschriebenen Fristen (z. B. dreißig (30) Tage bei der DSGVO und fünfundvierzig (45) Tage beim CPRA). Wenn Sie keinen Datenschutzgesetzen unterliegen, versuchen wir, alle Anfragen dennoch innerhalb von 45 Tagen zu erfüllen. Wir werden begrenzte personenbezogene Daten für Aufzeichnungszwecke oder zur Durchführung von Transaktionen speichern, die Sie vor dem Stellen bestimmter Anfragen begonnen haben.

e. Wir benachteiligen keinen Benutzer (z. B. indem wir Dienste in schlechterer Qualität anbieten oder mehr dafür verlangen), der eines der oben genannten Rechte ausübt.

9. Kontaktangaben; Beschwerden

Wenn Sie Fragen, Bedenken oder Beschwerden zu dieser Richtlinie oder unseren Verfahren zur Erfassung und Verarbeitung von Daten haben oder Sicherheitsverletzungen melden möchten, wenden Sie sich an unser Support-Center, schicken Sie eine E-Mail an legal@dashlane.com bzw. dpo@dashlane.com oder schreiben Sie an folgende Adresse:

Dashlane, Inc.
Attn: Legal
44 West 18th Street., 4th Fl.
New York, NY 10011, USA

Nur Benutzer in der Schweiz, der EU und im Vereinigten Königreich. Wir hoffen, dass wir alle Beschwerden umgehend beheben können, die uns zur Kenntnis gebracht werden. Wenn Sie jedoch der Meinung sind, dass Ihre Beschwerde nicht ausreichend gelöst wurde, können Sie sich jederzeit an Ihre lokale Datenschutzbehörde wenden. Eine Liste der Datenschutzbehörden ist hier abrufbar.