Dashlane Privacybeleid

Hieronder vindt u ons Privacybeleid. U moet dit beleid accepteren als u onze software wilt gebruiken, maar we zijn ons ervan bewust dat het een moeilijk te volgen onderwerp kan zijn. Om voor u begrijpelijk te maken waar u akkoord mee gaat, begint elk artikel met een korte 'niet-juridische' samenvatting. De samenvattingen maken technisch geen onderdeel uit van het beleid.

LAATST BIJGEWERKT: 15 maart 2024

1. INLEIDING

Samenvatting:
Dit Beleid beschrijft hoe we Persoonsgegevens (die kunnen worden gebruikt om een specifieke persoon te identificeren) en Anonieme Gegevens (die dat niet kunnen) over onze gebruikers verzamelen en gebruiken. Sommige gedeelten van het beleid zijn alleen van toepassing op specifieke gebruikers, zoals werknemers die Dashlane gebruiken op een door een werkgever aangeboden abonnement. We kunnen dit Beleid te allen tijde wijzigen door het herziene Beleid hier te publiceren. We zullen huidige gebruikers ook op de hoogte brengen van belangrijke wijzigingen via e-mail of in-app-berichten. Hoewel we bepaalde persoonsgegevens nodig hebben om de diensten te leveren, proberen we alleen te verzamelen wat we nodig hebben. We zullen persoonsgegevens van kinderen die geen geautoriseerde gebruikers zijn (bijvoorbeeld kinderen die geen deel uitmaken van een gezinsabonnement) verwijderen als daarom wordt gevraagd. ***Vanwege onze zero-knowledgearchitectuur weten we niet en kunnen we ook niet weten welke informatie u op de diensten opslaat.***

a. *Algemeen*. Dit privacybeleid (het "**Beleid**") beschrijft hoe Dashlane, Inc. en zijn gelieerde ondernemingen ("**Dashlane**" of "**wij**") informatie over bezoekers van onze website op www.dashlane.com (samen met de subdomeinen, zoals de blog van Dashlane, de "**Site**") en gebruikers van onze webextensies en mobiele en webapplicaties (elk een "**app**" en gezamenlijk de "**apps**"), worden verzameld, gebruikt en gedeeld. De apps en de site zijn samen de "**diensten**". "**U**" of de "**gebruiker**" verwijst naar iedereen die de diensten gebruikt of de site bezoekt. Woorden die in dit beleid worden gebruikt, maar niet zijn gedefinieerd, hebben de betekenissen die worden gegeven in onze dienstvoorwaarden (de "**voorwaarden**").

b. *Persoonlijke en anonieme gegevens*. "**Persoonsgegevens**" betekent informatie die, op zichzelf staand of in combinatie met andere informatie in het bezit van de houder, een individu identificeert, zoals naam, postadres, e-mailadres, IP-adres of telefoonnummer. "**Anonieme gegevens**" zijn gegevens die niet kunnen worden gebruikt om individuen te identificeren. We verzamelen en gebruiken zowel persoonlijke als anonieme gegevens zoals hieronder beschreven.

c. *Privacywetgeving*. Een toenemend aantal wetten, zoals de Californische privacyrechtenwet ("**CPRA**") en de algemene wetgeving inzake gegevensbescherming van de Europese Unie ("**GDPR**"), regelen hoe entities persoonsgegevens verzamelen, opslaan en gebruiken (gezamenlijk "**privacywetten**"). Privacywetten geven personen bepaalde rechten om te weten en te controleren hoe bedrijven hun persoonsgegevens gebruiken. We stellen ons beleid zo op dat het zoveel mogelijk voldoet aan de meest beschermende privacywetten en we passen dit beleid toe op alle gebruikers. Sectie 8 van dit beleid gaat specifiek in op de rechten die gebruikers kunnen hebben over hun persoonsgegevens die de kern vormen van de meeste privacywetten.

d. *Zakelijke gebruikers.* Bepaalde duidelijk gemarkeerde secties van het beleid zijn alleen van toepassing op gebruikers die toegang hebben tot de diensten via een account die is verstrekt door hun werkgever of soortgelijke entiteit (elk, een "**Zakelijke gebruiker**" en dergelijke accounts, een "B2B-account").

e. *Wijzigingen*. Wij kunnen dit beleid te allen tijde wijzigen. Wanneer we dit doen, zullen we het bijgewerkte beleid op deze pagina plaatsen en gebruikers op de hoogte brengen via e-mail of in-app-berichten.

f. *Kinderen*. De diensten zijn niet gericht op kinderen, maar kinderen kunnen de diensten gebruiken als leden van een Family-abonnement. Als u zich ervan bewust wordt dat een kind (op basis van de jurisdictie waar het kind woont, wat in de Verenigde Staten betekent dat iemand jonger is dan 13 jaar) persoonsgegevens heeft verstrekt zonder toestemming van de ouders, neem dan contact op met legal@dashlane.com. We zullen de informatie dan snel uit onze systemen verwijderen.

g. *Waarom hebben we uw persoonsgegevens nodig*? We hebben een aantal persoonsgegevens nodig om de diensten te leveren. U wordt gevraagd om deze informatie te verstrekken om de apps te downloaden en te gebruiken. Deze toestemming, die u op elk moment kunt intrekken, biedt de rechtsgrondslag die we nodig hebben om de persoonlijke gegevens van niet-zakelijke gebruikers te verwerken. U bent niet verplicht om persoonsgegevens te verstrekken, maar we kunnen de diensten niet leveren of reageren op vragen als u dat niet doet.

h. *Beveiligde gegevens*. Dit beleid heeft voornamelijk betrekking op gegevens die Dashlane gebruikt om betalingen te verwerken, problemen op te lossen, accounts te beheren, enz. Dit staat los van de informatie die onze gebruikers opslaan op onze diensten ("**Beveiligde** gegevens"). Dashlane heeft geen toegang tot beveiligde gegevens; deze zijn versleuteld met sleutels die uniek zijn voor elke gebruiker en die niet in ons bezit zijn. Er is ook geen "backdoor" of een gelijkwaardig mechanisme dat ons toegang geeft tot beveiligde gegevens. Bekijk onze whitepaper over beveiliging voor gedetailleerde informatie.

2. WELKE PERSOONSGEGEVENS WORDEN WEL (EN NIET) DOOR DASHLANE VERZAMELD?

Samenvatting:
De privacywetten van Californië vereisen dat we de soorten persoonsgegevens die we verzamelen openbaar maken. We verzamelen niet alles van elke gebruiker. We hebben namelijke geen factuurgegevens nodig voor "gratis" of zakelijke gebruikers van Dashlane. De volgende secties geven meer informatie over wat we verzamelen en hoe we deze gebruiken.

Californië vereist dat we bekendmaken of we persoonsgegevens verzamelen in elk van de onderstaande categorieën. Dit is een algemeen overzicht van de soorten persoonsgegevens die we verzamelen; *we verzamelen niet alle gegevens voor elke gebruiker.* Bekijk de volgende secties van het beleid voor meer informatie over hoe we deze informatie verkrijgen en gebruiken.

- *Identificatiecodes* omvatten naam, e-mailadres en postadres, evenals door de overheid uitgegeven identificatiegegevens zoals een rijbewijs of burgerservicenummer. We hebben een e-mailadres van elke gebruiker nodig om een account te maken. Behalve in zeer zeldzame situaties (wanneer we uw identiteit moeten verifiëren in verband met accountherstel), vragen we nooit om identiteitskaarten van de overheid of vergelijkbare informatie van gebruikers. Wanneer we dit doen, gebruiken we een derde partij om dergelijke informatie te verifiëren. De provider laat ons alleen weten of de gebruiker de identiteitscontrole heeft gepasseerd of heeft gefaald.
- *Klantgegevens* overlappen met identificatiegegevens (naam, adres, identiteitskaart), maar omvatten ook dingen zoals betaling, medische gegevens en verzekeringsinformatie. Uiteraard verwerken we betaalgegevens (bijvoorbeeld een creditcard) zoals vereist is voor betaalde accounts (maar we bewaren deze niet na verwerking). Intern wijzen we elke gebruiker een unieke ID toe die alleen binnen Dashlane-systemen wordt gebruikt.
- *Kenmerken van beschermde classificaties* zoals ras, afkomst, sexuele oriëntatie, burgerlijke staat, enz. **We verzamelen deze informatie niet**.
- *Commerciële informatie* zoals gegevens over persoonlijke eigendommen, gekochte producten of diensten of aankoop- of consumptiegeschiedenissen. We verzamelen

informatie over de betalingsgeschiedenis (indien van toepassing) en welk Dashlane-abonnement is gekoppeld aan een gebruiker of account.

- *Biometrische informatie*. **We verzamelen deze informatie niet.** Als u biometrische gegevens gebruikt om in te loggen op de dienst, wordt deze informatie alleen gebruikt op het apparaat.
- Informatie over *internet- of andere elektronische netwerkactiviteit* zoals browsegeschiedenis, zoekgeschiedenis of informatie over de interactie van een consument met een website, applicatie of reclame. We verzamelen IP-adressen zoals hieronder vermeld. We verzamelen informatie over met welke pagina's op de site een bezoeker interageert, en welke van onze advertenties (indien van toepassing) ze hebben gezien voordat ze de site bezochten. Apps moeten sites of diensten kunnen herkennen die u bezoekt om velden correct automatisch in te vullen, maar dit vindt lokaal plaats, op het apparaat van de gebruiker. Deze informatie is echter alleen beschikbaar voor Dashlane op geaggregeerde, anonieme basis. Afhankelijk van de accountconfiguratie kunnen beheerders van B2B-accounts van Dashlane sommige informatie bekijken (bijvoorbeeld of toegangsgegevens zijn gecompromitteerd) over sites die zakelijke gebruikers via hun account hebben bezocht.
- *Geolocatiegegevens*. We verzamelen het oorspronkelijke IP-adres voor alle gebruikers en vanaf welke IP-adressen de gebruiker toegang heeft tot de Diensten. We bewaren de meest recente IP-activiteit gedurende 45 dagen voor consumentengebruikers en tot één jaar voor B2B-gebruikers.
- *Audio, elektronische, visuele, thermische, reukkrachtige of soortgelijke informatie*. We nemen verkoop-, ondersteunings- en gebruikersonderzoeksgesprekken op, die alleen audio of audio en video kunnen zijn, met bevestigende toestemming. We kunnen deze informatie bewaren voor maximaal 2 jaar.
- *Professionele of werkgerelateerde informatie*. We verzamelen deze informatie voor beheerders van B2B-accounts en toekomstige B2B-klanten.
- *Onderwijsinformatie die niet als openbaar beschikbaar wordt beschouwd*. **We verzamelen deze informatie niet**.
- Afwegingen die een profiel kunnen maken over een consument die de voorkeuren, kenmerken, psychische trends, voorkeuren, aanleg, gedrag, attitudes, intelligentie, vaardigheden of aptitudes van de consument weerspiegelt. **We verzamelen deze informatie niet van B2C-gebruikers**.
- *Gevoelige persoonlijke informatie*. Dit omvat veel items die vallen in de bovenstaande categorieën, zoals financiële of medische accountinformatie, informatie over de overheid, raciale en andere "beschermde" demografische informatie en biometrische informatie. Behalve voor betaalgegevens en wanneer dit vereist is om de toegang tot een account te herstellen zoals hierboven vermeld, **verzamelen we deze informatie niet**.

3. HOE VERZAMELT DASHLANE UW GEGEVENS?

Samenvatting:
We krijgen gegevens van u (bijvoorbeeld wanneer u een account maakt of betaalt voor een abonnement), van anderen (bijvoorbeeld wanneer u door uw werkgever wordt uitgenodigd om Dashlane te gebruiken), automatisch van de apps of via cookies (bijvoorbeeld de regio waaruit u toegang hebt tot de apps) en van derden (zoals tools die de prestaties van de diensten evalueren). Persoonsgegevens die we verzamelen omvatten uw e-mail en (voor abonnementen) factureringsinformatie, hoewel volledige betalingsinformatie alleen wordt opgeslagen door onze betalingsverwerkers. We gebruiken technologie, waaronder cookies, om gebruiksgegevens te verzamelen. Aanvullende informatie is beschikbaar in ons cookiebeleid.

Wij verzamelen gegevens op de volgende wijze:

a. *Informatie die u verstrekt.*

- Registratiegegevens. U moet een account maken om een app te gebruiken en om dit te doen, moet u een geldig e-mailadres opgeven dat wordt gebruikt als uw login voor de Diensten (tenzij u een B2B-gebruiker bent die inlogt via eenmalige aanmelding op "**SSO**"). U kunt ook een telefoonnummer opgeven (om tweeledige verificatie in te stellen) en / of een extra e-mail (bijvoorbeeld als u de toegang verliest tot de e-mail die wordt gebruikt om in te loggen op uw account). *De enige persoonsgegevens die vereist zijn om een Dashlane Free-account te openen, zijn uw e-mail*. Voor betaalde accounts moeten gebruikers factureringsgegevens verstrekken zoals hieronder gespecificeerd. Voor B2B-accounts omvatten de registratiegegevens de bedrijfsnaam, het postadres (indien u per factuur betaalt) en de contactgegevens van de beheerder. **Het is van cruciaal belang om registratiegegevens actueel te houden**. We moeten in staat zijn om de accounteigenaar te verifiëren om te reageren op verzoeken om ondersteuning van gebruikers. Als u de toegang verliest tot het e-mailadres of het telefoonnummer van uw account (indien van toepassing), wordt u mogelijk buitengesloten van uw account en kunnen we u mogelijk niet helpen. We bewaren registratiegegevens voor maximaal 30 dagen na verwijdering van het account.
- Factureringsgegevens. We gebruiken derden om betalingen die via de site zijn gedaan te verwerken. We kunnen gedeeltelijke betalingsinformatie opslaan (zoals de vervaldatum en de laatste vier cijfers van een creditcard) voor belastingnaleving en gebruikersondersteuningsdoeleinden. We hebben mogelijk toegang tot de naam, het adres en het telefoonnummer geassocieerd met een betaalmethode op de dienst van een betalingsverwerker, maar deze informatie wordt alleen opgeslagen door de verwerker. We hebben nooit volledige betalingsinformatie voor accounts en we ontvangen of bewaren ook factureringsgegevens als u voor een abonnement betaalt via de Google Play of Apple App Stores ("***App Stores***"). Factureringsgegevens worden bewaard voor maximaal 30 dagen na verwijdering van het account.
- Masterwachtwoord. Behalve voor gebruikers van B2B-accounts die zijn geconfigureerd voor SSO-login en gebruikers die hun accounts hebben geconfigureerd voor een wachtwoordloze login, moet elke gebruiker een "**masterwachtwoord**" maken, dat wordt gebruikt om toegang te krijgen tot hun account en om de versleutelingssleutels te genereren die hun beveiligde gegevens beschermen. Hoe veiliger een masterwachtwoord is, hoe veiliger beveiligde gegevens zullen zijn. Apps slaan geen masterwachtwoorden lokaal op, tenzij dit door de gebruiker wordt aangegeven. Als u dit doet en uw apparaat is gestolen of gecompromitteerd, kunnen uw beveiligde gegevens worden blootgesteld. Dashlane heeft nooit toegang tot masterwachtwoorden.
- Beveiligde gegevens. Met onze apps kunt u digitale identiteitsgegevens beheren, waaronder gevoelige informatie zoals creditcardnummers en site- of applicatie-inloggegevens. Dit en alles wat u opslaat op de apps, zijn beveiligde gegevens. Beveiligde gegevens worden altijd versleuteld wanneer verzonden en opgeslagen en mogen alleen lokaal worden gedecodeerd op een geautoriseerd apparaat. **Dashlane heeft geen toegang tot beveiligde gegevens op onze servers omdat we niet over de versleutelingssleutels beschikken zoals hierboven vermeld**. Bekijk onze whitepaper over beveiliging voor meer informatie.
- Ondersteuning en correspondentie. U kunt persoonsgegevens verstrekken in verband met verzoeken om klantenservice en vragen van onze site. Klantenondersteuningsgeschiedenissen worden bijgehouden voor maximaal 30 dagen na verwijdering van het account.
- Feedback. Als u feedback verstrekt, waaronder recensies die zijn gepost op sociale kanalen, app stores of sites zoals Trustpilot, of suggesties die zijn gedaan in verband met marktonderzoek, kunnen we persoonsgegevens die met de feedback zijn verstrekt gebruiken om op u te reageren. We kunnen feedback gebruiken zonder beperking zoals beschreven in de voorwaarden.
- Verzoeken om productinformatie. Bepaalde informatie die bedoeld is om potentiële klanten van het zakelijke aanbod van Dashlane ('**Zakelijke Prospects**') te informeren, is alleen beschikbaar op de Site na het verstrekken van een geverifieerd e-mailadres.

- Andere gegevens. We kunnen ook andere soorten gegevens verzamelen op de door ons aangegeven wijze op het moment dat deze gegevens worden verzameld.

b. *Gegevens die u verstrekt over anderen.* Met de diensten kunt u anderen uitnodigen om de apps te proberen of zich bij uw account aan te melden. Als u dit doet (of op deze manier bent uitgenodigd), slaat Dashlane het e-mailadres van de genodigde en het bericht dat naar hem is verzonden op te volgen (en, indien van toepassing, de verwijzer te crediteren met een verwijzingsbonus). We zullen de genodigde laten weten wie hen heeft doorverwezen en laten ze vragen om hun informatie uit onze systemen te verwijderen. De verwijzer of genodigde kan contact opnemen met het ondersteuningscentrum om verwijdering van deze informatie te vragen.

c. *Technologisch verzamelde gegevens.*

- IP-adres. We verzamelen het IP-adres dat wordt gebruikt om een nieuw account te maken en de IP-adressen van waaruit gebruikers toegang hebben tot de Diensten zoals hierboven beschreven. Deze gegevens worden gebruikt om de diensten te leveren en te verbeteren en voor nalevingsdoeleinden (bijvoorbeeld het gebruik van de regio geassocieerd met een IP-adres om lokale kennisgevingen van regelgeving weer te geven). Het oorspronkelijke IP-adres wordt tot 30 dagen na verwijdering van het account bewaard. Toegangs-IP's worden 45 dagen bewaard voor B2C-accounts en voor maximaal één jaar voor B2B-accounts.
- Apparaat- en browsergegevens. We loggen automatisch de volgende informatie (voor zover van toepassing) wanneer u toegang hebt tot de diensten of de site bezoekt: naam en versie van het besturingssysteem, apparaat-id, browsertype en browser of apparaattaal. Sommige van deze gegevens worden verzameld met behulp van cookies, zoals uitgelegd in het cookiebeleid. Deze gegevens worden gebruikt om uw account te beveiligen, ervoor te zorgen dat de site en diensten worden gepresenteerd in de juiste taal en geoptimaliseerd voor uw apparaat en klantenondersteuning te faciliteren. Deze gegevens worden niet verwijderd, maar worden geanonimiseerd binnen 30 dagen na verwijdering van het account.
- Gebruiksgegevens. We gebruiken logboeken om gegevens te verzamelen over het gebruik van de diensten ("**Gebruiksgegevens**"). We handhaven twee soorten gebruiksgegevens:
    - "**Evenementgegevens**" registreert de interne functies van de apps (bijvoorbeeld welke functies zijn ingeschakeld, hoeveel inloggegevens worden opgeslagen in beveiligde gegevens) en wordt gebruikt om relevante informatie en ondersteuning te bieden aan de gebruiker en om de diensten te leveren, te analyseren en te verbeteren. Gebeurtenisgegevens bevatten geen informatie over de interactie tussen de Services en derden (we weten bijvoorbeeld wel hoeveel wachtwoorden een gebruiker heeft, maar niet voor welke sites of services deze wachtwoorden zijn). Nadat een account is verwijderd, worden evenementgegevens bewaard, maar worden volledig geanonimiseerd (zelfs als dezelfde gebruiker een nieuw account heeft gemaakt, kunnen evenementgegevens van het oude account niet worden geassocieerd met het nieuwe). Bewaring van geanonimiseerde gegevens van gebeurtenissen is noodzakelijk om nauwkeurige historische gegevens bij te houden over het gebruik van de diensten.
    - "**Gedragsgegevens**" zijn informatie over wat gebruikers doen buiten de diensten (bijvoorbeeld sites waar automatisch invullen wordt gebruikt om in te loggen; voor welke sites of apps een gebruiker inloggegevens heeft in hun beveiligde gegevens). Gedragsgegevens zijn van cruciaal belang voor de goede werking van de diensten – Apps moeten de site herkennen waarop een gebruiker inlogt om de toegangsgegevens te vullen, bijvoorbeeld. Sommige gedragsgegevens zijn beschikbaar voor geautoriseerde beheerders van B2B-accounts (elk, een "**B2B-beheerder**") op individuele basis om clientbeheerders in staat te stellen de beveiliging van klanten te verbeteren (B2B-beheerders kunnen bijvoorbeeld zien of een individuele gebruiker gecompromitteerde toegangsgegevens heeft), maar zijn alleen beschikbaar voor Dashlane op een volledig geanonimiseerde basis (bijv. Dashlane kan

zien welk percentage van alle gebruikers inloggegevens heeft voor een specifieke site, maar niet of een individuele gebruiker inloggegevens heeft voor die site).

Bepaalde Dashlane-medewerkers hebben toegang tot Gebeurtenisgegevens om het gebruik van de Diensten te analyseren en gebruikers- en technische ondersteuning te bieden. Zowel Gebeurtenisgegevens als Gedragsgegevens worden door de Diensten gebruikt om automatisch bij de context passende waarschuwingen te genereren (bijv. meldingen voor accountconfiguratie) en om geaggregeerde gegevens te genereren.

- Geaggregeerde gegevens. We leiden extra informatie af over het gebruik van de diensten door gebruiksgegevens te aggregeren (bijvoorbeeld aantal gebruikers binnen een specifiek rechtsgebied, meest populaire functies). Geaggregeerde gegevens zijn anonieme gegevens, zijn eigendom van Dashlane en worden voornamelijk gebruikt om te helpen bij het analyseren en verbeteren van de diensten.
- Cookies. Zoals beschreven in ons Cookiebeleid gebruiken we cookies en soortgelijke technologieën om u en/of uw apparaat of apparaten te herkennen en een meer persoonlijke en naadloze ervaring te bieden wanneer u de Site en de Diensten gebruikt. Cookies die niet essentieel zijn voor de werking van de diensten kunnen hier op elk moment worden uitgeschakeld.

d. *Van derden verkregen gegevens.*

- Zakelijke gebruikers. Als u een B2B-gebruiker bent, kan uw B2B-beheerder uw e-mail of SSO-informatie verstrekken als onderdeel van het maken van een account.
- Dienstverleners. We ontvangen informatie over gebruikers van onze serviceproviders (zoals bij het valideren van een account met een betalingsverwerker of bij het monitoren van app-prestaties met evaluatiediensten). We kunnen ook gebruikersinformatie verkrijgen van openbaar beschikbare bronnen zoals sociale-media-accounts, reviewsites en forums. We verkrijgen informatie over zakelijke vooruitzichten van gegevensverrijkingsdiensten. We controleren de juridische voorwaarden en zakelijke en beveiligingspraktijken van alle serviceproviders van wie we deze informatie ontvangen om ervoor te zorgen dat ze voldoen aan de toepasselijke wetten en dit beleid.

4. HOE GEBRUIKT DASHLANE PERSOONLIJKE GEGEVENS?

Samenvatting:
Wij gebruiken Persoonsgegevens om uw Account te valideren, de Diensten te verlenen en ondersteuning te bieden, met u te communiceren en marketingactiviteiten te coördineren. We voeren geen geautomatiseerde besluitvorming of profilering uit met behulp van persoonsgegevens.

a. *Algemeen.* Dashlane gebruikt persoonsgegevens om de diensten te leveren en te promoten en om te reageren op uw verzoeken, inclusief:

- Het aanmaken, onderhouden en beveiligen van uw account.
- Het identificeren van u als gebruiker en het verlenen van de door u verzochte Diensten.
- Het uitoefenen van fraudedetectie en authenticatie.
- Het meten van gebruiksgegevens en om de diensten en uw interacties daarmee te verbeteren.
- Verzending van administratieve mededelingen naar u, zoals betalingsherinneringen of ondersteunings- en onderhoudsadviezen. U ontvangt deze kennisgevingen, zelfs als u zich afmeldt voor marketingcommunicatie.
- Het verstrekken aan u van interfaces en opties die u aanvraagt of vereist worden door het rechtsgebied van waaruit u bij de diensten inlogt.

- Het verstrekken van gepersonaliseerde informatie door vast te stellen of u specifieke functies binnen de Diensten hebt gebruikt, pagina's op onze site hebt bezocht of een van onze advertenties hebt gezien.
- Het beantwoorden van ondersteuningsvragen en andere verzoeken.
- Stuur marketinginformatie van Dashlane, waaronder aankondigingen over aanbiedingen van geselecteerde Dashlane-partners. Waar vereist door lokale wetten, moeten gebruikers zich aanmelden om marketingcommunicatie te ontvangen. Anders wordt marketingcommunicatie standaard geactiveerd, maar gebruikers kunnen zich altijd afmelden voor deze communicatie. Let op: als u zich afmeldt voor marketingcommunicatie heeft dit geen invloed op de levering van administratieve meldingen zoals hierboven beschreven.
- Het beheren van reclameactiviteiten op sites en platformen van derden, zoals hieronder wordt beschreven.

b. *Geautomatiseerde besluitvorming en profilering.* We gebruiken geen persoonsgegevens voor geautomatiseerde besluitvorming.

5. HOE GAAT DASHLANE OM MET PERSOONSGEGEVENS?

Samenvatting:
Wij verkopen de Persoonsgegevens van onze gebruikers nooit. We wisselen persoonsgegevens met dienstverleners die contractueel verplicht zijn om te voldoen aan privacywetten en die alleen toegang hebben tot de gegevens die ze nodig hebben om de relevante diensten te leveren. De Diensten stellen u in staat Beveiligde Gegevens (waaronder mogelijk Persoonsgegevens) met anderen te delen als u daartoe instructies geeft. We delen gehashte e-mailadressen en apparaat-ID's van gebruikers met adverteerders om de reclame-inspanningen te verfijnen (zodat actieve gebruikers geen Dashlane-advertenties te zien krijgen). We kunnen Persoonsgegevens delen met onze gelieerde ondernemingen, die allemaal gebonden zijn door dit Beleid, en met een overnemer als Dashlane wordt verkocht of fuseert. B2B-beheerders van Dashlane hebben toegang tot sommige gebruiksgegevens van gebruikers in hun account. Tot slot kunnen wij Persoonsgegevens verstrekken wanneer dit vereist wordt door de wet of wanneer wij dit noodzakelijk achten om onze rechten of de Diensten te beschermen.

Dashlane zal uw Persoonsgegevens nooit verkopen (in de zin waarin "verkopen" normaal wordt gedefinieerd – zie Artikelen 2(b) en 8 voor informatie over "verkopen" zoals gedefinieerd in Californië) of op een andere manier gebruiken dan vermeld in dit Beleid. We delen uw Persoonsgegevens alleen in de volgende omstandigheden:

- Door u aangewezen derden. U kunt de "deel"-functie van de diensten gebruiken om zekere beveiligde gegevens beschikbaar te maken voor anderen. Hoewel deze gegevens worden overgedragen via onze servers, hebben we geen toegang tot deze, zoals elders in dit beleid wordt vermeld.
- Dienstverleners. We wisselen persoonsgegevens met dienstverleners uitsluitend voor zover dit vereist is om de diensten te leveren, waaronder om accounts te maken, ondersteuning te bieden, betalingen te verwerken of communicatie tussen u en Dashlane mogelijk te maken (persoonsgegevens met betrekking tot verzoeken om klantenservice zijn bijvoorbeeld beschikbaar voor onze ondersteuningsagenten op Zendesk). We evalueren de beveiligings- en gegevensprivacypraktijken van alle serviceproviders om ervoor te zorgen dat ze voldoen aan de toepasselijke wetten en dit beleid. Beveiligde gegevens die worden opgeslagen door onze gegevenshostingsprovider (AWS) worden altijd versleuteld zoals hierboven beschreven. De lijst met subverwerkers onthult welke dienstverleners toegang hebben tot persoonsgegevens in verband met onze levering van de diensten.
- Marketing. We bieden gehashte e-mails en/of apparaat-ID's aan dienstverleners om onze reclame-inspanningen te optimaliseren (om ervoor te zorgen dat huidige gebruikers geen

Dashlane-advertenties op andere sites worden getoond). Het is deze providers verboden om deze informatie te gebruiken voor andere doeleinden, waaronder het vergroten van profielen die ze onderhouden. We bieden gehashte e-mails van zakelijke vooruitzichten aan aanbieders van gegevensverrijkingsdiensten om marketinginspanningen te verbeteren.

- Gelieerde ondernemingen. Dit beleid is van toepassing op alle entities die eigendom zijn van of onder gemeenschappelijke controle staan van Dashlane, Inc. ("**Gelieerde ondernemingen**"). We wisselen persoonsgegevens van gelieerde ondernemingen voor zover dit vereist is om de diensten te leveren en te reageren op verzoeken. Sommige gelieerde ondernemingen bevinden zich in de Verenigde Staten, waar privacy en gerelateerde wetten door Europese regelgevers niet als toereikend worden beschouwd om persoonsgegevens te bewaren en te beschermen. Om de vereiste beschermingsniveaus te bieden, hebben we AVG-conforme addenda voor gegevensverwerking ter beschikking gesteld van onze gelieerde ondernemingen in de EU en de VS, naast de andere maatregelen die hieronder worden aangegeven.
- B2B-beheerders van Dashlane. Sommige B2B-gebruikers hebben toegang tot twee "ruimtes" in hun apps: een "zakelijke ruimte" om beveiligde gegevens met betrekking tot hun werk op te slaan, en een "persoonlijke ruimte" voor alles wat ze willen opslaan op de diensten. Met de diensten kunnen B2B-beheerders informatie bekijken over het gebruik van diensten door de B2B-gebruikers die zijn gekoppeld aan hun account, waaronder evenementgegevens, evenals sommige gedragsgegevens op een individuele basis. Een B2B-beheerder kan bijvoorbeeld de gezondheidsscores van wachtwoorden van zakelijke gebruikers zien van zakelijke gebruikers die aan hun account zijn gekoppeld. Ze kunnen ook zien voor welke sites of diensten een individuele zakelijke gebruiker referenties heeft opgeslagen in hun zakelijke ruimte en of deze referenties zijn gecompromitteerd.
- Herstructurering van het bedrijfsleven. Als Dashlane of zijn bedrijf of assets worden overgenomen door of gefuseerd met een ander bedrijf, zal dat bedrijf vervolgens over de persoonsgegevens die we bezitten bezitten en zal dit onze rechten en verplichtingen onder dit beleid vaststellen. Dienovereenkomstig kunnen we persoonsgegevens uitwisselen in verband met een dergelijke transactie. Persoonsgegevens en andere informatie kunnen ook worden overgedragen als een zakelijke verplichting in het geval van insolventie, faillissement of curatele van Dashlane.
- Andere openbaarmakingen. We zullen u op de hoogte brengen van andere openbaarmakingen van uw persoonsgegevens en uw toestemming verkrijgen voorafgaand aan een dergelijke openbaarmaking. Ongeacht uw keuzes met betrekking tot Persoonsgegevens kan Dashlane uw Persoonsgegevens vrijgeven: (a) waar nodig om te voldoen aan toepasselijke wetten of overheidsbevelen; (b) als we te goeder trouw geloven dat dit noodzakelijk is om onze rechten of de Diensten te beschermen. Vanwege onze zero-knowledgearchitectuur zijn we echter niet in staat om beveiligde gegevens te verstrekken, zelfs als we onderhevig zijn aan een geldige bestelling. Voor zover toegestaan door de wet, zullen we de getroffen gebruikers informeren over wettelijk verplichte openbaarmakingen van persoonsgegevens.

6. GEGEVENSBEVEILIGING EN INTERNATIONALE OVERDRACHT VAN INFORMATIE

Samenvatting:
Wij streven ernaar om alle gegevens die wij in ons bezit hebben, inclusief Persoonsgegevens, te beschermen door middel van verschillende maatregelen, en wij werken voortdurend aan de verbetering en actualisering daarvan. Wij kunnen de veiligheid van de Persoonsgegevens die wij verwerken echter niet garanderen en doen dit ook niet. Persoonsgegevens kunnen worden overgedragen naar rechtsgebieden met minder strenge privacywetten dan die in uw eigen land, waaronder de VS, maar we gebruiken technische en andere maatregelen die voldoen aan de toepasselijke Privacywetten om Persoonsgegevens te beschermen wanneer deze in de VS worden verwerkt.

a. We gebruiken robuuste fysieke, organisatorische, technische en administratieve maatregelen om alle gegevens die we bewaren of verwerken te beschermen, en we herzien ons beleid en onze praktijken om de beveiliging te verbeteren. Hoewel we veel moeite doen om uw gegevens te beschermen, is geen enkele methode voor gegevensoverdracht of -opslag volledig veilig; daarom kunnen we de beveiliging van gegevens waarover we controle hebben niet garanderen. Als u denkt dat uw gegevens door ons of het gebruik van de Diensten kunnen zijn gecompromitteerd, neem dan direct contact op met ons ondersteuningscentrum.

b. Uw gegevens, met inbegrip van de Persoonsgegevens die wij over u verzamelen, kunnen worden doorgegeven aan, opgeslagen bij en verwerkt door ons, onze Gelieerde Ondernemingen en dienstverleners buiten uw thuisland, inclusief in de Verenigde Staten, waar de voorschriften inzake gegevensbescherming en privacy niet dezelfde bescherming bieden als in andere delen van de wereld. Wanneer we dit doen, nemen we alle wettelijk verplichte stappen die zijn ontworpen om ervoor te zorgen dat alle persoonsgegevens die wij of onze dienstverleners verwerken (ongeacht waar deze afkomstig zijn) goed worden beschermd. Door gebruik te maken van de Diensten gaat u akkoord met de overdracht, opslag of verwerking van uw gegevens in overeenstemming met dit Beleid.

7. HOE KUNT U UW GEGEVENS BEHEREN?

Samenvatting:
U kunt uw persoonsgegevens bewerken en uw privacy- en gegevensvoorkeuren aanpassen via de secties "Account" of "Instellingen" van de apps. Als u momenteel marketing-e-mails ontvangt, maar dit niet langer wilt, kunt u zich uitschrijven in een dergelijke e-mail. Zelfs als u dit doet, sturen we u nog steeds operationele en transactionele e-mails (bijvoorbeeld kennisgevingen van verlenging). Het verwijderen van apps van uw apparaten verwijdert alle gegevens die zijn geassocieerd met de apps van dat apparaat. Door uw apps te verwijderen, wordt uw account niet verwijderd. Om dat te doen, bekijk de instructies hier. Zelfs als u niet onderworpen bent aan privacywetten, kunt u ook de processen gebruiken die worden beschreven in sectie 8 om uw persoonsgegevens te beheren.

a. *Uw informatie en privacy-instellingen wijzigen*. U kunt toegang krijgen tot persoonsgegevens die zijn gekoppeld aan uw account en deze wijzigen en uw privacy- en gegevensvoorkeuren wijzigen, via de secties "Mijn account" of "Instellingen" van de apps. Ga naar ons ondersteuningscentrum als u hulp nodig hebt.

b. *E-mailcommunicatie*. Met uw toestemming sturen we u periodiek e-mails ter bevordering van het gebruik van de diensten, waaronder tips over het gebruik van de apps of met de nadruk op aanbiedingen van geselecteerde Dashlane-partners. U kunt zich afmelden voor deze e-mails door de afmeldingsinstructies te volgen die in elke e-mail zijn opgenomen, of door uw privacy- en gegevens-instellingen in de diensten te wijzigen. U kunt ook verwijdering aanvragen via ons ondersteuningscentrumr. Het uitschrijven van marketingcommunicatie heeft geen invloed op operationele en transactionele communicatie, waaronder kennisgevingen van inbreuken en andere waarschuwingen in de apps, verlengings-e-mails, enz.

c. *Toepassingen*. U kunt alle verzameling van informatie door een app stoppen door die app te verwijderen. U kunt het standaard verwijderingsproces gebruiken voor het relevante apparaat of platform. Het verwijderen van een app verwijdert uw account niet. Bekijk hier de instructies om te weten hoe dit moet.

8. PRIVACYRECHTEN

Samenvatting:
*Gebruikers die onderworpen zijn aan privacywetten hebben een aantal rechten met betrekking tot hun persoonsgegevens, waaronder het recht om toegang te krijgen tot persoonsgegevens die worden bewaard door providers (zoals wij), en om providers persoonsgegevens te laten "vergeten" die niet langer relevant zijn. De meeste van deze rechten moeten worden geopend via de privacy- en gegevensvoorkeuren in de diensten, maar u kunt altijd contact met ons opnemen voor een antwoord. We zullen **nooit** slechtere diensten verlenen aan of op enigerlei wijze iemand straffen die ervoor kiest om deze rechten uit te oefenen. We ondersteunen de intentie achter deze wetten en zullen ons best*

doen om verzoeken om deze rechten uit te oefenen te honoreren, zelfs als ze niet technisch op u van toepassing zijn.

a. *Gegevensbeheerder*. Voor de doeleinden van de AVG, waar we optreden als een controller, is de controller Dashlane SAS van 21 Rue Pierre Picard, 75018 Parijs, Frankrijk. Vragen over de verwerking van gegevens die onder de AVG vallen, kunnen worden verzonden naar onze functionaris voor gegevensbescherming via dpo@dashlane.com.

b. *Verkoop en uitwisseling van persoonsgegevens*. We wisselen nooit persoonsgegevens uit voor geld of een andere overweging (bijvoorbeeld inruilen voor gratis diensten). Wanneer u echter op een advertentie klikt die u omleidt naar onze Site, sturen we een unieke identificatie naar de verwijzende site zodat ze krediet kunnen ontvangen voor de verwijzing. Dit wordt beschouwd als "uitwisseling" zoals onder de privacywetten van Californië. U kunt dit uitschakelen op de pagina Mijn persoonlijke gegevens niet verkopen of delen.

c. Personen die onderworpen zijn aan privacywetten hebben sommige of alle van de volgende rechten met betrekking tot hun persoonsgegevens die we verwerken. Zoals elders vermeld, zullen we deze verzoeken honoreren wanneer deze door ons zijn gemaakt, afhankelijk van de vereisten van de relevante privacywetten (indien van toepassing). Een B2B-gebruiker die onderworpen is aan de AVG kan bijvoorbeeld vragen dat we hun informatie verwijderen, maar in die situatie is het bedrijf met wiens account de gebruiker is geassocieerd de "beheerder" van die persoonsgegevens en we zijn verplicht om de relevante B2B-beheerder te informeren en hun instructies te volgen.

   - Toestemming intrekken: u kunt uw toestemming voor onze verwerking van uw persoonsgegevens geheel of gedeeltelijk intrekken (d.w.z. voor marketingdoeleinden). Sommige diensten kunnen ineffectief zijn bij afmelding.
   - Gegevens inzien/opvragen: u kunt de Persoonsgegevens die wij over u bewaren te allen tijde inzien via uw Account of door rechtstreeks contact met ons op te nemen.
   - Wijziging: u kunt incorrecte of verouderde Persoonsgegevens die wij over u bewaren te allen tijde wijzigen via uw Account of door rechtstreeks contact met ons op te nemen.
   - Wissen en vergeten. In sommige situaties, bijvoorbeeld wanneer registratiegegevens die we over u bewaren niet langer relevant of juist zijn, kunt u ons verzoeken om deze te wissen. Als u uw account verwijdert, worden alle persoonsgegevens automatisch verwijderd binnen 30 dagen na de datum van verwijdering. **Vanwege de gevoelige aard van beveiligde gegevens zullen we nooit een account van een gebruiker zelf verwijderen: accounts MOETEN worden verwijderd door de gebruiker of de "controller" of gelijkwaardige entiteit.**
   - Overdraagbaarheid: u kunt een kopie van uw Persoonsgegevens aanvragen en deze altijd naar andere door u gekozen entiteiten verzenden. Met de diensten kunt u op elk moment beveiligde gegevens exporteren.

d. Als u een van deze rechten wilt uitoefenen, dien dan het verzoek in via de pagina "Privacy- en gegevensinstellingen". Deze is toegankelijk vanuit de secties "Account" of "Instellingen" van de apps (als u dit niet rechtstreeks vanuit deze secties kunt doen). Als u hulp nodig hebt, ga dan naar ons ondersteuningscentrum of schrijf ons op het onderstaande adres. Geef in uw verzoek goed aan: (i) om **welke** persoonsgegevens het gaat; en (ii) **welke rechten** u wilt afdwingen. Voor uw bescherming kunnen we alleen voldoen aan verzoeken met betrekking tot de persoonsgegevens die zijn gekoppeld aan het e-mailadres waarvan u uw verzoek verzendt. We moeten mogelijk uw identiteit verifiëren voordat we dit doen. We zullen snel aan uw verzoek voldoen, maar in ieder geval binnen de wettelijk verplichte termijnen (bijvoorbeeld dertig (30) dagen voor de AVG en vijfenveertig (45) dagen voor de CPRA). Als u niet onderworpen bent aan privacywetten, proberen we toch om alle verzoeken binnen 45 dagen te verwerken. We bewaren beperkte persoonsgegevens voor registratiedoeleinden of om transacties af te ronden waarmee u bent begonnen voordat u bepaalde verzoeken indiende.

e. **We discrimineren geen enkele gebruiker (bijvoorbeeld door slechtere diensten aan te bieden of hogere vergoedingen in rekening te brengen) die bovengenoemde rechten uitoefent.**

9. CONTACTINFORMATIE; KLACHTEN

Als u vragen, zorgen of klachten hebt over dit beleid of onze praktijken voor het verzamelen of verwerken van gegevens, of als u een inbreuk op de beveiliging wilt melden, neem dan contact op met ons ondersteuningscentrum, stuur een e-mail naar legal@dashlane.com/ordpo@dashlane.com, of schrijf naar het onderstaande adres:

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

Alleen Zwitserse, EU en Britse gebruikers. We hopen elke klacht die onder onze aandacht wordt gebracht, snel op te lossen, maar als u van mening bent dat uw klacht niet adequaat is opgelost, kunt u altijd contact opnemen met uw lokale toezichthouder voor gegevensbescherming, waarvan u hier een lijst vindt.