GRAY DAWES GROUP

GDPR-beleid

Versie uitgegeven

13 februari 2026

Suzanne Horner, CEO

Inhoud

GDPR-nalevingsprocedure

Context en overzicht

BELANGRIJKSTE GEGEVENS

- Beleid opgesteld door: Jeffery Paul (functionaris voor gegevensbescherming)
- Goedgekeurd door: Suzanne Horner (algemeen directeur)
- Beleid van kracht sinds 4 april 2022

Onze verbintenis

Gray Dawes Group zorgt ervoor dat alle relevante wetten met betrekking tot het verzamelen, opslaan, beheren, verwerken en overdragen van persoonsgegevens worden nageleefd.

Deze omvatten, maar zijn niet beperkt tot:

- De Algemene Verordening Gegevensbescherming (EU AVG) (Verordening (EU) 2016/679)
- De Britse Algemene Verordening Gegevensbescherming (UK GDPR)
- De Data Protection Act 2018 (DPA 2018)
- De Nederlandse Algemene Verordening Gegevensbescherming (AVG), onder toezicht van de Autoriteit Persoonsgegevens (AP)
- De Australische Privacywet 1988 en de Australische Privacybeginselen (APPs)
- Toepasselijke privacywetgeving van de Amerikaanse staten (inclusief CCPA/CPRA waar relevant)
- De Personal Information Protection and Electronic Documents Act (PIPEDA) en Canadese provinciale wetten, waaronder Quebec Law 25, Alberta PIPA en British Columbia PIPA

Gray Dawes hanteert de AVG als wereldwijde basisnorm voor privacy.

Wanneer lokale wetgeving aanvullende of strengere eisen stelt, worden aanvullende controles uitgevoerd om naleving te waarborgen.

We houden klanten, leveranciers en medewerkers op de hoogte van beleidswijzigingen en procedurele veranderingen die worden doorgevoerd om voortdurende naleving te garanderen.

Waarom dit beleid bestaat

Dit gegevensbeschermingsbeleid zorgt ervoor dat Gray Dawes Group:

- Voldoet aan de wetgeving inzake gegevensbescherming en de beste praktijken volgt
- De rechten en vrijheden van medewerkers, klanten, reizigers en partners beschermt
- De verantwoordelijkheden van de verwerkingsverantwoordelijke en de verwerker duidelijk definieert
- Toont verantwoordelijkheid aan toezichthouders, waaronder de ICO en de Autoriteit Persoonsgegevens (AP)
- Is transparant over de manier waarop het persoonsgegevens opslaat en verwerkt
- Beschermt zichzelf tegen de risico's van datalekken, boetes van toezichthouders en reputatieschade

Herziening van dit beleid

Dit beleid wordt elk kwartaal herzien en bijgewerkt door de functionaris voor gegevensbescherming (DPO) in overleg met het senior management en de CEO.

Er worden ook jaarlijkse nalevingsbeoordelingen uitgevoerd om ervoor te zorgen dat de regelgevingskaders blijven worden nageleefd, waaronder:

- UK GDPR en DPA 2018
- EU GDPR / AVG
- Australische Privacywet
- Canadese federale en provinciale privacywetten
- Toepasselijke privacywetgeving van Amerikaanse staten
- ISO/IEC 27001:2022-vereisten

Beginselen inzake gegevensbescherming

Volgens de AVG en gelijkwaardige wereldwijde privacykaders moeten persoonsgegevens:

- Op rechtmatige, eerlijke en transparante wijze worden verwerkt
- worden verzameld voor welbepaalde, uitdrukkelijke en gerechtvaardigde doeleinden
- Adequaat, relevant en beperkt zijn tot wat noodzakelijk is
- Nauwkeurig en actueel zijn
- Niet langer worden bewaard dan nodig is
- Op een veilige manier worden verwerkt om de vertrouwelijkheid en integriteit te waarborgen
- Onderworpen zijn aan verantwoordings- en governancecontroles

Toepassingsgebied van dit beleid

Dit beleid is van toepassing op:

- Het hoofdkantoor en alle vestigingen van Gray Dawes Group (inclusief activiteiten in het Verenigd Koninkrijk, Nederland, Australië, de Verenigde Staten en Canada)
- Alle werknemers van Gray Dawes Group
- Aannemers, leveranciers en andere personen die namens Gray Dawes Group werken
- Digitale systemen en externe dienstverleners die Gray Dawes Group ondersteunen Het is van

toepassing op alle persoonsgegevens die het bedrijf in zijn bezit heeft, waaronder:

- Naam
- Paspoortgegevens
- Geboortedatum
- Visumgegevens
- Contactgegevens
- Thuisadres
- Frequent flyer- en andere lidmaatschappen
- Betalingsgegevens
- Reisvoorkeuren (inclusief dieet- of toegankelijkheidseisen, die speciale categorieën gegevens kunnen vormen)

Risico's op het gebied van gegevensbescherming

Naleving van dit beleid beperkt risico's, waaronder:

- Ongeautoriseerde toegang
- Schendingen van de vertrouwelijkheid
- Identiteitsdiefstal
- Overtredingen van grensoverschrijdende overdrachten
- Niet-naleving van regelgeving
- Financiële sancties en reputatieschade

Verantwoordelijkheden

Alle medewerkers zijn verantwoordelijk voor het waarborgen dat persoonsgegevens worden verzameld, opgeslagen, behandeld en verwerkt in overeenstemming met dit beleid.

CEO (SUZANNE HORNER)

Draagt de eindverantwoordelijkheid voor het waarborgen dat de organisatie wettelijk compliant en veerkrachtig blijft op het gebied van gegevensbescherming. Zij zorgt voor strategisch leiderschap, zorgt voor adequate

toewijzing van middelen voor nalevingsinitiatieven en bevordert een cultuur van bewustzijn rond gegevensbescherming in het hele bedrijf.

DPO (JEFFERY PAUL)

Verantwoordelijk voor de implementatie en handhaving van het gegevensbeschermingsbeleid binnen de Gray Dawes Group. Hij verzorgt trainingen en bewustwordingsprogramma's voor medewerkers, fungeert als eerste aanspreekpunt voor toezichthoudende autoriteiten en ziet toe op de naleving van de AVG en andere relevante wetgeving op het gebied van gegevensbescherming. Daarnaast voert hij regelmatig audits en risicobeoordelingen uit om kwetsbaarheden in de gegevensbeveiliging op te sporen en te verminderen.

CHIEF TECHNOLOGY OFFICER (SOPHIE TAYLOR)

Verantwoordelijk voor het onderhouden van een veilige IT-infrastructuur die persoonsgegevens beschermt. Zij zorgt ervoor dat passende cyberbeveiligingsmaatregelen, zoals encryptie, toegangscontroles en incidentresponsplannen, worden getroffen. Bovendien evalueert zij de beveiligingsstatus van externe dienstverleners en verbetert zij voortdurend de digitale beveiliging tegen cyberdreigingen.

MARKETINGDIRECTEUR (JOHN COOPER)

Zorgt ervoor dat alle marketingactiviteiten in overeenstemming zijn met de regelgeving inzake gegevensbescherming. Hij houdt toezicht op het toestemmingsbeheer voor marketingcommunicatie en zorgt ervoor dat klantgegevens op de juiste wijze en in overeenstemming met de AVG worden gebruikt. Hij werkt nauw samen met de DPO om toe te zien op de veilige omgang met persoonsgegevens in marketingdatabases en om transparantie te waarborgen in de interacties met klanten.

CHIEF OPERATING OFFICER (DAVID BISHOP)

Verantwoordelijk voor het beheer van leverancierscontracten en het waarborgen van de naleving van gegevensbeschermings- en beveiligingsvereisten door derden. Hij voert due diligence uit bij externe dienstverleners, houdt toezicht op jaarlijkse leveranciersaudits en zorgt ervoor dat leveranciers voldoen aan de AVG en contractuele verplichtingen. Daarnaast integreert hij gegevensbeschermingsmaatregelen in operationele processen om de naleving en beveiliging van alle bedrijfsactiviteiten te waarborgen.

Algemene richtlijnen voor gegevensverwerking

- Gegevens mogen alleen worden geraadpleegd door bevoegd personeel voor legitieme zakelijke doeleinden.
- Persoonsgegevens mogen niet informeel of buiten goedgekeurde systemen om worden gedeeld.
- Medewerkers moeten de richtlijnen voor versleuteling en veilige gegevensoverdracht volgen.
- Werkstations moeten worden vergrendeld wanneer ze onbeheerd zijn om ongeoorloofde toegang te voorkomen.

Gegevensgebruik - Reizigersprofielen

- Reizigersprofielen worden bijgehouden om boekings- en reisbeheerdiensten te vergemakkelijken.
- De verzamelde gegevens omvatten persoonlijke informatie, reisvoorkeuren, betalingsgegevens en lidmaatschappen van loyaliteitsprogramma's.
- Profielgegevens worden alleen verwerkt met toestemming van de reiziger of op grond van contractuele verplichtingen.
- Reizigers hebben het recht om hun profielgegevens in te zien, te wijzigen of te laten verwijderen.
- Gegevens e beveiligingsmaatregelen , , waaronder encryptie en beperkte toegang, zorgen voor vertrouwelijkheid.

Gegevensgebruik – Marketing

- Persoonsgegevens worden alleen voor marketingdoeleinden gebruikt wanneer daarvoor uitdrukkelijke toestemming is verkregen.
- Marketingcommunicatie voldoet aan de AVG.
- Gebruikers kunnen zich op elk moment afmelden voor marketingcommunicatie.
- Marketing -databases worden regelmatig beoordeeld om te gegevens nauwkeurigheid en naleving te waarborgen.

Beleid inzake gegevensbeheer en registratie

- Gray Dawes Group houdt nauwkeurige gegevens bij van **gegevensverwerkingsactiviteiten** overeenkomstig **artikel 30 van de AVG**.
- Verwerkingsactiviteiten worden gedocumenteerd om naleving te waarborgen en regelgevende audits te ondersteunen.
- Beveiligingsmaatregelen, toegangsbeperkingen en auditlogboeken zorgen voor gecontroleerde toegang tot gegevens.
- Medewerkers die met gevoelige gegevens omgaan, worden getraind om te voldoen aan het beleid voor gegevensbeheer.

Gegevensopslag en -beveiliging

- Gray Dawes Group werkt in een papierloze omgeving en zorgt voor digitale beveiligingsmaatregelen voor gegevens. Alle afgedrukte gegevens moeten veilig worden opgeslagen en onmiddellijk na gebruik worden vernietigd.
- Gegevens worden tijdens opslag en verzending versleuteld om ongeoorloofde toegang te voorkomen.
- Servers en cloudgebaseerde oplossingen worden continu gecontroleerd op naleving van de beveiligingsvoorschriften.
- Er moeten regelmatig back-ups van gegevens worden gemaakt en getest.
- Gegevensoverdrachten buiten het Verenigd Koninkrijk/de EU moeten voldoen aan door de AVG goedgekeurde waarborgen (bijv. standaardcontractbepalingen, UK IDTA).

Beleid inzake gegevensgebruik

- Persoonsgegevens mogen alleen worden gebruikt voor het beoogde doel en mogen alleen worden verwerkt met toestemming.

- Ongeautoriseerde toegang tot of wijziging van persoonsgegevens is ten strengste verboden.
- Medewerkers moeten zich houden aan duidelijke richtlijnen voor het omgaan met en overdragen van gevoelige gegevens.

Nauwkeurigheid en onderhoud van gegevens

- Medewerkers moeten klant- en werknemersgegevens controleren om de nauwkeurigheid ervan te waarborgen.
- Verouderde of onjuiste gegevens moeten onmiddellijk worden bijgewerkt.
- Persoonsgegevens die niet langer nodig zijn, moeten veilig worden verwijderd in overeenstemming met het beleid inzake gegevensbewaring.

Beleid inzake het verwijderen van gegevens

- Persoonsgegevens worden alleen bewaard zolang dat nodig is voor operationele of wettelijke doeleinden.
- Onnodige gegevens worden veilig verwijderd met behulp van goedgekeurde verwijderingsmethoden.
- Betrokkenen kunnen verzoeken om verwijdering van gegevens, wat zal worden verwerkt in overeenstemming met de AVG-voorschriften.
- Regelmatige audits zorgen ervoor dat het beleid inzake gegevensbewaring en -verwijdering wordt nageleefd.

Beleid inzake het vrijgeven van gegevens

- Persoonsgegevens worden alleen vrijgegeven met uitdrukkelijke toestemming en voor legitieme doeleinden.
- Verzoeken om gegevens van klanten, reizigers of regelgevende instanties worden veilig verwerkt.
- Gegevens worden met behulp van versleutelde methoden overgedragen om ongeoorloofde toegang te voorkomen.
- Alle vrijgegeven gegevens worden bijgehouden voor nalevings- en auditdoeleinden.

Reactie op incidenten en datalekken

- Elk vermoeden of daadwerkelijk datalek moet onmiddellijk worden gemeld aan de DPO.
- Incidenten worden beoordeeld op basis van hun impact, waarbij ook wordt gekeken of er sprake is van grensoverschrijdende gegevensverwerking.
- Als een inbreuk een hoog risico voor personen inhoudt, worden de betrokken partijen binnen 48 uur op de hoogte gebracht.
- De ICO wordt binnen 72 uur op de hoogte gebracht van elke significante inbreuk.
- Er zal een volledig onderzoek en een evaluatie na het incident worden uitgevoerd om de veiligheidsmaatregelen te versterken en herhaling te voorkomen.

Verzoeken om inzage

- Betrokkenen hebben het recht om toegang te vragen tot hun persoonsgegevens.
- Verzoeken om toegang moeten worden ingediend bij de functionaris voor gegevensbescherming.
- Verzoeken worden binnen een maand verwerkt, tenzij ze als buitensporig worden beschouwd, in welk geval een redelijke vergoeding in rekening kan worden gebracht.

Openbaarmaking van gegevens voor juridische doeleinden

- Persoonsgegevens kunnen worden verstrekt aan wetshandhavings- of regelgevende instanties wanneer dit wettelijk vereist is en door de DPO is beoordeeld op naleving.
- Internationale gegevensoverdrachten voldoen aan de standaardcontractbepalingen (SCC's) of bindende bedrijfsregels (BCR's) om naleving van de AVG te waarborgen.
- Voor overdrachten buiten de EER zijn risicobeoordelingen en waarborgen vereist.
- Contracten met derden bevatten juridisch bindende bepalingen inzake gegevensbescherming en beveiliging.
- Betrokken personen worden geïnformeerd, tenzij dit wettelijk verboden is.
- Alle openbaarmakingen worden geregistreerd voor nalevingscontrole. aan wetshandhavings- of regelgevende instanties wanneer dit wettelijk vereist is en door de DPO is beoordeeld op naleving.

Gegevensverwerkingsactiviteiten

- Gray Dawes Group treedt voornamelijk op als **gegevensverwerker** en beheert de profielen van reizigers van klanten en aanverwante informatie.
- De gegevensverwerking omvat het verzamelen, opslaan, ophalen, verzenden en verwijderen van gegevens, waarbij in alle stadia een veilige verwerking wordt gegarandeerd.
- Er wordt gebruikgemaakt van encryptie, toegangscontrole en audittrails om de integriteit en vertrouwelijkheid van de gegevens te waarborgen.
- Gegevens worden alleen verwerkt volgens contractuele afspraken, zonder ongeoorloofd hergebruik.
- Het bedrijf houdt zich niet bezig met geautomatiseerde besluitvorming of profilering die juridische of significante gevolgen heeft voor individuen.
- Als er in de toekomst geautomatiseerde verwerking wordt ingevoerd, zal deze worden getoetst op naleving van de AVG en zullen personen worden geïnformeerd over hun rechten met betrekking tot een dergelijke verwerking.

Controle- en nalevingsmaatregelen

- Er worden elk kwartaal interne audits uitgevoerd om naleving van het gegevensbeveiligings- en privacybeleid te waarborgen, waaronder de EU-AVG, de Britse AVG en de DPA 2018.
- Jaarlijkse externe audits valideren de naleving van industrienormen en wereldwijde wetgeving inzake gegevensbescherming, waaronder de CCPA (California Consumer Privacy Act) en de PDPA (Personal Data Protection Act in Singapore en andere rechtsgebieden waar van toepassing).
- Externe leveranciers worden jaarlijks gecontroleerd om te bevestigen dat zij voldoen aan contractuele en wettelijke verplichtingen, zodat alle gegevens die met leveranciers worden gedeeld, voldoen aan de hoogste veiligheids- en privacynormen.
- De training van medewerkers wordt regelmatig bijgewerkt, zodat deze niet alleen betrekking heeft op de AVG, maar ook op internationale wetgeving inzake gegevensbescherming, waardoor een wereldwijde norm voor naleving wordt gewaarborgd.
- Nalevingsrapporten en risicobeoordelingen worden gedocumenteerd en beoordeeld door het senior management om te voldoen aan de steeds veranderende wereldwijde regelgeving.
- Waar nodig worden gegevensbeschermingseffectbeoordelingen (DPIA's) uitgevoerd om de risico's van nieuwe verwerkingsactiviteiten of systeemimplementaties te beoordelen, in overeenstemming met de AVG en andere regelgevingskaders.

Beheer van werknemersgegevens

- Persoonsgegevens van werknemers worden verzameld en verwerkt in overeenstemming met de toepasselijke arbeids- en gegevensbeschermingswetgeving in de verschillende regio's waar Gray Dawes Group actief is.
- De gegevens worden verwerkt voor legitieme HR- en operationele doeleinden, zoals salarisadministratie, beheer van secundaire arbeidsvoorwaarden en prestatiebeheer.
- Personeelsdossiers worden veilig opgeslagen en alleen bewaard gedurende de wettelijk vereiste periode in elk rechtsgebied.
- De toegang tot werknemersgegevens is strikt beperkt tot HR-personeel en bevoegde personen op basis van een need-to-know-basis.
- Internationale overdrachten van werknemersgegevens voldoen aan de AVG en relevante lokale regelgeving door middel van mechanismen zoals standaardcontractbepalingen (SCC's) en bindende bedrijfsregels (BCR's).
- Werknemers hebben het recht om hun persoonsgegevens in te zien, bij te werken of te laten verwijderen, met inachtneming van de toepasselijke wettelijke en contractuele verplichtingen.
- Er zijn specifieke beleidsregels van kracht voor de verwerking van gevoelige werknemersgegevens, waaronder medische dossiers en antecedentenonderzoeken, in overeenstemming met de wereldwijde privacywetgeving.

Nalevingsverklaring

- Alle werknemers, aannemers en externe dienstverleners moeten zich aan dit beleid houden.
- Er worden regelmatig trainingen gegeven om het bewustzijn rond gegevensbescherming te vergroten.
- Niet-naleving van het gegevensbeschermingsbeleid kan leiden tot disciplinaire maatregelen of beëindiging van de overeenkomst.
- Het management bevordert een cultuur van verantwoordelijkheid en transparantie bij alle gegevensverwerkingsactiviteiten.


GRAY DAWES
GROUP