Intern Privacybeleid - De Dagpas B.V.

Datum: 09-04-2019 00:00:00

Versie: 1

Inleiding

Dit interne privacybeleid fungeert als een leidraad hoe binnen onze organisatie wordt omgegaan met privacy gerelateerde gegevens, zogeheten persoonsgegevens. Niet enkel dient dit privacybeleid als bewustwording voor het gebruiken van persoonsgegevens, maar ook als handvat naar de buitenwereld hoe binnen De Dagpas B.V. (hierna: 'de Organisatie') wordt omgegaan met privacy. Dit document is de basis, het uitgangspunt voor alle privacy gerelateerd onderwerpen.

In dit privacybeleid wordt uitgelegd wat persoonsgegevens zijn, welke regels er gelden bij het gebruik van deze gegevens en maatregelen wij nemen bij het gebruik van deze gegevens. Het is belangrijk dit privacybeleid strikt na te leven. Privacy en betrouwbaarheid staan bij de Organisatie hoog in het vaandel. Door als organisatie dit privacybeleid na te leven wordt de privacy van alle personen (hierna: 'betrokkenen') van wie de gegevens door De Dagpas B.V. worden verwerkt gewaarborgd.

De privacy van de betrokkenen kan worden geschonden als wij ons niet aan dit privacybeleid houden, dan bestaat er een kans dat gegevens van de betrokkenen bijvoorbeeld verloren raken. Als organisatie willen wij dit voorkomen. Houd je daarom altijd aan de regels van dit privacybeleid wanneer je met persoonsgegevens werkt.

Het privacybeleid heeft een dynamisch karakter en kan van tijd tot tijd worden aangevuld of herzien. Dit kan naar aanleiding van veranderingen in de organisatie, bedrijfsprocessen, aanpassing van informatie systemen of wetswijzigingen. Indien het privacybeleid aangepast wordt, zullen wij je hierop attenderen.

Het privacybeleid wordt door het managementteam (hierna: 'MT') van de Organisatie ondersteund en uitgedragen in de organisatie. Naast dit intern privacybeleid zijn uiteraard alle andere gedragscodes en –regels aanvullend van toepassing.

Hoofdstuk 1. Intern gebruik van gegevens

1.1. Wat zijn persoonsgegevens?

Om duidelijk aan te geven hoe binnen onze organisatie wordt omgegaan met persoonsgegevens, is het van belang eerst duidelijk te definiëren wat persoonsgegevens precies zijn.

Persoonsgegevens zijn de gegevens over een persoon die ervoor zorgen dat een persoon identificeerbaar is, of geïdentificeerd kan worden. Een persoonsgegeven kan direct of indirect naar een persoon herleiden.

Aan de hand van een naam of adres is zonder veel omwegen vast te stellen om welke persoon het gaat. Maar ook als er meerdere gegevens gecombineerd moeten worden om vast te stellen om wie het gaat, kan er sprake zijn van een persoonsgegeven. Zo kan een postcode of IP-adres naar een persoon herleid worden. Soms zijn daar echter wel aanvullende gegevens voor nodig, zoals bijvoorbeeld een huisnummer.

Persoonsgegevens van betrokkenen zijn bijvoorbeeld:

- NAW-gegevens
- telefoonnummer
- e-mailadres
- geslacht
- geboortedatum of leeftijd
- klant- of personeelsnummer
- IP-adres

Welke persoonsgegevens van betrokkenen in onze systemen precies gebruikt worden, wordt nader toegelicht in dit document.

1.2. Verwerken van gegevens

Als er persoonsgegevens worden gebruikt, wordt dit het verwerken van gegevens genoemd, of een gegevensverwerking. Aan gegevensverwerking zijn wettelijke rechten en plichten verbonden. Onder verwerken vallen alle handelingen die met persoonsgegevens worden verricht zoals:

- Het opslaan van gegevens
- Het verwijderen van gegevens
- Het kopiëren van gegevens
- Het wijzigen van gegevens

Aangezien de gegevens van de betrokkenen persoonsgegevens zijn, is het van belang bij het verwerken van deze gegevens voortdurend rekening te houden met de wettelijke rechten en plichten.

Het mag voor een betrokkene geen verrassing zijn welke gegevens van hem gebruikt worden. Een betrokkene moet van te voren kunnen weten wat hij van ons kan verwachten. Op deze manier is het mogelijk een betrouwbare organisatie te blijven.

Het is daarnaast wettelijk verplicht om het verwerken van de gegevens te melden bij de Autoriteit Persoonsgegevens.
Om als organisatie een goed overzicht te houden over de gegevens waarmee binnen de Organisatie wordt gewerkt, zijn er een vijftal vragen opgesteld die over het gebruik van gegevens beantwoord moeten kunnen worden. Deze vragen geven ook inzicht ten aanzien van hoe te handelen bij het uitwisselen van gegevens.

Aan de hand van deze vragen kan er inzicht worden gekregen hoe met de gegevens omgegaan moet worden en aan welke regels gehouden moet worden zodat de Organisatie als organisatie voldoet aan de wet- en regelgeving. Het is daarom belangrijk dat je de volgende vijf vragen, bij elke nieuwe aansluiting en informatiebron, kan beantwoorden:

1. Wat is de oorsprong van de gegevens waarmee gewerkt wordt?
Geef aan waar de gegevens vandaan komen. Zijn deze bijvoorbeeld bij klanten of leverancier via een webformulier of via tracking cookies op de website?

2. Wat is de classificatie van deze gegevens (persoonsgegevens, etc.)?
Geef aan om wat voor gegevens het gaat. Gaat het bijvoorbeeld om NAW-gegevens, bankgegevens, zoekgedrag, kooporders, medische gegevens, of bepaalde voorkeuren?

3. Waar worden deze gegevens bewerkt/verwerkt, en in welke systemen en/of omgeving/locatie?

Bijvoorbeeld: Bestanden staan in datacenter van leverancier van De Dagpas B.V. en worden geladen in marketing analyse data-warehouse programma van De Dagpas B.V..

4. Wie heeft toegang tot deze gegevens?
Benoem alle personen of functies van de betrokken partijen die toegang tot deze gegevens hebben. In het geval van gegevens in de personeeladministratie, zou dit bijvoorbeeld medewerkers van HR kunnen zijn.

5. Hoe wordt met deze gegevens omgegaan als in beveiliging, opslag, archivering, mutatie en vernietiging?
Geef aan welke beveiligingseisen men hanteert (bijvoorbeeld ISO norm 27001), hoe wordt omgegaan met archiveren en wanneer de gegevens worden vernietigd. Veelal is er een beveiligingsbeleid op te vragen.

Indien het verwerken van de gegevens een onderdeel van een project is, kun je ondersteuning binnen het project krijgen. Veelal kan de leverancier van de gegevens het merendeel van de vragen beantwoorden.

Bij het uitwisselen van gegevens is altijd een bewerkersovereenkomst van toepassing. In bepaalde gevallen ook een geheimhoudingsverklaring. De antwoorden op de bovenstaande vragen zijn de basis voor deze overeenkomsten.

Indien je geen helder antwoord kunt geven op één van bovenstaande vijf vragen, of als dit antwoord onduidelijk dan wel onvolledig is, dan mag de aansluiting of de informatiebron niet binnen de Organisatie worden gebruikt. Als je twijfelt of een aansluiting of informatiebron gebruikt mag worden, neem dan contact op met je leidinggevende. Het kan nodig zijn dat voor het gebruik van de gegevens andere maatregelen genomen moeten worden, bijvoorbeeld het sluiten van een bewerkersovereenkomst met een partner en/of leverancier. Anderzijds is het mogelijk om een geaccepteerd risico te benoemen welke schriftelijk door het MT vastgelegd wordt. Dit geaccepteerde risico wordt door het MT vastgesteld op advies van de proceseigenaar.

De toetsing van deze vragen moet ook periodiek op reeds bestaande aansluitingen en informatiebronnen uitgevoerd worden. Deze toetsing is een onderdeel van de jaarlijkse cyclus vanuit het security- en privacyplan. Door deze toetsing kunnen we inzicht en controle houden op de gegevens die worden verwerkt binnen De Dagpas B.V..

In dit interne privacybeleid zullen de verschillende onderwerpen van de vragen verder toegelicht worden.

1.3. Soorten persoonsgegevens
Er worden verschillende persoonsgegevens binnen de Organisatie verwerkt. De volgende gegevens van de betrokkenen worden in onze systemen verwerkt:

- NAW-gegevens
- telefoonnummers
- e-mailadressen
- geslacht
- paspoort- en ID-kaartnummers
- transactiegegevens

De gegevens die verzameld worden van de betrokkenen, mogen enkel voor deze doeleinden gebruikt worden. Het is uitdrukkelijk niet toegestaan de gegevens van de betrokkenen voor andere doeleinden te gebruiken.
Bijzondere persoonsgegevens
Persoonsgegevens kunnen daarnaast nog aangemerkt worden als 'bijzonder', waarvoor een extra strikt regime geldt. Daarom moet grote terughoudendheid worden getracht als het gaat om de verzameling en verwerking van deze gegevens. Bijzondere persoonsgegevens zijn gegevens die direct of indirect iets zeggen over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, alsmede persoonsgegevens betreffende het lidmaatschap van een vakvereniging.

1.4. Doeleinden verwerken gegevens
Alle (persoons)gegevens worden door De Dagpas B.V. voor specifieke doeleinden verwerkt. Gegevens mogen in principe alleen voor die doeleinden worden verwerkt, waarvoor ze zijn verzameld. Het is dan ook uitdrukkelijk niet toegestaan gegevens te gebruiken voor andere doeleinden.

Gegevens personeel
Vanzelfsprekend worden gegevens van onze medewerkers verwerkt om de personeelsadministratie op een juiste manier uit te voeren. Gegevens van medewerkers mogen enkel door de HR-afdeling gebruikt worden voor de taken die zij toegewezen hebben gekregen, of andere afdelingen en personen indien zij ook concrete taken toegewezen hebben gekregen waarbij het verwerken van gegevens van medewerkers noodzakelijk is. Gegevens van medewerkers worden verwerkt voor onder andere:

- Het verwerken van de loonadministratie;
- Het regelen van ziekte en verlof;
- Het regelen van in- en uitdiensttreding.

1.5. Verzenden van gegevens

Het is eenvoudig bestanden te verzenden via je werkmail. Het is echter mogelijk dat deze bestanden persoonsgegevens bevatten van klanten en/of medewerkers. Wanneer je bestanden via je werkmail verzendt is het van belang met het volgende rekening te houden:

- *Intern*: Voor het intern verzenden van bestanden via je werkmail naar andere medewerkers, is dit geen probleem indien de bestanden worden verzonden via ons interne netwerk naar de werkmail van een andere medewerker.
- *Extern*: Voor het verzenden van bestanden naar externe personen/organisaties is het van belang dat, indien de inhoud van deze bestanden gevoelig is, deze bestanden versleuteld verzonden worden. Denk hierbij aan bestanden waar gegevens van klanten en/of medewerkers in staan. Dit kunnen bijvoorbeeld facturen, mailinglijsten, CV's en loonstroken zijn. Verstuur enkel gegevens wanneer hiervoor de juiste afspraken zijn gemaakt met de ontvanger, zoals een bewerkersovereenkomst.

Binnen De Dagpas B.V. maken we gebruik van de volgende applicaties om bestanden te delen of te versturen:

Gebruik deze applicaties om bestanden te delen en/of te versturen. Indien dit niet mogelijk is, neem dan contact op met Merijn Bouwmeestser (Facilitair manager en personeelszaken). Neem ook contact op met Merijn Bouwmeestser indien je twijfelt of je bestanden mag versturen en/of moet versleutelen, of hier vragen over hebt.

Let op! Verstuur enkel bestanden via je werkmail en het interne netwerk van De Dagpas B.V., of via een andere door De Dagpas B.V. aangeboden beveiligde verzendwijze. Verstuur geen bestanden met je privé-mail, en gebruik geen privé-accounts van applicaties zoals Dropbox of Skype. Download en upload enkel bestanden met je werkapparatuur, en niet met je privé-laptop, -telefoon of -tablet.

1.6. Bewaren van gegevens

Het bewaren van gegevens kan opgedeeld worden in twee handelingen:

1. Het fysiek opslaan van gegevens
2. Het bewaren van gegevens

Wat betreft de fysieke opslag van gegevens hanteren wij de volgende minimale eisen:

- De gegevens moeten tijdens de opslag voldoende beschermd zijn. Dit is mede afhankelijk van de aard van de gegevens. De bescherming dient te voldoen aan de verplichte wet- en regelgeving. Denk hierbij aan encryptie op je computer, het beveiligd opslaan van documenten op je computer en niet op eigen apparatuur, het opslaan van documenten op de netwerkschijf (my documents) waarvan ook een back-up gemaakt wordt of het afsluiten van kasten waarin papieren documenten worden bewaard.
- Er moet adequate bescherming ingericht zijn, passend bij de aard van de gegevens en volgens gangbare industriële standaard of door wet- en regelgeving opgelegd.

De door De Dagpas B.V. erkende omgevingen voldoen aan deze eisen.

Het beleid ten aanzien van het opslaan van gegevens is van toepassing voor alle systemen waar betrokkenegegevens mee worden verwerkt. Dit kan dus ook het systeem bij een gecontracteerde partij zijn waarop betrokkenegegevens staan. Dit beleid wordt overeengekomen in een contract of een bewerkersovereenkomst.

Alle gegevens die door de belastingdienst wettelijk verplicht zijn om te bewaren, worden voor een termijn van 7 jaar bewaard. Hieronder vallen de volgende gegevens:

- het grootboek
- de debiteuren- en crediteurenadministratie
- de voorraadadministratie
- de in- en verkoopadministratie
- de loonadministratie.

Voor alle andere gegevens geldt dat deze niet langer mogen worden bewaard dan nodig is voor de doeleinden waarvoor ze zijn verzameld. Het vaststellen van de duur van het termijn en het toezicht op de bewaartermijn wordt uitgevoerd door de eigenaar van het bedrijfsproces dat deze gegevens verwerkt.

Voor veel gegevens die je gebruikt, is het ook van belang dat je zelf oordeelt of het bewaren van de gegevens noodzakelijk is of niet. Verwijder direct e-mails die niet langer noodzakelijk zijn. Belangrijke e-mails kunnen bewaard blijven en opgeslagen worden in specifieke mappen, alle andere e-mails moeten worden verwijderd.

Hetzelfde geldt uiteraard voor alle ander digitale documenten en tevens voor papieren documentatie. Zorg ervoor dat alle papieren documenten die nog noodzakelijk zijn, op de juiste wijze zijn opgeborgen. Alle papieren documenten die niet meer noodzakelijk zijn, dienen direct versnipperd te worden. Zorg dat papieren documentatie minimaal eenmaal per jaar wordt nagelopen om te controleren of alle documenten écht noodzakelijk zijn om te bewaren.

1.7. Verwijderen van gegevens

Indien wij in opdracht van een betrokkene gegevens verwijderen, of indien een verzoek bij ons hiervoor wordt ingediend, wordt dit door middel van certificaten en ander vergelijkbaar bewijs gecontroleerd en vastgesteld. Zo kunnen wij er op toezien dat het verwijderen van gegevens volgens de industriële standaarden die gelden in onze branche wordt uitgevoerd.

Het verwijderen van een grote hoeveelheid gegevens – dit geldt dus niet voor enkele persoonsgegevens – wordt uitgevoerd volgens de industriële standaard. Ook dit wordt door middel van certificaten en ander vergelijkbaar bewijs gecontroleerd. Dit wordt door de IT-afdeling begeleid.

Jij bent zelf verantwoordelijk voor het verwijderen van gegevens waarvoor jij zelf moet bepalen of deze nog noodzakelijk zijn of niet (zoals ook hierboven beschreven), zoals jouw e-mails of papieren documenten. Zorg ervoor dat papieren documenten met persoonsgegevens, die niet meer noodzakelijk zijn, versnipperd worden, of in een veilige, daarvoor bestemde container worden gedeponeerd. Wat betreft digitale documenten, dien je er zorg voor te dragen dat deze verwijderd worden uit de mailbox, of van de door jou gebruikte apparatuur.

Hoofdstuk 2. Beveiligen van gegevens

2.1. Beveiligingsmaatregelen en handleidingen

Indien er persoonsgegevens worden verwerkt, verplicht de wet dat deze gegevens worden beschermd tegen verlies of onrechtmatige verwerking. Om de gegevens van de betrokkenen op een juiste manier te beveiligen, worden er binnen de organisatie verschillende maatregelen toegepast.

Dit kunnen technische maatregelen zijn, zoals het gebruik van Secure Socket Layer op onze websites en een beveiligde interne verbinding. De IT-afdeling ziet er op toe dat deze beveiligingsmaatregelen goed worden uitgevoerd en up-to-date zijn.
Daarnaast is het van belang dat alle medewerkers zelf de juiste maatregelen nemen om ongeoorloofde toegang, of het verlies van data te voorkomen. Er kunnen namelijk veel technische maatregelen gehanteerd worden om gegevens te beveiligen, maar zolang medewerkers niet bewust omgaan met de beveiliging van gegevens kan het alsnog misgaan. Let daarom op de volgende punten tijdens je dagelijkse werkzaamheden:

1. Laat je scherm nooit onbeveiligd achter als je je werkplek verlaat. Ook al verlaat je je werkplek maar voor heel even, zorg ervoor dat je altijd je scherm vergrendeld hebt. Doe je dit niet, dan kan iemand met een kwade wil zichzelf zonder enige moeite toegang verschaffen tot onze systemen.
2. Gebruik sterke wachtwoorden en zorg er ook voor dat al jouw apparatuur met een wachtwoord is beveiligd. Een aantal tips voor het gebruik van wachtwoorden:
    - Gebruik geen wachtwoorden zoals 1234, je eigen naam, geboortedatum of woonplaats. Ook geen combinatie hiervan zoals Marie1985 maar wissel af met tekens, hoofdletters en cijfers.
    - Gebruik geen woorden uit het woordenboek. Hackers kunnen namelijk gebruik maken van zogenaamde ‘dictionary attacks’ waarbij alle woorden uit het woordenboek worden uitgeprobeerd als wachtwoord. Weet dit daarom te voorkomen door niet één eenvoudig woord als wachtwoord te gebruiken.
    - Deel inloggegevens niet met een ander, ook niet met een kennis. Schrijf je inloggegevens ook niet op bijvoorbeeld briefje en deel ze niet in een e-mails. Wil je toch ergens je wachtwoord noteren, zorg er dan voor dat dit nooit genoteerd wordt in de buurt van je computer.
    - Gebruik niet overal hetzelfde wachtwoord voor.

3. Zorg ervoor dat je computer of laptop niet pal voor een raam staat. Zo voorkom je dat mensen ongevraagd mee kunnen kijken, maar zo voorkom je ook mogelijke diefstal.
4. Indien je gebruik maakt van werkapparatuur, zoals een laptop of mobiele telefoon, gebruik je werkapparatuur dan voor zover mogelijk uitsluitend voor werkdoeleinden. Zorg er bovendien voor dat de IT-afdeling, of andere daarvoor verantwoordelijke, jouw apparatuur gecontroleerd heeft op beveiliging. Maak daarnaast geen verbinding met een openbaar Wi-Fi netwerk zoals bijvoorbeeld in de trein, of in openbare ruimtes. Zo voorkom je dat er via een onbeveiligd netwerk toegang verkregen wordt tot jouw apparatuur.
5. Accepteer alleen bijlagen van e-mails, indien je zeker weet dat dit van een betrouwbare afzender afkomt en het een betrouwbaar bestand is. Hetzelfde geldt voor het openen van links naar websites die zijn opgenomen in e-mails en gelijksoortige berichten afkomstig van derden.

2.2. Beperkte toegang tot gegevens

Een andere wijze om de gegevens van betrokkenen te beschermen is door het hanteren van beperkte toegang tot de gegevens. Je hebt slechts toegang tot de systemen en gegevens die nodig zijn voor het uitvoeren van je functie. Naast de autorisatie is er ook een expliciete functiescheiding ingericht. Toegang tot gegevens kan enkel met een versleutelde verbinding worden verkregen. Dit gaat op basis van een gecontroleerde autorisatie waardoor het mogelijk is te herleiden wie er precies toegang heeft verkregen. Op deze manier wordt misbruik en/of fraude met gegevens beperkt.

De aanvraag of mutatie van een autorisatie verloopt altijd via de IT-afdeling. Wil je een aanvraag of wijziging indienen? Dan kun je daarmee contact opnemen.

Hoofdstuk 3. Datalek

3.1. Datalek

Ondanks de beveiligingsmaatregelen die binnen de Organisatie worden gehanteerd, kan een kans op ongeautoriseerde toegang tot gegevens of verlies en/of diefstal van gegevens (een datalek) nooit volledig worden uitgesloten. Om de reputatie en betrouwbaarheid van De Dagpas B.V. hoog te houden, vragen wij alle medewerkers alert te zijn op mogelijke verdachte zaken en/of overtredingen. Met onze beveiligingsmaatregelen en de medewerking van het personeel wordt de kans op een datalek verkleind.

Het proces van meldingen van datalekken en vermoedens daarvan, worden beschreven in ons calamiteitenplan voor datalekken. Raadpleeg de meest recente versie hiervan, om te weten wat je moet doen bij ontdekking van een beveiligingsincident en mogelijk datalek.

Hoofdstuk 4. De betrokkenen

4.1. Rechten van betrokkenen

Voor bezoekers van onze website is in de privacy- en cookieverklaring op de website beschreven wat ze kunnen verwachten bij het gebruik van onze website en diensten, wat wij met hun gegevens doen en wat hun rechten zijn.
Betrokkenen hebben volgens de wet verschillende rechten. Zo heeft een betrokkene bijvoorbeeld het recht bij ons zijn of haar gegevens op te vragen, deze in te zien en/of deze te laten wijzen en/of verwijderen. Daarnaast wordt, voor de mailings, in elke e-mail altijd een afmeldmogelijkheid opgenomen.

Dergelijke aanvragen komen in de eerste instantie bij Merijn Bouwmeester terecht. Indien je de vraag van een betrokkene krijgt om inzage in gegevens te verlenen, of deze te wijzigen of te verwijderen, dan kun je deze aanvraag doorzetten naar Merijn Bouwmeester. Wanneer een dergelijk verzoek binnenkomt, verifieer dan altijd of de verzoeker wel is wie hij zegt te zijn. Vraag bijvoorbeeld naar aanvullende identificerende gegevens.

Hoofdstuk 5. Contact

5.1. Aanspreekpunt privacy zaken

De Dagpas B.V. streeft ernaar toegankelijk en beschikbaar te zijn voor al jouw vragen of meldingen omtrent privacy en security. Indien er sprake is van een overtreding, verlies of diefstal van gegevens of een verdenking van dergelijke zaken, vragen wij jou hier direct een melding van te maken.

Indien een privacy- of beveiligingsprobleem actief is binnen onze organisatie, zullen wij dit aan alle medewerkers doorgeven. Hierbij kunnen tips, advies en mogelijk te nemen maatregelen medegedeeld worden. Op deze manier proberen wij de medewerkers up-to-date te houden en actief te betrekken.