Privacybeleid

Eurides en NS Mobiliteitsdiensten

Maart 2021

1. Inleiding

Eurides en NS Mobiliteitsdiensten zijn organisaties die privacy hoog in het vaandel hebben. De Algemene Verordening Gegevensbescherming (hierna: AVG) vereist goed na te denken over hoe je als organisatie persoonsgegevens verwerkt en beschermt. Door te voldoen aan de verantwoordingsplicht wordt een belangrijke bijdrage geleverd aan de bescherming van het grondrecht op privacy. Eurides en NS Mobiliteitsdiensten verwerken persoonsgegevens van verschillende betrokkenen, zoals van hun eigen medewerkers, maar ook van klanten en gebruikers van de mobiliteitsplatformen Vaigo en NS Go. In dit beleid worden de regels uitgewerkt voor de omgang met persoonsgegevens door Eurides en NS Mobiliteitsdiensten.

2. Visie

Eurides en NS Mobiliteitsdiensten zijn zich ervan bewust dat de bescherming van persoonsgegevens belangrijk is en hechten er veel waarde aan dat deze op een rechtmatige, behoorlijke en transparante manier worden verwerkt binnen de organisatie. Eurides en NS Mobiliteitsdiensten vinden het dan ook belangrijk dat de medewerkers bewust zijn van het belang van privacy en op de hoogte zijn van de regels hieromtrent. Dit verkleint de kans op onjuist gebruik van gegevens en datalekken. Om hiervoor te zorgen worden er regelmatig awareness trainingen gegeven. Daarnaast worden de regels omtrent privacy behandeld wanneer er een nieuwe werknemer in dienst komt.

3. Wetgeving en definities

De AVG geeft regels voor de versterking en uitbreiding van het recht op bescherming van persoonsgegevens. Aanvullende regels en nationale keuzes van Nederland zijn te vinden in de Uitvoeringswet AVG. De AVG en UAVG vormen het algemeen juridisch kader voor de omgang met persoonsgegevens.

Hieronder is een korte omschrijving gegeven van enkele belangrijke gehanteerde begrippen uit de AVG:

Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon. Het gaat hier dus om ieder gegeven dat te herleiden is tot een bepaald persoon.

Betrokkene: de persoon op wie de persoonsgegevens betrekking hebben. De betrokkene is degene van wie de gegevens worden verwerkt. Dit is niet alleen een burger, maar heeft bijvoorbeeld ook betrekking op de huurders, bezoekers en medewerkers van Eurides en NS Mobiliteitsdiensten.

Data Protection Impact Assessment (DPIA): met een Data Protection Impact Assessment worden de effecten en risico's van nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy. Dit heet ook wel een gegevensbeschermingseffectbeoordeling.

Verwerking: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

Verwerkingsverantwoordelijke: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.
Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die ten behoeve van de verwerkingsverantwoordelijke (in opdracht van) persoonsgegevens verwerkt.

4. Reikwijdte

Dit privacybeleid is van toepassing op alle verwerkingen van persoonsgegevens door alle medewerkers van Eurides en NS Mobiliteitsdiensten. Dit beleid vormt een uitwerking van de wettelijke regelgeving en een handleiding voor de medewerkers van Eurides en NS Mobiliteitsdiensten. Het geeft de regels en uitgangspunten voor de eerlijke, zorgvuldige en rechtmatige verwerking van persoonsgegevens.

5. Verwerkingen

Een verwerking van persoonsgegevens is elke handeling of elk geheel van handelingen met persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde processen. Onder verwerken worden in de AVG in ieder geval de volgende handelingen begrepen:

- Verzamelen, vastleggen en ordenen
- Bewaren, bijwerken en wijzigen
- Opvragen, raadplegen, gebruiken
- Verstrekken door middel van doorzending
- Verspreiding of enige andere vorm van ter beschikkingstellen
- Samenbrengen, met elkaar in verband brengen
- Afschermen, uitwissen of vernietigen van gegevens

Uit deze opsomming blijkt dat eigenlijk alles wat je doet met een persoonsgegeven een verwerking is.

Als Eurides en NS Mobiliteitsdiensten verzamelen wij verschillende soorten persoonsgegevens voor de uitvoering van onze werkzaamheden. Hierbij valt te denken aan verwerkingen in het kader van sollicitaties, het gebruik van het mobiliteitsplatform en het uitbetalen van salarissen. Hierbij worden verschillende categorieën van persoonsgegevens verzameld waaronder NAW-, contact-, reis- en financiële gegevens.

Eurides en NS Mobiliteitsdiensten hebben in hun verwerkingsregister een overzicht gemaakt van de verschillende verwerkingsactiviteiten die zij uitvoeren. Dit register houden Eurides en NS Mobiliteitsdiensten altijd up-to-date. Het verwerkingsregister bevat van iedere verwerking nadere informatie over onder nadere de verwerkingsdoeleinden, categorieën van persoonsgegevens, categorieën van betrokkenen en ontvangers en de bewaartermijn van de gegevens.

6. Doeleinden

Persoonsgegevens mogen alleen verzameld worden als daarvoor een doel bestaat. Dit doel moet welbepaald, duidelijk omschreven en gerechtvaardigd zijn. Ook moet steeds nagegaan worden of het verwerken van persoonsgegevens noodzakelijk is voor het doel. Deze verwerkingsdoeleinden

zijn het “waarom” van het verwerken van persoonsgegevens. Doelen zijn van belang voor verschillende normen. Denk hierbij aan onder andere het bepalen wie verantwoordelijk is voor de verwerking van persoonsgegevens. Of de vraag of het delen van deze gegevens met andere organisaties is toegestaan. Ook zijn de doelen van belang voor het vaststellen van bewaartermijnen en het informeren van de burger. Zo weet je hoe lang het nodig is om de persoonsgegevens te bewaren of waar je betrokkenen over moet informeren.

Een belangrijke eis is dat de doelen vooraf specifiek geformuleerd moeten zijn. De doelen mogen dus niet te ruim en vaag omschreven zijn of achteraf bepaald worden. Verwerking voor een ander doel dan het oorspronkelijke doel is alleen onder strikte voorwaarden toegestaan. zo zal er een directe relatie moeten zijn met het doel waarvoor de persoonsgegevens eerder zijn verzameld. Ook moet je rekening houden met de soort gegevens. Algemeen geldt: hoe gevoeliger het gegeven, hoe minder snel er sprake is van verenigbaar gebruik. De gegevens mogen dan dus minder snel worden gebruikt voor een ander doel dan waarvoor deze eerder zijn verzameld. Ook moet men rekening houden met de gevolgen van de beoogde verwerking voor de betrokkene. Denk hierbij aan het vooraf inlichten van de betrokkene over het doel waarvoor de gegevens worden gebruikt als de betrokkene zijn persoonsgegevens aan Eurides en NS Mobiliteitsdiensten verstrekt.

7. Rechtmatige grondslag

Voor elke verwerking van persoonsgegevens moet een rechtmatige grondslag uit de wet van toepassing zijn. Dit betekent dat Eurides en NS Mobiliteitsdiensten altijd moeten kunnen verantwoorden op basis waarvan de persoonsgegevens van de betrokkenen worden verwerkt. Een uitzondering hierop is het hiervoor besproken geval waarin persoonsgegevens worden verwerkt voor een ander doel dan het doel waarvoor ze zijn verzameld. Dit is enkel onder strikte voorwaarden toegestaan.

Voor elke verwerking moet een van de volgende zes grondslagen van toepassing zijn:

- de betrokkene heeft voor de verwerking zijn ondubbelzinnige toestemming verleend;
- de gegevensverwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, waarbij ook rekening moet worden gehouden met de onderhandelingsfase;
- de gegevensverwerking is noodzakelijk om een wettelijke verplichting na te komen waaraan Eurides en NS Mobiliteitsdiensten onderworpen zijn;
- de gegevensverwerking is noodzakelijk ter vrijwaring van een vitaal belang van de betrokkene (in het kader van leven of dood, bijvoorbeeld delen van gegevens bij opname spoedeisende hulp);
- de gegevensverwerking is noodzakelijk voor de goede vervulling van een taak van algemeen belang door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt, of
- de gegevensverwerking is noodzakelijk voor de behartiging van het gerechtvaardigde belang van Eurides/NS Mobiliteitsdiensten of van een derde aan wie de gegevens worden verstrekt. Maar als het belang op bescherming van zijn privacy voor de betrokkene zwaarder weegt, dan is het verwerken van gegevens op grond van een gerechtvaardigd belang niet van toepassing.

Voor alle grondslagen zal er altijd een noodzaak moeten zijn om die gegevens te verwerken. Of het verwerken van bepaalde gegevens noodzakelijk is, moet altijd gemotiveerd worden.
Van de zes grondslagen zijn voor Eurides en NS Mobiliteitsdiensten toestemming, uitvoering van een overeenkomst, wettelijke verplichting en gerechtvaardigd belang van toepassing.

8. Wijze van verwerking

Een verwerking van persoonsgegevens is alleen toegestaan in overeenstemming met de wet en op een zorgvuldige wijze. Persoonsgegevens worden zoveel mogelijk verzameld bij de betrokkene zelf. De wet gaat uit van subsidiariteit. Dit betekent dat een verwerking alleen is toegestaan wanneer het doel niet op een andere manier kan worden bereikt. In de wet wordt ook gesproken over proportionaliteit. Dit betekent dat persoonsgegevens alleen mogen worden verwerkt als dit in verhouding staat tot het doel. Wanneer met geen, of minder (belastende), persoonsgegevens hetzelfde doel kan worden bereikt moet daar altijd voor gekozen worden.

Persoonsgegevens moeten dus juist, ter zake dienend, up-to-date en niet bovenmatig veel zijn in het licht van het doel van de verwerking. Dit betekent dat alleen die persoonsgegevens mogen worden gebruikt die strikt noodzakelijk zijn voor het doel van de verwerking. Wanneer het bijvoorbeeld voldoende is om iemands contactgegevens te gebruiken, is het niet nodig om ook een pasfoto en BSN te vragen. Sowieso gelden voor het gebruik van het BSN strenge regels. Wanneer ook met anonieme gegevens volstaan kan worden, mogen geen herleidbare persoonsgegevens gebruikt worden. Bij bijvoorbeeld de aanmelding voor een bezoek vragen we alleen nog maar de (voor- en achter-)naam van de bezoeker.

Organisatorische maatregelen

De organisatorische maatregelen die NSM/Eurides heeft getroffen zijn: geheimhoudingsverklaringen, verwerkers ook een geheimhoudingsplicht, medewerkers ingelicht over de AVG d.m.v. een training, privacybeleid voor de omgang met persoonsgegevens door medewerkers waar zij zich aan dienen te houden.

Beveiliging

De manier waarop NSM/Eurides persoonsgegevens beveiligt zijn d.m.v.: wachtwoorden, logging, VPN toegang, IT-policy.

9. Doorgifte aan derden

Persoonsgegevens mogen in principe niet worden doorgegeven naar een organisatie in een land buiten de EU. Dit komt omdat binnen de EU een goede bescherming voor de persoonsgegevens is, en daarbuiten niet in alle gevallen. Onder doorgifte wordt o.a. verstaan: het opslaan (bijvoorbeeld in de Cloud) of het ter beschikking stellen aan een organisatie buiten de EU. Hieronder valt niet het via internet zichtbaar maken van persoonsgegevens aan personen buiten de EU. Eurides en NS Mobiliteitsdiensten maken gebruik van enkele verwerkers die persoonsgegevens doorgeven aan een land buiten de Europese Economische Ruimte (EER). Dit zijn Pipedrive, Help Scout en Office 365. Met deze partijen

hebben wij een verwerkersovereenkomst gesloten waarin is vastgelegd dat deze partijen AVG-compliant zijn.

10. Transparantie en communicatie

Informatieplicht

Betrokkenen moeten geïnformeerd worden over de verwerking van hun persoonsgegevens door Eurides en NS Mobiliteitsdiensten. Het moment van informeren en de manier waarop is afhankelijk van de vraag hoe de persoonsgegevens worden verzameld. Namelijk, zijn de gegevens rechtstreeks van de betrokkene verkregen of op een andere manier.

Als de persoonsgegevens door de betrokkene zelf worden aangeleverd, dan moet deze over de verwerking van zijn gegevens vooraf worden geïnformeerd. Als persoonsgegevens over de betrokkene niet direct bij deze persoon maar ergens anders, zoals een andere organisatie, dan hoeft de betrokkene pas op een later moment geïnformeerd te worden. De betrokkene moet dan pas geïnformeerd worden als die persoonsgegevens door Eurides en NS Mobiliteitsdiensten worden vastgelegd. Of op het moment dat de gegevens voor het eerst aan een andere organisatie worden gegeven en dit uiteraard nodig is.

Inzage

Betrokkenen hebben recht op inzage in de eigen persoonsgegevens. De betrokkene hoeft geen reden op te geven voor zijn inzageverzoek, maar hij mag niet overdreven veel verzoeken in korte tijd indienen. Als een betrokkene vraagt om inzage, dan heeft hij of zij recht op een volledig overzicht van de gegevens die worden gebruikt. Ook moet inzage worden gegeven in de herkomst van de gegevens, de ontvangers van de gegevens en de doelen van de verwerking van de persoonsgegevens. Eurides en NS Mobiliteitsdiensten zorgen ervoor dat aan dit verzoek tijdig en volledig wordt voldaan.

Correctie en verwijdering

Naast een recht op inzage heeft de betrokkene ook recht op correctie, aanvullen, verwijderen of afschermen van de eigen persoonsgegevens. Aan dit verzoek moet alleen gehoor worden gegeven als de gegevens onjuist zijn of onvolledig zijn voor het doel waarvoor de gegevens worden verzameld. Dit verzoek moet ook worden gerespecteerd als de gegevens niet relevant zijn of in strijd met de wet worden gebruikt.

De betrokkene moet in zijn verzoek duidelijk aangeven welke gegevens om welke reden moeten worden aangepast. Het recht kan niet worden gebruikt om meningen of onderzoeksresultaten te wijzigen. Als positief wordt besloten op het verzoek, dan moeten de wijzigingen zo snel mogelijk worden doorgevoerd.

De wijzigingen of verwijderingen van persoonsgegevens moeten ook worden doorgegeven aan andere organisaties aan wie Eurides en NS Mobiliteitsdiensten de gegevens hebben verstrekt.

Bezwaar

De betrokkene heeft de mogelijkheid om zich te verzetten tegen het gebruik van zijn persoonsgegevens. Als een betrokkene zich verzet tegen gebruik van de gegevens, dan mogen Eurides en NS Mobiliteitsdiensten de gegevens niet meer gebruiken. Ook al is de gegevensverwerking op zich gerechtvaardigd en toegestaan. Er zijn een aantal situaties waar het recht van verzet kan worden ingezet. Allereerst in het geval er sprake is van bijzondere persoonlijke omstandigheden en de verwerking is gebaseerd op de publiekrechtelijke taak. Of in de situatie dat het een medewerker is en deze vanwege bijzondere persoonlijke omstandigheden bezwaar maakt tegen de verwerking van zijn gegevens gebaseerd op een gerechtvaardigd belang.

De betrokkene kan zich altijd verzetten tegen het gebruik van persoonsgegevens voor direct marketing-doeleinden of liefdadigheidsdoelen.

Indienen van verzoek

Om gebruik te maken van zijn of haar rechten kan de betrokkene een verzoek indienen. Dit verzoek kan zowel schriftelijk als via de e-mail ingediend worden. Eurides en NS Mobiliteitsdiensten hebben een maand de tijd, vanaf de ontvangst van het verzoek, om te beoordelen of het verzoek gerechtvaardigd is. Binnen een maand zullen Eurides en NS Mobiliteitsdiensten laten weten wat er met het verzoek gaat gebeuren. Als het verzoek niet wordt opgevolgd is er de mogelijkheid om bezwaar te maken bij Eurides/NS Mobiliteitsdiensten of een klacht in te dienen bij de Autoriteit Persoonsgegevens (AP). Aan de hand van een verzoek kunnen Eurides en NS Mobiliteitsdiensten aanvullende informatie opvragen om zeker te zijn van de identiteit van de betrokkene. De wijze waarop de behandeling en afhandeling van een verzoek plaatsvindt is vastgelegd in de procedure *Rechten van betrokkenen*.

11. Plichten van Eurides en NS Mobiliteitsdiensten

Register van verwerkingen

Eurides en NS Mobiliteitsdiensten zijn verplicht om te documenteren welke persoonsgegevens zij verwerkt, wat het doel is, van wie of waar deze gegevens afkomstig zijn en met wie deze gegevens worden gedeeld. Daarnaast moeten we per verwerking documenteren en verantwoorden op basis van welke wettelijke grondslag Eurides en NS Mobiliteitsdiensten deze persoonsgegevens verwerken.

Bewaartermijnen

Eurides en NS Mobiliteitsdiensten bewaren gegevens niet langer dan nodig is voor het doel van de verwerking. In een aantal wetten zijn specifieke bewaartermijnen opgenomen voor bepaalde persoonsgegevens. Als geen bewaartermijn aanwezig is dan moet goed kunnen worden onderbouwd waarom persoonsgegevens voor een bepaalde termijn worden bewaard. Wanneer er nog persoonsgegevens opgeslagen zijn die niet langer nodig zijn voor het bereiken van het doel worden deze zo snel mogelijk verwijderd. Na afloop van de bewaartermijnen moeten de persoonsgegevens worden vernietigd of geanonimiseerd. Dit geldt niet alleen voor de gegevens zelf, maar ook voor kopieën en back-ups. Voor alle

persoonsgegevens geldt dat de vernietiging onomkeerbaar moet zijn. Het gaat dus niet om het plaatsen van de bestanden in de prullenbak en de prullenbak legen, maar bijvoorbeeld om het overschrijven van data met nullen, enen en willekeurige karakters (data wiping).

De wijze waarop de bewaar- en vernietigingstermijnen worden toegepast is vastgelegd in het *Bewaartermijnenbeleid*.

Meldplicht datalekken

De meldplicht datalekken houdt in dat Eurides en NS Mobiliteitsdiensten zo snel mogelijk (binnen 72 uur) een melding doen bij de AP zodra een ernstig datalek zich heeft voorgedaan. Een datalek is een inbreuk op de beveiliging, die flinke nadelige gevolgen heeft voor de betrokkene of voor de bescherming van de persoonsgegevens. Denk hierbij aan een kwijtgeraakte USB-stick met persoonsgegevens, een gestolen laptop of een inbraak op het netwerk (hack). Als de kans bestaat dat het datalek nadelige gevolgen zou kunnen hebben voor betrokkenen, dan moeten Eurides en NS Mobiliteitsdiensten het daarnaast óók melden bij de betrokkenen zelf. Daarnaast moet de betrokkene worden geïnformeerd over welke maatregelen Eurides en NS Mobiliteitsdiensten nemen om de risico's en schade te beperken.

Naast het melden moeten wij ook alle datalekken documenteren. Met deze documentatie moet de Autoriteit Persoonsgegevens kunnen controleren of wij als Eurides en NS Mobiliteitsdiensten aan de meldplicht hebben voldaan.

De wijze waarop gehandeld wordt op het moment dat er een datalek heeft plaatsgevonden is te vinden in procedure *Datalekken.*

Verwerkersovereenkomst

Verwerkersovereenkomsten moeten iedere keer worden afgesloten wanneer derden – ook wel verwerkers genoemd – in opdracht van Eurides en NS Mobiliteitsdiensten persoonsgegevens verwerken. Uiteraard moeten er duidelijke afspraken worden gemaakt over hoe deze verwerkers moeten omgaan met de gegevens die zij van Eurides en NS Mobiliteitsdiensten krijgen. Denk hierbij aan welke gegevens men nodig heeft om haar taak uit te oefenen. Of aan de manier waarop de organisatie de gegevens heeft beveiligd en wat zij moet doen als er een datalek is. Eurides en NS Mobiliteitsdiensten hebben een standaard verwerkersovereenkomst beschikbaar gesteld die in al deze gevallen moet worden gebruikt.

Data Protection Impact Assessment (DPIA)

Met een DPIA worden de effecten en risico's van nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy. Dit geldt in het bijzonder bij verwerkingen waarbij nieuwe technologieën worden gebruikt. Eurides en NS Mobiliteitsdiensten voeren deze alleen uit wanneer:

- er een (geautomatiseerde) verwerking plaatsvindt met een hoog risico,
- er een (geautomatiseerde) verwerking plaatsvindt waarvan de Autoriteit Persoonsgegevens heeft aangegeven dat daarvoor een DPIA verplicht is;
- een grootschalige verwerking plaatsvindt,

- of wanneer er een grootschalige monitoring van openbare ruimten plaatsvindt.

Privacy by Design en Privacy by Default

Bij de aanschaf of ontwikkeling van producten, systemen of processen moet altijd rekening worden gehouden met de bescherming van persoonsgegevens. We noemen dit Privacy by Design (PbD) en Privacy by Default. Voor alle producten, systemen of processen moeten de technische en organisatorische maatregelen ervoor zorgen dat standaard alleen die gegevens worden gebruikt die nodig zijn voor het doel. Als blijkt dat bij een systeem gevoelige of bijzondere persoonsgegevens worden verwerkt en dit mogelijk een hoog privacyrisico met zich meebrengt, zijn we verplicht om een Data Protection Impact Assessment (DPIA) uit te voeren.

Verantwoordelijkheid

Het management draagt de verantwoordelijkheid over de wijze waarop binnen Eurides en NS Mobiliteitsdiensten omgegaan wordt met persoonsgegevens. Voor inhoudelijke vragen hierover of over het beleid en de AVG kunt u daarom contact opnemen met het management. Te bereiken via privacy@eurides.eu.

Ook kunt u voor vragen contact opnemen met onze Functionaris Gegevensbescherming, Annemarie Nijhoff. Zij is te bereiken via FG@ns.nl.