AUTORITEIT
PERSOONSGEGEVENS

Autoriteit Persoonsgegevens
Postbus 93374, 2509 AJ Den Haag
Hoge Nieuwstraat 8, 2514 EL Den Haag
T 070 8888 500 - F 070 8888 501
autoriteitpersoonsgegevens.nl

Vertrouwelijk/Aangetekend
De Staatssecretaris Koninkrijksrelaties en Digitalisering
drs. F.Z. Szabó
Postbus 20011
2500 EA Den Haag

Datum
9 juli 2024

Ons kenmerk
z2023-303796

Contactpersoon

Onderwerp
Datadeler-apps

Geachte heer Szabó,

Op 23 april 2024 heeft het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) advies gevraagd aan de Autoriteit Persoonsgegevens in het kader van een reguleringsvraagstuk over zogenoemde datadeler-apps of datadeelplatforms (hierna: datadeler-apps). Datadeler-apps zijn applicaties waarmee mensen gegevens over zichzelf uit overheidsregistraties kunnen (laten) verzamelen, bijvoorbeeld om een hypothecaire lening of een huurwoning te kunnen krijgen. Het ministerie van BZK maakt zich zorgen over het gebruik van deze datadeler-apps en overweegt om afspraken te maken met aanbieders van datadeler-apps en deze afspraken vast te leggen in een convenant. Het ministerie heeft een concept voor een convenant aan de AP voorgelegd en heeft de AP verzocht om hierop te reageren en het ministerie van advies te voorzien, hetgeen de AP in deze brief zal doen.

Scraping door datadeler-apps
Er zijn verschillende aanbieders van datadeler-apps actief. Organisaties die gegevens van burgers nodig hebben, bijvoorbeeld voor de beoordeling van een aanvraag van een hypothecaire lening, vragen in toenemende mate aan hun klanten om gebruik te maken van een datadeler-app. In grote lijnen werkt dit soort applicaties als volgt. De betrokkene moet de applicatie downloaden en vervolgens zelf, vanuit de applicatie, via DigiD inloggen op de verschillende overheidswebsites, bijvoorbeeld van DUO, het UWV of de Belastingdienst. Na het inloggen via DigiD heeft de applicatie toegang tot alle gegevens die over de betrokkene op de betreffende overheidswebsite staan. Deze gegevens worden eerst allemaal geautomatiseerd verzameld (gescrapet) door de datadeler-app. Daarna selecteert de applicatie de benodigde (beperktere) set gegevens, en stuurt deze, na toestemming van de betrokkene, door aan de dienstverlener, bijvoorbeeld een bank.

Zorgen over de rechtmatigheid

Het ministerie van BZK maakt zich zorgen over de gevolgen van het gebruik van datadeler-apps voor de bescherming van persoonsgegevens van de burgers die deze apps gebruiken. Zo hebben de datadeler-apps na het inloggen via DigiD door de betrokkene toegang tot alle gegevens die over de betrokkene op de betreffende overheidswebsite staan, terwijl voor het doel waarvoor de gegevens worden opgevraagd, doorgaans alleen maar een deel van deze gegevens nodig is. Dit betekent dat er door een datadeler-app persoonsgegevens worden ingezien en verwerkt, die niet nodig zijn voor de dienstverlening waarvoor de burger de app gebruikt. Dit is problematisch, omdat het indruist tegen een belangrijk beginsel uit de Algemene Verordening Gegevensbescherming (AVG): het beginsel van minimale gegevensverwerking (artikel 5 lid 1 onder c AVG). Dit beginsel houdt onder andere in dat de persoonsgegevens die verwerkt worden, beperkt moeten blijven tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt. Het scrapen van alle gegevens van een betrokkene van een bepaalde overheidswebsite, terwijl slechts een beperkte set van die gegevens nodig is, is niet in lijn met het beginsel van minimale gegevensverwerking. Een andere zorg van het ministerie betreft het inloggen via DigiD. Bij het inloggen op overheidswebsites kunnen de datadeler-apps niet gebruikt worden in combinatie met de DigiD-app, maar alleen met de minder veilige inlogmethode van gebruikersnaam en wachtwoord, al dan niet in combinatie met een sms. Als een betrokkene met zijn gebruikersnaam en wachtwoord inlogt via DigiD, zijn diens gebruikersnaam en wachtwoord bovendien zichtbaar voor de datadeler-app.
Ook maakt BZK zich zorgen over de geringe transparantie richting de burgers die van deze apps gebruik maken. Zij worden volgens het ministerie in de huidige praktijk onvoldoende geïnformeerd over de techniek (scraping) en werking van deze apps, en over de risico's voor de bescherming van persoonsgegevens die het gebruik van deze apps met zich meebrengt.

De AP heeft net als het ministerie zorgen over het gebruik van datadeler-apps. De grondslag voor het gebruik van een datadeler-app, is de toestemming van de betrokkene (artikel 6 lid 1 onder a AVG). Deze grondslag kan alleen rechtsgeldig zijn, als de betrokkenen de vrije keuze hebben om al dan niet gebruik te maken van deze apps. Alleen dan kan sprake zijn van 'toestemming' als rechtsgeldige grondslag. Betrokkenen moeten er altijd voor kunnen kiezen om zelf de gegevens aan te leveren en geen gebruik te maken van een datadeler-app, zonder dat zij van deze keuze nadelige gevolgen ondervinden. Dit betekent ook dat zij moeten worden geïnformeerd over het feit dat zij deze vrije keuze hebben. De AP heeft signalen dat burgers in de praktijk niet altijd deze vrije keuze hebben, of daarover niet afdoende worden geïnformeerd. Ook heeft de AP signalen uit de praktijk dat datadeler-apps niet altijd transparant zijn over de techniek die zij gebruiken en over welke persoonsgegevens zij precies verwerken. De manier van inloggen is ook problematisch. Ten eerste wordt het beveiligingsniveau van DigiD verlaagd doordat de datadeler-apps niet de DigiD-app kunnen gebruiken bij het inloggen op overheidswebsites. Ten tweede zijn de DigiD-gebruikersnaam en -wachtwoord van de gebruiker zichtbaar voor de datadeler-app, wat een risico op identiteitsfraude tot gevolg kan hebben. Hoewel de AP zelf geen onderzoek heeft uitgevoerd om de precieze werking van datadeler-apps vast te stellen, deelt de AP daarom de zorgen van het ministerie.

Advies gevraagd over een concept convenant

Het ministerie van BZK heeft overwogen om het gebruik van datadeler-apps te verbieden, maar heeft daar (vooralsnog) van afgezien, onder andere omdat een verbod lastig te effectueren zou zijn. Dit heeft te maken

met de omstandigheid dat het voor websitehouders op het moment van inloggen niet zichtbaar is of een burger alleen zelf inlogt of daarbij een datadeler-app gebruikt. Scraping door datadeler-apps kan daardoor op dit moment niet met technische middelen worden voorkomen. Ook signaleert het ministerie dat in de markt een grote behoefte bestaat aan dit soort applicaties, zowel bij dienstverleners als bij de burgers die van deze apps gebruik maken. Het met behulp van een datadeler-app gegevens verzamelen gaat sneller dan het handmatig aanleveren van deze gegevens door burgers, en ook zouden vaker direct de juiste gegevens worden aangeleverd aan de dienstverleners.

Om een deel van de problemen die het ministerie van BZK signaleert tegen te gaan, overweegt het ministerie om met de aanbieders van datadeler-apps afspraken te maken en deze vast te leggen in een convenant. Als nadeel ziet het ministerie, dat met het sluiten van een dergelijk convenant de verwerkingen door datadeler-apps indirect door het ministerie zullen worden gelegitimeerd, terwijl niet alle problemen die het ministerie ziet door het maken van afspraken kunnen worden opgelost.

Het ministerie heeft een concept voor een convenant voorgelegd en toegelicht aan de AP en heeft de AP gevraagd om het ministerie te adviseren. De AP voldoet graag aan dit verzoek en adviseert als volgt.

Advies AP

eIDAS ID-wallet als toekomstige oplossing
In het kader van de per 20 mei 2024 in werking getreden herziene versie van de Europese eIDAS-verordening,[1] wordt door BZK gewerkt aan een zogenoemde ID-wallet. Met een dergelijke ID-wallet, in de vorm van een app, kunnen burgers zich online identificeren en zelf selectief (persoons)gegevens uitwisselen met bijvoorbeeld een overheidsinstantie of een bank, dat wil zeggen, alleen de gegevens die daadwerkelijk nodig zijn in de betreffende situatie. Deze wallets zullen een veilig en voor de burger kosteloos alternatief zijn voor de datadeler-apps die op dit moment in de markt actief zijn. Totdat dit veilige alternatief geregeld is, overweegt het ministerie van BZK om met de aanbieders van de huidige datadelers-apps afspraken te maken.

Geen convenant sluiten over onrechtmatige verwerkingen
Het eerste advies van de AP ziet op deze mogelijke keuze van het ministerie om door middel van een convenant afspraken te maken met aanbieders van datadeler-apps. De AP heeft kennisgenomen van het concept-convenant en begrijpt dat het ministerie hiermee verbeteringen beoogt te bewerkstellingen. Maar ook als deze verbeteringen kunnen worden bereikt, neemt dat nog niet het probleem weg dat datadeler-apps alle gegevens over iemand van de overheidswebsite kunnen scrapen waar de betrokkene heeft ingelogd. Ook de omstandigheid dat betrokkenen die gebruik maken van een datadeler-app niet met behulp van de DigiD-app kunnen inloggen, verandert niet door het convenant. Zolang en voor zover in dit convenant sprake is van verwerkingen die in strijd zijn met de AVG, acht de AP het ongewenst dat het ministerie van BZK die verwerkingen zou reguleren en daarmee zou legitimeren. Weliswaar kan het

[1] Verordening (EU) 2024/1183 van het Europees Parlement en de Raad van 11 april 2024 tot wijziging van Verordening (EU) nr. 910/2014, wat betreft de vaststelling van het Europees kader voor digitale identiteit (*PbEU* L 30.4.2024).

gebruik van datadeler-apps voor dienstverleners en burgers praktische voordelen hebben, en geeft het ministerie aan dat een verbod lastig te effectueren zou zijn, maar de AP acht het niet juist om om die redenen verwerkingen te faciliteren die, naar het zich laat aanzien, in strijd zijn met de AVG en grote risico's met zich mee brengen voor de bescherming van persoonsgegevens van burgers. De AP adviseert het ministerie van BZK dan ook om onrechtmatige verwerkingen door datadeler-apps niet te legitimeren door het sluiten van een convenant.

Met spoed inzetten op API's of andere technische maatregelen
Zolang het ministerie van oordeel is dat sprake is van verwerkingen in strijd met de AVG, ligt het wat de AP betreft voor de hand dat het ministerie van BZK – vanuit haar maatschappelijke verantwoordelijkheid - passende maatregelen neemt om onrechtmatige verwerkingen door datadeler-apps tegen te gaan. In dat licht adviseert de AP het ministerie van BZK om met spoed in te zetten op technische maatregelen waarmee wordt voorkomen dat datadeler-apps toegang hebben tot méér persoonsgegevens van betrokkenen, dan die noodzakelijk zijn. Een technische oplossing waarbij bovenmatige toegang tot persoonsgegevens van burgers op overheidswebsites wordt tegengegaan, verdient wat de AP betreft sterk de voorkeur boven het maken van afspraken met de aanbieders van datadeler-apps. Dit ook, omdat het voor websitehouders op het moment van inloggen niet zichtbaar is of een burger zelf inlogt of daarbij een datadeler-app gebruikt. Dit bemoeilijkt de controle op datadeler-apps. Het beschikbaar stellen van API's (Application Programming Interfaces), in combinatie met het inrichten van accounts voor de datadeler-apps waarbij het gebruik van de API's gecontroleerd kan worden, kan een passende maatregel zijn om het bovenmatig verwerken van persoonsgegevens van burgers tegen te gaan. Als de betreffende overheidswebsites API's beschikbaar zouden hebben, kan worden afgebakend welke gegevens verzameld kunnen worden door de datadeler-apps en kan het bovenmatig (en daarmee onrechtmatig) verwerken van persoonsgegevens worden tegengegaan. Het scrapen van iemands persoonsgegevens op een overheidswebsite is dan niet langer mogelijk, terwijl wel de benodigde gegevens kunnen worden verkregen. De AP adviseert het ministerie om het beschikbaar stellen van API's en accounts voor datadeler-apps nader te onderzoeken, en deze bij geschiktheid technisch en waar nodig ook wettelijk zo snel als mogelijk is in te regelen. Indien deze maatregelen de risico's onvoldoende mitigeren, adviseert de AP het ministerie van BZK om het gebruik van de commerciële datadeler-apps in afwachting van de (eIDAS) ID-wallet te verbieden.

Als u vragen heeft naar aanleiding van deze brief, dan horen wij dat graag.

Hoogachtend,
Autoriteit Persoonsgegevens,