AUTORITEIT
PERSOONSGEGEVENS

Autoriteit Persoonsgegevens
Postbus 93374, 2509 AJ Den Haag
Bezuidenhoutseweg 30, 2594 AV Den Haag
T 070 8888 500 - F 070 8888 501
autoriteitpersoonsgegevens.nl

Aangetekend

Datum

Ons kenmerk

Contactpersoon

070 8888 500

Onderwerp
Bescherming van persoonsgegevens bij betaaldienstverlening

Geachte directie,

Uw organisatie heeft bij De Nederlandse Bank (DNB) een vergunning gekregen voor een rekeninginformatiedienst [en, indien van toepassing, een betaalinitiatiedienst] in het kader van PSD2. Een belangrijk onderdeel van uw bedrijfsmodel is op de verwerking van persoonsgegevens gebaseerd, waaronder financiële persoonsgegevens. Financiële persoonsgegevens zijn gevoelig. Dit betekent dat de verwerking daarvan verhoogde risico's voor de desbetreffende persoon oplevert. Het is daarom belangrijk dat heel zorgvuldig met deze persoonsgegevens wordt omgegaan. Als directie bent u hiervoor eindverantwoordelijk.[1] In deze brief geven wij u meer informatie over de belangrijkste verplichtingen.

Toezicht door de Autoriteit Persoonsgegevens

De Autoriteit Persoonsgegevens (AP) is de Nederlandse toezichthouder op de naleving van gegevensbeschermingsregels; wij bevorderen en bewaken de bescherming van persoonsgegevens. De AP kan een onderzoek instellen naar de verwerking van persoonsgegevens door of voor uw onderneming. Zo'n onderzoek kunnen we starten naar aanleiding van klachten of tips van consumenten, maar ook op eigen initiatief. Bij onderzoeken kunnen wij samenwerken met andere nationale en internationale toezichthouders.

[1] Vanaf het moment dat u persoonsgegevens verzamelt, bent u (doorgaans) verwerkingsverantwoordelijke. Zie artikel 4 (7) AVG. Een verwerkingsverantwoordelijke is 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. Dit houdt kortweg in dat u verantwoordelijk bent voor een rechtmatige, behoorlijke en transparante verwerking van de persoonsgegevens.

De AP heeft verschillende instrumenten om ervoor te zorgen dat de persoonsgegevens goed beschermd worden. Stelt de AP vast dat een organisatie de wet overtreedt? Dan kan de AP daartegen optreden, bijvoorbeeld met handhavende maatregelen. Daarbij kunt u denken aan het opleggen van een boete, een last onder dwangsom of het opleggen van een verwerkingsverbod.

Belangrijkste verplichtingen

Met deze brief wil de AP u graag informeren over de belangrijkste[2] verplichtingen die de AVG met betrekking tot uw dienstverlening stelt:

1. u moet de beginselen voor de verwerking van persoonsgegevens naleven en bij het ontwerp van processen waarbij persoonsgegevens worden verwerkt moet rekening worden gehouden met de principes van 'privacy by design' en 'privacy by default';
2. u moet waarschijnlijk voor voorgenomen verwerkingen van financiële persoonsgegevens een Data Protection Impact Assessment (DPIA) uitvoeren;
3. u moet uw klanten/gebruikers informeren over de door u uitgevoerde verwerking van hen betreffende persoonsgegevens;
4. u moet kunnen aantonen dat uw klanten/gebruikers uitdrukkelijke toestemming hebben gegeven voor de situaties waarin dat is vereist;
5. u moet uw klanten/gebruikers goed over hun rechten en de contactmogelijkheden met uw onderneming informeren.

U moet altijd kunnen aantonen dat u de AVG-verplichtingen naleeft. Dit noemen wij de verantwoordingsplicht. Hieronder geven wij meer informatie over deze AVG-verplichtingen.

Verder willen we u er op wijzen dat ook wanneer uw dienstverlening alleen op organisaties is gericht, het zeer wel mogelijk is dat de rekeninginformatie van uw klanten gegevens bevatten van personen die een transactie met uw klanten zijn aangegaan.[3] Daarmee verwerkt u persoonsgegevens en moet u dus voldoen aan de AVG. In het navolgende gaan wij er dan ook van uit dat er in het kader van uw betaaldienst persoonsgegevens worden verwerkt.

1. Ga na of u de beginselen voor de verwerking van persoonsgegevens naleeft

Artikel 5 van de AVG bevat de basisbeginselen die van toepassing zijn op het gebruik van persoonsgegevens.[4] Kort gezegd komen deze beginselen op het volgende neer.

Persoonsgegevens mogen alleen worden verwerkt in overeenstemming met de wet. Voor de betrokkene moet het behoorlijk en transparant zijn hoe en waarom de persoonsgegevens verwerkt worden.

[2] De AP beschrijft in deze brief de belangrijkste AVG-verplichtingen die waarschijnlijk op u van toepassing zijn. Naast de genoemde verplichtingen zijn er nog andere verplichtingen die mogelijk voor u van toepassing zijn. Het moge duidelijk zijn dat u ook aan die verplichtingen dient te voldoen.
[3] Dit zijn de zogenaamde 'silent party data'.
[4] De volledige wetstekst van de AVG is hier te vinden: https://autoriteitpersoonsgegevens.nl/nl/over-privacy/wetten/algemene-verordening-gegevensbescherming-avg.

Persoonsgegevens mogen alleen verzameld worden met een gerechtvaardigd doel. Dat doel moet welbepaald zijn en vooraf uitdrukkelijk zijn omschreven. Het doel waarvoor een organisatie de persoonsgegevens gaat verwerken moet verenigbaar zijn met het doel waarmee de persoonsgegevens zijn verzameld.

De persoon van wie de persoonsgegevens worden verwerkt moet goed geïnformeerd worden over de verwerking: dat betekent dat de persoon in ieder geval op de hoogte moet zijn van de identiteit van de organisatie die deze persoonsgegevens verwerkt (de zogeheten verwerkingsverantwoordelijke) en van het doel van de gegevensverwerking.

Als organisaties persoonsgegevens verwerken, dan moeten ze daarbij als uitgangspunt hanteren 'zo min mogelijk'. Dat houdt onder andere in dat alleen de gegevens die écht nodig zijn voor de dienstverlening worden verzameld en dat de gegevens worden verwijderd zodra ze niet meer nodig zijn. De organisatie moet ervoor zorgen dat de gegevens juist zijn en zo nodig worden geactualiseerd. Persoonsgegevens moeten op een passende manier goed worden beveiligd. Let op dat voor bijzondere gegevens, zoals over ras, gezondheid en geloofsovertuiging extra strenge regels gelden, ook als deze gegevens kunnen worden afgeleid uit betalingsgegevens.

Bij het ontwerp van processen waarbij persoonsgegevens worden verwerkt moet rekening worden gehouden met de principes van 'privacy by design' en 'privacy by default'. Dit houdt in dat u zowel bij het bepalen van de middelen waarmee persoonsgegevens worden verwerkt als bij de verwerking van de persoonsgegevens zelf, passende technische en organisatorische maatregelen moet treffen. Deze maatregelen moeten het doel hebben om de voorgaande gegevensbeschermingsbeginselen, zoals minimale gegevensverwerking, op een doeltreffende manier uit te voeren en de nodige waarborgen in de processen te bouwen, ter naleving van de AVG en om de rechten van de mensen waarvan u persoonsgegevens verwerkt te beschermen. Deze verplichting wordt ook wel met 'privacy by design' aangeduid. Bij de beoordeling of de maatregelen die u moet treffen passend zijn, moet u rekening houden met de volgende factoren:

- de stand van de techniek en de uitvoeringskosten;
- de aard, omvang, context en het doel van de verwerking; en
- de waarschijnlijkheid en ernst van de risico's voor de rechten en vrijheden van de personen waarvan u persoonsgegevens verwerkt.

'Privacy by default' houdt in dat u passende technische en organisatorische maatregelen treft om ervoor te zorgen dat in principe alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking. Deze verplichting geldt voor de hoeveelheid verzamelde persoonsgegevens, de mate waarin zij worden verwerkt, de termijn waarvoor zij worden opgeslagen en de toegankelijkheid daarvan.
Deze maatregelen moeten er ook voor zorgen dat persoonsgegevens niet zomaar, zonder menselijke tussenkomst, voor een onbeperkt aantal personen toegankelijk (kunnen) worden gemaakt (bijvoorbeeld op het internet).

2. Ga na of u een Data Protection Impact Assessment moet uitvoeren

Voor sommige gegevensverwerkingen moet een gegevensbeschermingseffectbeoordeling worden uitgevoerd (ook wel *data protection impact assessment*, 'DPIA' genoemd). Een DPIA bevat een beoordeling van:

- de noodzaak en de evenredigheid van de beoogde verwerkingsactiviteiten in relatie tot de doeleinden;
- de risico's voor rechten en vrijheden van betrokkenen; en
- de maatregelen die kunnen worden getroffen om die risico's zoveel mogelijk te verminderen en de getroffen maatregelen die garanderen, en waarmee men kan aantonen, dat de voorgenomen gegevensverwerking(en) aan de AVG voldoen.

Een DPIA moet worden uitgevoerd vóórdat wordt gestart met de verwerking van persoonsgegevens. Daarnaast wordt aanbevolen om een DPIA onderdeel van een voortdurende cyclus van kwaliteitsmanagement te laten zijn en het assessment regelmatig te herhalen.[5]

Voor bepaalde verwerkingen is het uitvoeren van een DPIA altijd verplicht.[6] Bijvoorbeeld bij grootschalige verwerkingen of wanneer u stelselmatig financiële gegevens monitort waaruit de inkomens- of vermogenspositie of het bestedingspatroon van mensen valt af te leiden. Dat is het geval bij overzichten van bankoverschrijvingen, overzichten van de saldi van iemands bankrekeningen of overzichten van mobiele- of pinbetalingen.

Blijkt uit de DPIA dat de verwerking een hoog risico kan opleveren als u als verwerkingsverantwoordelijke geen maatregelen neemt om het risico te beperken? Dan moet u bij de AP een Voorafgaande Raadpleging indienen voordat u met de verwerking start.[7] U mag dan nog niet met de verwerking beginnen totdat u daarover advies van de AP hebt ontvangen.

3. Ga na of u uw klanten/gebruikers alle informatie heeft gegeven over de persoonsgegevens die u van hen verwerkt

U moet passende maatregelen nemen om klanten informatie te verstrekken over de persoonsgegevens die uw onderneming van hen verwerkt.[8] Deze informatie moet in beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal beschikbaar worden gesteld. De informatie mag niet zijn weggestopt in algemene voorwaarden en moet kosteloos worden verstrekt.[9]

[5] Zie voor meer informatie over de gegevensbeschermingseffectbeoordeling de Richtsnoeren voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking "waarschijnlijk een hoog risico inhoudt" in de zin van Verordening 2016/679, WP 248 rev.01.
[6] Zie: https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia#voor-welke-soorten-verwerkingen-is-het-uitvoeren-van-een-dpia-verplicht-6667.
[7] Zie art. 36 AVG. Zie ook: https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/voorafgaande-raadpleging.
[8] Zie art. 12 AVG. Zie tevens de: Richtsnoeren inzake transparantie overeenkomstig Verordening (EU) 2016/679, WP260, v. 01.
[9] Zie voor meer informatie over de het transparantievereiste de Richtsnoeren inzake transparantie overeenkomstig Verordening (EU) 2016/679, WP260, Rev. 01.

4. Ga na of u uw klanten/gebruikers om uitdrukkelijke toestemming moet vragen

Ga na of u uw klanten/gebruikers uitdrukkelijke toestemming moet vragen voordat u om toegang vraagt tot hun betaalrekeninggegevens bij de bank.[10] Hierover treft u informatie aan op onze website.[11]
De uitdrukkelijke toestemming geldt als extra waarborg naast de overeenkomst[12] met de consument, die vanuit AVG-perspectief doorgaans de basis vormt voor de verwerking van de voor het uitvoeren van de betaaldienst noodzakelijke persoonsgegevens.

De toestemmingseis in PSD2 moet zoveel mogelijk in overeenstemming met de AVG worden uitgelegd. De AVG stelt een aantal eisen aan uitdrukkelijke toestemming:

- de toestemming moet afzonderlijk van andere onderdelen van de overeenkomst worden gevraagd;
- de toestemming moet 'specifiek' zijn en moet steeds gelden voor een specifiek doel;
- de toestemming moet 'vrij' zijn, de consument mag niet onder druk worden gezet of nadeel ondervinden van een eventuele weigering van toestemming;
- de toestemming moet 'geïnformeerd' zijn, de consument moet in duidelijke taal uitgelegd krijgen aan wie toestemming wordt gegeven, waarvoor toestemming wordt gegeven, welke gegevens worden verzameld en gebruikt en hoe de toestemming weer kan worden ingetrokken; en
- de toestemming moet eenvoudig in te trekken zijn.[13]

Als verwerkingsverantwoordelijke moet u vastleggen dat u rechtsgeldige toestemming heeft gekregen.[14] Het verkrijgen van rechtsgeldige toestemming moet u achteraf op alle voorgaande onderdelen kunnen aantonen.

5. Ga na of u uw klanten/gebruikers alle informatie heeft gegeven over hun rechten

U moet uw klanten en andere natuurlijke personen waarvan u gegevens heeft in de gelegenheid stellen hun privacyrechten uit te oefenen. Daartoe moet u passende maatregelen nemen om uw klanten/gebruikers informatie te geven over de rechten die zij als betrokkenen hebben.[15] Het gaat hierbij bijvoorbeeld om:

- het recht op inzage in alle persoonsgegevens die u over hem/haar heeft;
- het recht om onjuiste persoonsgegevens te rectificeren;
- het recht om persoonsgegevens te wissen; en
- het recht om persoonsgegevens over te (laten) dragen.[16]

---

[10] Zie art. 94 (2) PSD2.
[11] Op basis van art. 33 (2) PSD2 geldt deze verplichting niet voor natuurlijke- of rechtspersonen die uitsluitend een rekeninginformatiedienst aanbieden. Indien de rekeninginformatiedienst wordt gecombineerd met een andere betaaldienst, bijvoorbeeld een betaalinitiatiedienst, dan geldt het vereiste van uitdrukkelijke toestemming voor de toegang tot persoonsgegevens wél. Zie ook: https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-geeft-betaaldienstverleners-uitleg-over-uitdrukkelijke-toestemming-psd2#subtopic-6852.
[12] Zie voor meer informatie over de verwerkingsgrondslag 'overeenkomst' de EDPB-guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of onlineservices to data subjects, v. 2.0.
[13] Zie voor meer informatie: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/financien/betaaldiensten.
[14] Zie voor de wettelijke voorwaarden voor rechtsgeldige AVG-toestemming artikel 7 AVG. Zie voor meer informatie hierover de Richtsnoeren inzake toestemming overeenkomstig Verordening 2016/679, WP259 v.01..
[15] Zie art. 15 e.v. AVG.
[16] Zie ook: https://www.autoriteitpersoonsgegevens.nl/nl/zelf-doen/privacyrechten.

Andere AVG-verplichtingen

Uit de AVG volgen ook een aantal andere verplichtingen waar uw organisatie aan moet voldoen. Zonder uitputtend te zijn gaat dat bijvoorbeeld om de volgende zaken:

1. mogelijk is de verplichting om een functionaris voor de gegevensbescherming (FG) aan te stellen op uw organisatie van toepassing. Ook zonder verplichting raadt de AP u aan te overwegen een FG aan te stellen;
2. uw organisatie is verplicht om over een passend beveiligingsbeleid, datalekprocedures en een datalekregistratie te beschikken;[17]
3. uw organisatie moet een volledig en actueel register van verwerkingsactiviteiten hebben;
4. Werkt u samen met partijen die voor uw organisatie persoonsgegevens verwerken, bijvoorbeeld door uitbesteding? Dan moet u in een verwerkersovereenkomst afdwingbare afspraken met deze partijen maken;[18]
5. bent u voornemens persoonsgegevens vanuit Nederland door te geven naar een land buiten de Europese Unie? Dan zijn aan die doorgifte belangrijke voorwaarden verbonden.[19]

Tot slot

Wij wensen u succes met uw nieuwe bedrijfsactiviteiten en wij hopen dat u uw voordeel kunt doen met de inhoud van deze brief. Bent u op zoek naar aanvullende informatie? Kijk dan eens op onze website voor een uitgebreide toelichting op de gegevensbeschermingswetgeving: www.autoriteitpersoonsgegevens.nl. Heeft u naar aanleiding van deze brief nog vragen? Aarzelt u dan niet om contact op te nemen met ons Informatie- en Meldpunt Privacy, tijdens kantooruren bereikbaar op telefoonnummer 088 - 1805 250.

Hoogachtend,
Namens de Autoriteit Persoonsgegevens,

Ir. C.M. Schut, MPA
Directeur Systeemtoezicht, beveiliging en technologie

[17] Zie voor meer informatie over 'datalekken', en het melden daarvan, de Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679, WP250, rev. 01.
[18] Zie voor een overzicht van belangrijke regels uit de AVG: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-europese-privacywetgeving.
[19] Zie voor meer informatie: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internationaal-gegevensverkeer/doorgifte-binnen-en-buiten-de-eu.