Gemeente Amsterdam

Werkinstructie
Directies
Rechten van betrokkenen AVG/Wpg

Versie: 1.0
Datum: december 2025
Vastgesteld door: Managementteam Digitale Rechten, Ethiek en Privacy

Vakgroep Digitale Rechten, Ethiek en Privacy (DREP)
Digitale Strategie en Informatie (DS&I)
Digitale Innovatie en Informatie (DII)

Inhoudsopgave

1. Inleiding 3

2. Voorbereidingshandelingen nieuw verzoek 4

2.1 Verantwoordelijkheden en termijnen bij verzoeken 5

2.2.1 Binnenkomst via loket 6

2.2.2 Binnenkomst bij directie: directie stuurt het verzoek door naar het loket 6

2.3 Loket identificeert betrokkene 6

2.4 Loket vraagt om specificatie van het verzoek indien nodig 7

2.5 Loket stuurt verzoek door naar privacy contactpersonen van directies die relevant zijn 7

3. Directie zet binnen de directie het verzoek uit en zoekactie start 8

3.1 Ontvangen verzoek van het loket in het juiste teams mapje plaatsen bij de desbetreffende directie(s) 9

3.2 Termijnen 9

3.3 Werkwijze m.b.t. persoonsgegevens 9

3.4 Zoekactie 9

3.5 Richtlijnen verzoek uitzetten 9

3.6 Afhandeling 9

4. De verzamelde gegevens worden beoordeeld door de directie 10

5. Inhoudelijke behandeling verzoek door de directie 14

5.1 Recht op inzage (artikel 15 AVG) 15

5.2 Recht op rectificatie/ correctie (artikel 16 AVG) 16

5.3 Recht op verwijdering/ gegevenswissing / vergetelheid (artikel 17 AVG) 17

5.4 Recht op beperking van gegevensverwerking (artikel 18 AVG) 19

5.5 Recht op dataportabiliteit (artikel 20 AVG) 20

5.6 Recht van bezwaar tegen gegevensverwerking (artikel 21 AVG) 20

5.6.1 Algemeen bezwaar 20

5.6.2 Bezwaar tegen direct marketing 21

6. Input versturen naar loket 22

6.1 Loket neemt besluit 22

6.2 Loket Persoonsgegevens stuurt het besluit op 22

7. Dwangsommen, bezwaar en beroep 22

7.1 Ingebrekestelling en dwangsommen 22

7.2 Bezwaar, beroep en hoger beroep 23

1. Inleiding

Deze werkinstructie is bedoeld voor medewerkers van de gemeente Amsterdam.
In deze werkinstructie worden de procesafspraken toegelicht die binnen de gemeente Amsterdam gelden wanneer burgers op grond van de Algemene verordening gegevensbescherming (Avg) en/of de Wet Politiegegevens (WPG) een verzoek doen. Dit omvat in ieder geval de volgende types verzoeken:

- Recht op inzage
- Recht op rectificatie/ correctie
- Recht op verwijdering/ gegevenswissing / vergetelheid
- Recht op beperking van gegevensverwerking
- Recht op dataportabiliteit
- Recht van bezwaar

Het is noodzakelijk om goede afspraken te maken rondom dit proces. We hebben namelijk te maken met termijnen en andere specifieke vereisten uit de wet. Het kan bijvoorbeeld gaan een verzoek om inzage in stukken met persoonsgegevens, waarbij ook andere personen dan betrokkene identificeerbaar zijn, zoals bijvoorbeeld bij inzage in de dossiers van meldpunten zoals het meldpunt Zorg en Woonoverlast. Raadpleeg in dat geval altijd je Privacy Officer en/of je toegewezen sectorjurist.

Dit proces geldt voor zowel digitale dossiers als analoge dossiers. Hieronder staan de te doorlopen stappen benoemd. De nummering van de stappen komt overeen met de nummering van hoofdstukken. Dus: stap 1 is verder uitgewerkt in hoofdstuk 1, daar lees je wat er bij deze stap moet gebeuren.

Let op: in de handleiding wordt gesproken over de teamsomgeving van het Loket Persoonsgegevens. Op dit moment is deze teamsomgeving nog niet ingericht. Volg daarom tot nader bericht de instructies van het Loket Persoonsgegevens.

Betrokken actoren

- Loket persoonsgegevens: de meeste verzoeken komen bij het loket binnen via het online formulier: https://www.amsterdam.nl/privacy/avg-verzoek-indienen/ Het loket controleert de basiseisen aan verzoeken en stuurt deze dan door naar de desbetreffende directies.
- Privacy contactpersoon voor het loket: de persoon binnen een directie die verzoeken van het loket ontvangt (eerstelijns). De privacy contactpersoon zet het verzoek uit bij de relevante teams/personen binnen de directie en bij de relevante verwerkers (bijvoorbeeld leveranciers van systemen). De privacy contactpersoon koppelt het antwoord op het verzoek terug aan het loket. Let op: de privacy contactpersoon voor het loket, is niet altijd dezelfde persoon als de algemene privacy contactpersoon voor de directie.
- Privacy officer: de privacy officer van de directie ondersteunt waar nodig bij het beoordelen en beantwoorden van het verzoek (tweedelijns).

2. Voorbereidingshandelingen nieuw verzoek

2.1 Verantwoordelijkheden en termijnen bij verzoeken

Stedelijk is afgesproken dat directie Dienstverlening verantwoordelijk is voor de termijnbewaking van AVG-verzoeken. Dat betekent dat het Loket Persoonsgegevens ervoor zorgt dat de verzoeker binnen de wettelijke termijnen wordt geïnformeerd over zijn verzoek, het verzoek doorstuurt naar de verantwoordelijke directie(s) en/of stadsde(e)l(en), herinneringsacties doet, controleert dat alle stukken van de directie(s) op tijd binnen zijn, en escaleert als een verzoek buiten termijnen dreigt te lopen. Hiervoor is er tijdig respons nodig vanuit de keten (de verantwoordelijke directie(s) en/of stadsde(e)l(en)).

Deze tabel geeft een overzicht van alle taken die het loket en de directies moeten uitvoeren. Hieraan zijn ook uiterlijke termijnen gebonden. Uiteraard mogen stappen ook sneller worden doorlopen (het genoemde aantal dagen is het absolute maximum).

Actie	**Maximaal standaard aantal kalenderdagen vanaf dag indiening verzoek (dag 0). Mag uiteraard ook eerder (graag zelfs).**
Indien verzoek direct is binnengekomen bij ander organisatieonderdeel, stuurt het organisatieonderdeel per email het verzoek naar het Loket.	3
Loket stuurt specificatieverzoek naar verzoeker indien nodig (stopt de klok). Loket stuurt verzoek tot identificatie naar de verzoeker indien nodig (stopt de klok).	3
Loket stuurt verzoek door naar contactpersonen van relevante directies.	5
Contactpersonen directies sturen het verzoek naar relevante personen binnen directie en naar eventuele (sub)verwerkers voor antwoord. Contactpersonen bevestigen aan loket dat het verzoek in behandeling is genomen.	8
Loket stuurt herinnering naar contactpersonen directies indien nog geen bevestiging ontvangen.	11
Loket escaleert indien nog geen bevestiging van directies ontvangen.	14
Contactpersonen directies hun verzameling met beoordeelde persoonsgegevens en verdere informatie voor het verzoek naar het loket. Indien verlenging van max 2 maanden nodig is, sturen contactpersonen verzoek tot verlenging naar het loket.	20
Indien contactpersonen directies niet op dag 20 hebben geleverd, escaleert het loket.	23
Loket stuurt het opgestelde besluit naar verzoeker. In het geval van verlenging informeert loket de verzoeker over de verlenging van 2 maanden. Indien niet is	28 (wettelijke deadline)

gereageerd op specificatieverzoek of verzoek tot identificatie, stuurt loket het besluit buiten behandelingstelling.	
Onderstaande alleen bij verlenging	
Loket stuurt herinnering aan contactpersonen directies indien nog geen volledig antwoord ontvangen en vraagt ook om een update.	49
Loket stuurt herinnering aan contactpersonen directies indien nog geen volledig antwoord ontvangen en vraagt ook om een update.	61
Indien was verlengd, sturen contactpersonen directies hun antwoord op het verzoek naar het loket.	70
Indien contactpersonen directies niet op dag 70 hebben geleverd, escaleert het loket.	73
Indien was verlengd, stuurt het loket het opgestelde besluit naar de verzoeker.	84 (wettelijke deadline)

2.2.1 Binnenkomst via loket

Een verzoek kan bij het Loket Persoonsgegevens (het loket) binnenkomen hetzij via het vastgestelde webformulier, het contactformulier, per post, dan wel via de balie van stadsloketten. Het loket registreert het verzoek in haar systeem en stuurt het door naar de privacy contactpersonen van de betreffende organisatieonderdelen.

Op de website van de gemeente Amsterdam en op andere documenten en op Amsterdam.nl wordt op de mogelijkheid voor betrokkenen tot het indienen van een verzoek gewezen. Deze plaatsen zijn goed vindbaar. De betrokkenen kunnen een verzoek indienen voor het uitoefenen van hun rechten via amsterdam.nl en de daarvoor vastgestelde formulieren. De verzoeken komen in dat geval direct binnen bij het loket.

2.2.2 Binnenkomst bij directie: directie stuurt het verzoek door naar het loket

Het kan ook zijn dat verzoeken zijn vermeld in klachten of andere berichtgeving (brieven of e-mails) van een betrokkene naar een organisatieonderdeel (zoals een directie of Stadsdeel). Dit geldt voor alle types verzoeken van betrokkenen (zie Inleiding en Hoofdstuk 5).

Actie directies: In dit geval dient het organisatieonderdeel het verzoek naar het loket door te sturen per email naar 5.1, 2, i @amsterdam.nl. Dit dient snel na ontvangst te gebeuren, zie de tabel in 2.1.

Het loket registreert dan centraal het verzoek. Het is belangrijk dat het verzoek door wordt gestuurd naar het Loket Persoonsgegevens vanwege de centrale registratie, identificatie van betrokkene en de termijnbewaking. Na registratie door het Loket zal het Loket het verzoek bij de relevante directies uitzetten voor actie door de directies (zie 2.5).

2.3 Loket identificeert betrokkene

De gemeente Amsterdam dient er voor zorg te dragen dat de betrokkene ook daadwerkelijk geïdentificeerd kan worden als de rechtmatige verzoeker. Dat geldt ook voor het mondeling delen van informatie. De identiteit van de aanvrager wordt gecontroleerd voordat informatie

verstrekt wordt. Als de betrokkene namens een ander optreedt, moet hiervan een machtiging worden overlegd. Als de betrokkene jonger dan 16 jaar is of onder curatele is gesteld, moet het verzoek normaliter door de wettelijke vertegenwoordiger (bijvoorbeeld een ouder) worden gedaan. Het antwoord wordt ook aan deze wettelijke vertegenwoordiger gericht. Indien nodig of bij twijfel kan aanvullende informatie worden opgevraagd of kan verzoeker gevraagd worden naar kantoor te komen voor vaststelling van zijn of haar identiteit.

Het Loket Persoonsgegevens draagt zorg voor de identificatie van verzoeker. Dit gebeurt door het gebruik van een DigiD-koppeling of bij een stadsloket.

2.4 Loket vraagt om specificatie van het verzoek indien nodig

Als een betrokkene een breed verzoek indient, bijvoorbeeld in welke systemen van de gemeente hij of zij voorkomt, dan kan het Loket contact opnemen met verzoeker om te vragen of de betrokkene het verzoek kan specificeren. De termijn voor het beantwoorden van het verzoek wordt dan gepauzeerd tot het moment dat de betrokkene op de specificatievraag reageert.

LET OP: een betrokkene is **niet** verplicht het verzoek te specificeren. En verzoek mag dus niet geweigerd worden omdat een betrokkene het verzoek niet kan of wil specificeren. Als een betrokkene aangeeft alle informatie te willen hebben, dan moet de gemeente in principe daaraan voldoen. Dat neemt uiteraard niet weg dat het wel aan betrokkene mag worden gevraagd, door specificering van een verzoek kan vaak beter en sneller aan een verzoek worden voldaan. Naar aanleiding van contact met de betrokkene maakt het Loket waar mogelijk het verzoek concreter. Op die manier kan aan de slag worden gegaan met een gerichte zoekslag.

De mogelijkheid bestaat dat het niet lukt om een verzoek te specificeren, bijvoorbeeld omdat betrokkene daar niet aan kan of wil meewerken. In dat geval dient ook een zoekslag worden gestart in alle systemen waar de betrokkene redelijkerwijs in voor zou kunnen komen.

2.5 Loket stuurt verzoek door naar privacy contactpersonen van directies die relevant zijn

Het Loket zorgt voor doorgeleiding van het verzoek naar de privacycontactpersoon van de relevante organisatieonderdelen/ directies. Indien onduidelijk is binnen welk organisatieonderdeel de persoonsgegevens worden verwerkt en dus onduidelijk is wie procesverantwoordelijke is, dan moet dit door de relevante directies worden uitgezocht. Bij directie-overstijgende verzoeken wordt de vraag bij alle betreffende privacycontactpersonen uitgezet. Bij Wpg-verzoeken dient het loket het verzoek ook uit te zetten naar de Wpg-coordinator / Privacy Officer.

Voorbeeld: er komt een verzoek binnen waarbij alle directies/afdelingen (25 in totaal) aangevinkt worden. Na contact met de betrokkene blijkt dat deze niet wil specificeren. In dit geval betekent dat in principe dat bij alle 25 directies/afdelingen informatie moet worden uitgevraagd.

Voorbeeld: er komt een verzoek binnen voor een directie wat zowel een Wpg- als een AVG-verzoek is. Dit gecombineerde verzoek moet worden opgevat als twee verzoeken. Het is verstandig om parallel aan elkaar te werken door het verzoek uit te zetten naar de

betreffende directie (privacycontactpersoon van de directie) en gelijktijdig de Wpg-coordinator aan te haken zodat deze op de hoogte is van het Wpg verzoek. De directie beoordeelt beide verzoeken inhoudelijk, maar de directie kan de Wpg-coordinator eventueel om advies vragen voor het Wpg-gedeelte. Uiteindelijk resulteert het gecombineerde verzoek in twee Awb-besluiten: een op het AVG-gedeelte en een op het Wpg-gedeelte. Deze worden opgemaakt door het Loket na inhoudelijke beoordeling van de directie.
De uitkomst kan zijn dat beide verzoeken worden toe- of afgewezen, maar let op dat het in theorie ook mogelijk is dat de directie op basis van de AVG een verzoek kan toewijzen, terwijl tegelijk op basis van de Wpg het verzoek kan worden afgewezen.
De verschillende termijnen dienen in acht te worden genomen bij het oppakken van een gecombineerd verzoek. Het AVG-gedeelte moet binnen een maand (28 kalenderdagen) en het Wpg-gedeelte binnen zes weken) worden beantwoord.

3. Directie zet binnen de directie het verzoek uit en zoekactie start

3.1 Ontvangen verzoek van het loket in het juiste teams mapje plaatsen bij de desbetreffende directie(s)

Nadat het loket het verzoek naar de privacycontactpersoon van de desbetreffende directie heeft gestuurd, kan het inzageverzoek in behandeling genomen worden. De privacycontactpersoon bevestigt aan loket dat het verzoek in behandeling is genomen door een reactie op de mail van het loket. De privacycontactpersoon zet het verzoek/de benodigde documenten in de aangewezen submap de privacy contactpersoon toegang tot heeft.

3.2 Termijnen

De termijn voor het loket die het verzoek naar de privacycontactpersoon van de relevantie directie (s) moet sturen kan je vinden in het voorgaande hoofdstuk (2)

3.3 Werkwijze m.b.t. persoonsgegevens

Het is belangrijk dat de persoonsgegevens op juiste wijze wordt verstuurd naar de mensen die het verzoek behandelen. Er zijn twee personen aangewezen per afdeling die onderzoeken wie de behandelaar is en of diegene relevante e-mails/stukken heeft om zo het verzoek te kunnen af te handelen. Het is dan ook van uiterst belang dat het in de teams-omgeving blijft en niet per e-mail. Zo wordt er voorkomen dat informatie bij een verkeerd persoon belandt (voorkomen datalekken) of in een (persoonlijke) inbox blijft liggen (voorkomen datavervuiling, bewaartermijnen in acht nemen).

3.4 Zoekactie

De proceseigenaar zet het verzoek door naar de desbetreffende collega's of voert de zoekslag zelf uit. Het is belangrijk dat in deze stap de juiste stukken worden verzameld, zodat er hierna inhoudelijk beoordeeld kan worden.

In geval van verwerkers moet de privacycontactpersoon expliciet doorsturen aan de verwerkers.

3.5 Richtlijnen verzoek uitzetten

- Contactpersoon directie ontvangt het verzoek.
- Maak voor elke applicatie van de directie een submap in het Teams dossier.
- Geef de relevante personen die toegang hebben tot de applicatie ook toegang tot de betreffende submap. Een applicatiebeheerder mag geen toegang krijgen tot submappen voor andere applicaties.
- Stuur een mail via Outlook dat er een verzoek binnen is gekomen en verwijs naar een link naar de teamsmap. Stuur geen persoonsgegevens in de mail.
- Applicatiebeheerders voeren zoekslag uit en uploaden gegevens in hun submap.
- Contactpersoon voegt alles samen en lakt waar nog nodig.

3.6 Afhandeling

De Privacy contactpersoon plaats het resultaat van afhandelen van het verzoek (de documentatie) in het Teams kanaal van het desbetreffende dossier bij het Loket Persoonsgegevens.

Het loket stuurt bevestiging dat het verzoek in behandeling wordt genomen

In geval van verwerkers moet de privacycontactpersoon expliciet doorsturen aan de verwerkers.

4. De verzamelde gegevens worden beoordeeld door de directie

Nadat alle gegevens verzameld zijn, moeten deze inhoudelijk worden beoordeeld. Hierbij moet gekeken worden naar de aard en inhoud van de persoonsgegevens die in de gevonden stukken zijn opgenomen. Het gaat om zowel direct als indirect herleidbare gegevens. Dit houdt in dat de naam van een verzoeker een persoonsgegeven is, maar ook een beschrijving van het gedrag van verzoeker die te herleiden is naar de persoon.[1] Ook kan het zijn dat sommige documentatie (met persoonsgegevens) niet overhandigd hoeft te worden. Hieronder wordt duidelijk welke stukken dit zijn.

Persoonsgegevens
Persoonsgegevens kunnen zijn opgenomen in bijvoorbeeld e-mails, (concept) documentatie, berichten in SMS/Whatsapp/Signal en andere applicaties. De **niet-limitatieve** lijst hieronder somt een aantal voorbeelden van persoonsgegevens op.

- Naam, initialen, adres, woonplaats, telefoonnummer, e-mailadres, geboortedatum en geboorteplaats.
- BSN, financiële gegevens (bankgegevens), IP-adres.
- Strafrechtelijke gegevens of politiegegevens.
- Ras of etniciteit, politieke opvattingen, religie/ levensbeschouwelijk overtuiging, lidmaatschap vakbond, genetische gegevens, biometrische gegevens, gezondheidsgegevens en seksueel gedrag/ geaardheid.
- Gegevens over op welke datum een persoon aanwezig is geweest.
- Incidentbeschrijving over het gedrag van een persoon.
- Opnames of transcripties van gesprekken die over een persoon gaan.
- Boetedossier van een persoon.
- Meningen over een persoon.[2]

Voor meer informatie, zie: https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/privacy-en-persoonsgegevens/wat-zijn-persoonsgegevens Neem bij twijfel contact op met de Privacy Officer.

Politiegegevens
Indien de zoekslag wordt gemaakt bij een directie die politiegegevens onder de Wet Politiegegevens (Wpg) verwerkt, dan kan het voorkomen dat politiegegevens in de documentatie voorkomen. Voor de uitoefening van rechten bij politiegegevens bestaat een aparte werkinstructie. Voor het deel van de gegevens die onder de Wpg valt, dient deze werkinstructie te worden gevolgd. Schakel de Coördinator/Privacy Officer Wpg in bij twijfel.

Persoonsgegevens waar geheimhouding op rust vanuit de Wpg
Prsoonsgegevens afkomstig uit het Wpg-domein (ex-Wpg-gegevens) kunnen onder geheimhouding vallen. Schakel de Coördinator/Privacy officer Wpg in bij twijfel.

Verzamelen extra transparantie-informatie
Voor de persoonsgegevens is ook de volgende informatie nodig (artikel 15 lid 1):
a) de verwerkingsdoeleinden;
b), de betrokken categorieën van persoonsgegevens;

[1] https://www.raadvanstate.nl/uitspraken/@138714/202105922-1-a3/
[2] https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf, paragraaf 96.

c), de ontvangers of categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt, met name ontvangers in derde landen of internationale organisaties;
d), indien mogelijk, de periode gedurende welke de persoonsgegevens naar verwachting zullen worden opgeslagen, of indien dat niet mogelijk is, de criteria om die termijn te bepalen;
e), dat de betrokkene het recht heeft de verwerkingsverantwoordelijke te verzoeken dat persoonsgegevens worden gerectificeerd of gewist, of dat de verwerking van hem betreffende persoonsgegevens wordt beperkt, alsmede het recht tegen die verwerking bezwaar te maken;
f), dat de betrokkene het recht heeft klacht in te dienen bij een toezichthoudende autoriteit;
g), wanneer de persoonsgegevens niet bij de betrokkene worden verzameld, alle beschikbare informatie over de bron van die gegevens;
h), het bestaan van geautomatiseerde besluitvorming, met inbegrip van de in artikel 22, leden 1 en 4, bedoelde profilering, en, ten minste in die gevallen, nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.

De toepassing van beperkingsgronden
Let op: beperkingsgronden worden ook wel uitzonderingsgronden genoemd.

Voor de toepassing van beperkingsgronden dient gemotiveerd en gedocumenteerd te worden. Dit dient de directie mee te geven aan het Loket Persoonsgegevens zodat deze het kan delen met de betrokkenen.

Lijst van de beperkingsgronden:
De toepassing van de beperkingsgronden is afhankelijk van de aard van de persoonsgegevens. Een directie-specifieke instructie omtrent de toepassing van beperkingsgronden wordt daarom geadviseerd om de procedure goed in kaart te brengen (eventueel in samenwerking met de Privacy Officer.

De bescherming van de betrokkene(n)
(*artikel 41 lid 1 onder i van de Uitvoeringswet AVG)*

Dit beperkingsgrond komt vrijwel niet voor en dient met de toegewezen Privacy Officer (van de directie/het cluster) te worden afgestemd.

Bescherming van derden
(Artikel 15 lid 4 van de AVG en artikel 41 lid 1 onder i van de Uitvoeringswet AVG)

Het recht van de betrokkenen om documentatie te ontvangt zal de rechten en vrijheden van een derde niet nadelig mogen beïnvloeden. Derden betekent zowel personen in de nabijheid van de verzoeker, zowel buren en gezinsleden als professionals zoals ambtenaren en medewerkers. Hun persoonsgegevens kunnen verweven zijn met de persoonsgegevens van de verzoeker. Dit betekent dat een afweging gemaakt moet worden tussen de persoonsgegevens van de betrokkene en het recht op privacy van de derden. Denk hierbij aan het beperken inzage in meldingen van derden over de verzoeker, of gegevens van ambtenaren. Hierbij is het vaak niet nodig om de volledige verwerking te beperken, maar kan je de inzage beperken door de kopieën van deze gegevens niet op te nemen in het besluit. De afwijzing kan enkel worden gemaakt in de concrete situatie. Het is niet de bedoeling dat structureel wordt afgewezen op deze beperkingsgrond.[3]

[3] https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf. P. 5

Openbare veiligheid
(artikel 41 lid 1 sub a, b en c Uitvoeringswet AVG)

Deze beperkingsgrond kan het meest relevant zijn voor het veiligheidsdomein (bijvoorbeeld directie OOV) van de gemeente. Om keuze te maken voor dit beperkingsgrond dient afgestemd te worden met de toegewezen Privacy Officer (van de directie/het cluster).

Voorkoming, het onderzoek, de opsporing en vervolging van strafbare feiten
(artikel 41, lid 1 sub d Uitvoeringswet AVG)

Deze beperkingsgrond moet gemotiveerd worden door het concrete belang dat is verbonden met voorkoming, opsporing en vervolging van strafbare feiten dat zou worden geschonden het toekennen van inzage in de betreffende persoonsgegevens aan te geven.[4]
Denk hierbij aan lopende onderzoeken van bijvoorbeeld de sociale recherche.

Ongegrond of excessief
(art. 12, lid 5 AVG)

[to reject requests that are manifestly unfounded or excessive, or to charge a reasonable fee for such requests. These concepts have to be interpreted narrowly. Since there are very few prerequisites regarding access requests, the scope of considering a request as manifestly unfounded is rather limited. Excessive requests depend on the specifics of the sector in which the controller operates. The more often changes occur in the controller's database, the more often the data subject may be permitted to request access without it being excessive. Instead of refusing access, the controller may decide to charge a fee from the data subject. This would only be relevant in the case of excessive requests in order to cover the administrative costs that such requests may cause. The controller must be able to demonstrate the manifestly unfounded or excessive character of a request.] p.5

Voorbeeld: Betrokkene dient een inzageverzoek in. Dit verzoek wordt ingewilligd. Twee weken later dient betrokkene een nieuw inzageverzoek in om inzage te krijgen in dezelfde gegevens. Deze gegevens hoeven wij niet nogmaals te verstrekken. Het inzageverzoek kan in dergelijke gevallen worden afgewezen door het Loket Persoonsgegevens.

Vertrouwelijkheid van de informatie
Het is ook mogelijk dat wettelijk is bepaald dat er een geheimhouding rust op de gegevens, waardoor deze gegevens niet gedeeld mogen worden met de verzoeker. Denk hierbij aan de geheimhoudingsplicht uit artikel 23 wet Bibob en fiscale geheimhoudingsplicht uit artikel 67 AWR

Toepassing van beperkingsgronden[5]
Als het noodzakelijk is om bepaalde informatie niet te delen, bijvoorbeeld gelet op de rechten en vrijheden van anderen, kan het nodig zijn om beperkingsgronden toe te passen.

Het toepassen van de beperkingsgronden moet, naast noodzakelijk, ook proportioneel zijn. Afhankelijk van de zwaarte van de beperkingsgrond kan bijvoorbeeld enkel de inzage in de kopie van het persoonsgegeven beperkt worden, maar het kan ook voorkomen dat de hele verwerking beperkt, en dus weggelaten, moet worden. Zorg ervoor dat deze afweging beargumenteerd is en gedocumenteerd wordt, zodat het bij eventuele bezwaren en verdere juridische procedures duidelijk is waarom bepaalde onderdelen zijn beperkt. Als je twijfelt over het toepassen van de beperkingsgrond, schakel dan je Privacy Officer in.

---

[4] Zie: ABRvS 24 januari 2007, ECLI:NL:RVS:2007:AZ6853
[5] art. 41 lid 2 UAVG

Voorbeeld: Een verzoeker vraagt om inzage in meldingen over deze persoon. Deze meldingen zijn gedaan door buren die zich zorgen maakten over deze verzoeker. De inhoud van deze melding bevat zowel persoonsgegevens van de verzoeker als van de buren. Deze buren nemen wij in bescherming omdat hun rechten en vrijheden in het geding zouden komen bij het verstrekken van de inhoud van de melding. De inhoud van de melding verstrekken wij niet voor zover dit impact kan hebben op de buren. De rest van de informatie/melding wordt wel verstrekt.

Voorbeeld: De verzoeker vraagt expliciet om inzage in communicatie omtrent diens persoon. Na het uitvoeren van de zoekslag komt naar boven dat de directie correspondentie heeft vanuit diens advocaat. Gezien de advocaat de verzoeker bijstaat, schaadt het de rechten en vrijheden van de advocaat niet indien deze gegevens verstrekt worden aan de verzoeker. De gegevens van de advocaat hoeven daarom niet beperkt te worden.

5. Inhoudelijke behandeling verzoek door de directie

Betrokkenen kunnen verschillende rechten uitoefenen ten aanzien van hun persoonsgegevens. De onderstaande rechten van betrokkenen hebben betrekking op de AVG (artikel 15 en verder). Rechten van betrokkenen op grond van de Wpg (artikel 25 en verder) zijn uitgewerkt in de aparte werkinstructie voor de Wpg.

5.1 Recht op inzage (artikel 15 AVG)

Een betrokkene kan een aanvraag doen voor het recht op inzage op grond van artikel 15 AVG.
De directie beoordeelt het verzoek tijdig, binnen de tijdslijnen zoals bedoeld in hoofdstuk 2.
Middels zoekslagen dient te worden nagegaan of er persoonsgegevens van de betrokkene worden verwerkt.

- Bevestiging *of* er persoonsgegevens van de betrokkene verwerkt worden.
- Als er geen gegevens worden verwerkt, moet dit eveneens door de betreffende directie(s) aan het Loket Persoonsgegevens binnen de afgesproken tijdslijnen zoals bedoeld in hoofdstuk 2 teruggekoppeld worden zodat dit in het besluit kan worden opgenomen. Het Loket Persoonsgegevens koppelt dit terug aan de betrokkene en verwijst hierbij naar de specifieke privacyverklaring (als deze beschikbaar is).

In geval dat er persoonsgegevens van de betrokkene worden verwerkt heeft de betrokkene in beginsel recht op inzage en ook op de volgende informatie:

- Het doel van de verwerking(en)
- Categorieën van persoonsgegevens
- Kopieën van persoonsgegevens. Indien nodig, kopieën van extracten van documenten dan wel volledige documenten als dit nodig is om de context van de gegevensverwerking te begrijpen, bijvoorbeeld in het geval van facturen. [6]
- Toegepaste beperkingsgronden met motivatie, zie hiervoor hoofdstuk 4.
- Bron(nen) van de gegevens
- Ontvanger(s) van de gegevens
- Bewaartermijn per verwerking, wanneer loopt deze af en wat de uitzonderingen zijn voor het verlengen van de bewaartermijn
- Of er sprake is van (deels) geautomatiseerde besluitvorming

De directie heeft de taak om te beoordelen of de verzamelde informatie gedeeld kan worden. Betrek bij twijfel de Privacy Officer. Welke informatie wel of niet wordt gedeeld dient gemotiveerd te worden. Houd daarbij rekening met het feit dat het inzagerecht geen afbreuk mag doen aan rechten of vrijheden van anderen.

Lakken
De directie draagt zorg voor het lakken van de documenten. Er zijn licenties voor Adobe voor lakken persoonsgegevens beschikbaar. De directies moeten dat via Topdesk aanvragen. Het ligt voor de hand om in elk geval aan de privacy contactpersoon een licentie toe te kennen. Aanbeveling is om minimaal twee personen per directie te hebben met deze licentie.

[6] Zie ook jurisprudentie (HvJEU C-487/21) en richtlijnen van de AP

Er is een werkinstructie lakken beschikbaar. Zie: 5.1, 2, i

5.1, 2, i

Let er bij het lakken op dat metadata (verborgen data in het bestand dan wel de eigenschappen daarvan) wordt verwijderd.

Voor een deel van deze gegevens, te weten het doel van de verwerking(en), de categorieën, de bewaartermijnen van deze gegevens en of er sprake is van (deels) geautomatiseerde besluitvorming kan verwezen naar de privacyverklaring, indien deze aanwezig is. Als deze informatie niet blijkt uit de privacyverklaring, kan deze informatie ook grotendeels verwerkt worden in een tabel met een begeleidende tekst, zoals onderstaand voorbeeld:

In de onderstaande tabel zijn uw persoonsgegevens opgenomen die zijn verwerkt in het kader van [doel verwerking], met uitzondering van persoonsgegevens waarop een beperkingsgrond van toepassing is.

■ **Categorie**	■ **Persoonsgegevens**	■ **Bron**	■ **Ontvanger**	■ **Toelichting**
■ *In wat voor type document het persoonsgegeven is opgenomen*	■ *Bekend bij betrokkene/geen inzage vanwege beperkingsgrond X/kopie van persoonsgegeven (bijvoorbeeld naam/ adres)/ bijlage met langer document als persoonsgegevens veelomvattend zijn en verwijs dan naar de bijlage (bijvoorbeeld een email over een persoon)/ kopie extract document als bijlage toevoegen indien nodig om de context van de verwerking te begrijpen (bijvoorbeeld een factuur).*	■ *Directies binnen de gemeente, partners, burgers etc.*	■ *Directies binnen de gemeente, partners, burgers etc.*	■ *Context over de verwerking, indien de toelichting niet nodig is, kan deze kolom verwijderd worden.*

Met het inzagerecht wordt onder andere beoogd dat de betrokkene in staat wordt gesteld om op de hoogte te zijn van wat er wordt verwerkt en of dit juist is (controle van de rechtmatigheid). Een inzageverzoek kan leiden tot de uitoefening van andere rechten (zoals bijvoorbeeld een rectificatie- of verwijderverzoek). Deze andere rechten worden verderop in dit hoofdstuk toegelicht.

5.2 Recht op rectificatie/ correctie (artikel 16 AVG)

Als de persoonsgegevens onjuist of onvolledig zijn, heeft de betrokkene recht op het vragen om het verbeteren of aanvullen van de gegevens. De betreffende directie dient na te gaan of de persoonsgegevens uit het verzoek overeenkomen met de persoonsgegevens zoals bekend bij de directie. Indien deze niet overeenkomen dient de directie de persoonsgegevens te verbeteren of aan te vullen.
Let op dat het rectificatie- of correctierecht niet is bedoeld om indrukken, meningen, onderzoeksresultaten en conclusies waarmee de betrokkene zich niet kan verenigen te corrigeren of te verwijderen. De rectificatie/correctie dient wel te worden opgenomen in het dossier als aannemelijk is dat dit correct is.

Wel kan het zijn dat een feitelijke weergave onjuist blijkt te zijn. Als de onjuistheid aannemelijk is gemaakt, kan er wel een beroep worden gedaan om dit te verbeteren.

Correctie mening/ indruk/ onderzoeksresultaat/ conclusie	**Correctie feitelijke vastlegging**
In het dossier van persoon X staat de volgende notitie die is gemaakt door persoon Y: 'Ik zag dat persoon X op maandag te laat op kantoor was'. Indien X aantoont dat hij maandag op tijd was, wordt dit toegevoegd aan het dossier van X. De mening kan van Y wel worden bewaard, als maar duidelijk is dat deze mening succesvol is weerlegd door X.	In de absentiekalender van persoon X staat dat hij op maandag 'te laat' was. Indien X aantoont dat hij op tijd was, dient de feitelijke 'te laat' melding uit de absentiekalender van persoon X te worden aangepast naar 'op tijd'.

5.3 Recht op verwijdering/ gegevenswissing / vergetelheid (artikel 17 AVG)

Onder bepaalde omstandigheden mag een betrokkene verzoeken om zijn persoonsgegevens te laten verwijderen. In de AVG heet dit het 'recht op gegevenswissing of 'recht op vergetelheid'. Soms zijn er wettelijke bewaartermijnen die ervoor zorgen dat een recht op vergetelheid niet volledig voor een dossier kan gelden, maar slechts deels. Mensen hebben het recht op verwijdering van persoonsgegevens als er geen goede reden (meer) is om de gegevens nog te bewaren. Het gaat in principe om alle informatie die direct of indirect naar de verzoeker herleidbaar is. Dat betekent dat de directie die de persoonsgegevens heeft verwerkt ook moet zorgen dat gegevens die elders terecht zijn gekomen (bijvoorbeeld bij een verwerker) daar ook verwijderd worden.

Wanneer de directie een verzoek om verwijdering ontvangt, neemt deze het verzoek in behandeling. Hierbij dient de directie na te gaan of aan één van de volgende vereisten in voldaan:

- Of de persoonsgegevens niet langer nodig zijn (neem contact op met de Adviseur Informatiebeheer voor de bewaartermijn(en) van het desbetreffende proces);
- Of toestemming is ingetrokken (wanneer om toestemming gevraagd is om de persoonsgegevens te verwerken) en er geen andere rechtsgrond is om de gegevens te verwerken;
- Indien er terecht bezwaar is gemaakt tegen de verwerking en er geen dwingende gerechtvaardigde gronden voor de verwerking zijn die prevaleren;

- Indien er onrechtmatig wordt verwerkt (dus de directie de gegevens helemaal niet zou mogen verwerken);
- Indien de persoonsgegevens volgens een wettelijke bepaling moeten worden verwijderd;
- Wanneer het verzoek gaat over persoonsgegevens van een kind die door een directie worden verwerkt (de juridische omschrijving is "Wanneer aan kinderen aangeboden diensten van de informatiemaatschappij betreft"). In de AVG is opgenomen dat kinderen recht hebben op specifieke bescherming van hun persoonsgegevens. Van kinderen wordt aangenomen dat zij nog niet volledig bewust zijn van de risico van gegevensverwerking, (vooral als het bijvoorbeeld gaat om diensten die via internet worden aangeboden).

Is aan geen van de bovenstaande eisen voldaan? Dan moet de directie duidelijk motiveren waarom en dit terugkoppelen aan het loket. De persoonsgegevens hoeven dan niet verwijderd te worden.

Is wel aan (minstens) één van de bovenstaande eisen voldaan, dan moet de directie controleren of een uitzondering op het recht op verwijdering geldt. De verwijdering hoeft niet te worden uitgevoerd voor zover verwerking nodig is voor een van de volgende uitzonderingen:
a) voor het uitoefenen van het recht op vrijheid van meningsuiting en informatie;
b) voor het nakomen van een wettelijke verwerkingsverplichting (zoals de Archiefwet of de fiscale bewaarplicht van 7 jaar). Of voor het vervullen van een taak van algemeen belang of het uitoefenen van het openbaar gezag dat aan de verwerkingsverantwoordelijke is verleend;
c) om redenen van algemeen belang op het gebied van volksgezondheid;
d) met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden, voor zover verwijdering deze doeleinden onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen;
e) voor de instelling, uitoefening of onderbouwing van een rechtsvordering.
NB: Soms wordt ook wel de buitensporigheid (het voorkomen van misbruik, artikel 12 lid 6 AVG) genoemd als grond om een verzoek tot vergetelheid af te wijzen, maar dit komt slechts bij hoge uitzondering voor. Betrek hierbij altijd de privacy officer.

Geldt er geen uitzondering? Dan moet de directie de persoonsgegevens verwijderen. Geldt er wel een uitzondering? Dan moet de directie duidelijk motiveren waarom.

De directie koppelt aan het loket terug wat de afwegingen zijn waarom het verwijderverzoek al dan niet ingewilligd kan worden. Het loket maakt daarna het besluit op en verzendt dit naar de verzoeker.

De applicaties die directies (en hun verwerkers) gebruiken moet de persoonsgegevens volledig kunnen verwijderen/vernietigen. Archiveren of verstoppen is niet voldoende.

In geval van gegevenswissing moet de directie ook alle andere organisaties die de persoonsgegevens hebben gekregen informeren dat de betreffende persoonsgegevens moeten worden gewist.

De directie is verplicht om iedereen met wie de (verwijderde) persoonsgegevens zijn uitgewisseld, te informeren over de vernietiging. Tenzij dit onmogelijk is of onevenredig veel inspanning vraagt.

Voorbeeld: Meneer X heeft een vergunning aangevraagd, die is afgewezen. Volgens de archiefwet geldt hiervoor een bewaartermijn van 3 jaar. Na 1 jaar dient meneer X een verwijderingsverzoek in.

De directie wijst het verzoek af, omdat een wettelijke verwerkingsverplichting onder de archiefwet een uitzonderingsgrond op verwijdering vormt.
Na 3 jaar en 2 maanden dient meneer X nogmaals een verwijderingsverzoek in. De gegevens zijn dan nog niet verwijderd. De directie dient nu wel de gegevens te verwijderen, omdat de wettelijke bewaartermijn is verlopen en er geen verdere gronden zijn om de gegevens te bewaren. De directie geeft de leverancier van het vergunningsysteem (een verwerker) opdracht om de persoonsgegevens te verwijderen. De verwerker laat weten dat dit is gebeurd. De directie koppelt aan het loket terug dat de persoonsgegevens verwijderd zijn.

5.4 Recht op beperking van gegevensverwerking (artikel 18 AVG)

Het recht op beperking van verwerking houdt in dat betrokkenen in een beperkt aantal gevallen tijdelijk de verwerking van hun persoonsgegevens stil kunnen laten zetten. De verwerking mag dan alleen nog maar in bepaalde gevallen. Dit kan voorkomen als iemand het niet eens is met het gebruik van bepaalde gegevens en een beroep heeft gedaan op correctie van die gegevens. Je mag dan alleen nog maar de gegevens bewaren, niet gebruiken. Ze zijn dan bevroren. Totdat daarover is beslist worden die betwiste gegevens niet gebruikt door de gemeente.

De persoonsgegevens van de betrokkene(n) moeten worden beperkt als:

- De betrokkene stelt dat de persoonsgegevens onjuist zijn gedurende een periode waarin die de verwerkingsverantwoordelijke in staat stelt om de juistheid te controleren;
- De verwerking onrechtmatig is en de betrokkene zich verzet tegen het wissen van de persoonsgegevens en verzoekt in plaats daarvan gebruik te maken van beperking;
- De verwerkingsverantwoordelijke de persoonsgegevens niet meer nodig heeft voor de verwerkingsdoeleinden, maar de betrokkene deze nodig heeft voor de instelling, uitoefening of onderbouwing van een rechtsvordering;
- De betrokkene bezwaar heeft gemaakt tegen de verwerking in afwachting van een antwoord op de vraag of de gerechtvaardigde gronden van de verwerkingsverantwoordelijke zwaarder wegen dan die van betrokkene.

De directie die het verzoek ontvangt dient na te gaan wat er precies gevraagd wordt en indien juist het recht op beperking toe te passen. Zo lang de discussie loopt, mag de gemeente de betwiste persoonsgegevens niet gebruiken of uitwisselen.
Het feit dat de verwerking van de persoonsgegevens beperkt is, moet door de verwerkingsverantwoordelijke duidelijk zijn aangegeven, zodat dit ook duidelijk is voor de (dagelijkse) gebruikers en ontvangers van de persoonsgegevens. Voorkom dat er toch per ongeluk gebruik wordt gemaakt van bevroren gegevens. Geef het recht van beperking van de verwerking van deze persoonsgegevens door aan de betreffende directies, afdelingen en verwerkers die deze persoonsgegevens verwerken.

Wanneer de verwerkingsverantwoordelijke overgaat op opschorting van de verwerking, kan de verwerkingsverantwoordelijke (met uitzondering van de opslag van persoonsgegevens) enkel nog verwerken:

- Met toestemming van de betrokkene
- In het kader van een rechtsvordering
- Ter rechtsbescherming van rechten van anderen
- In gewichtige redenen van algemeen belang

Daarnaast dient de verwerkingsverantwoordelijke de betrokkene vooraf op te hoogte stellen wanneer de beperking wordt opgeheven.

Voorbeeld:
Een discussie over een postadres van een betrokkene. De betrokkene dient een verzoek tot beperking van het ogenschijnlijk foutieve postadres in. Zo lang er geen duidelijkheid is over de juistheid van het postadres stuurt de gemeenten geen post naar het (ogenschijnlijke foutieve) postadres.

5.5 Recht op dataportabiliteit (artikel 20 AVG)

Het recht op dataportabiliteit houdt in dat een betrokkene zijn digitale persoonsgegevens meeneemt en overdraagt aan een andere organisatie. Het doel van dit recht is om de zeggenschap van de betrokkene over en uitwisseling van hun persoonsgegevens te vergroten. De betrokkene heeft een recht op een kopie in een gangbare en machineleesbare vorm (bijvoorbeeld CSV, JSON en XML).

Ook hij heeft het recht die gegevens aan een andere verwerkingsverantwoordelijke over te dragen. Indien dit technisch mogelijk is, dient de verwerkingsverantwoordelijke de gegevens rechtstreeks aan de andere verwerkingsverantwoordelijke over te dragen indien de betrokkene hierom vraagt.

De betrokkene heeft het recht op dataportabiliteit alleen indien:
1. De verwerking op de grondslag 'toestemming' of 'overeenkomst' is gebaseerd; en
2. De verwerking via geautomatiseerde procedés wordt verricht (dus bijvoorbeeld via een computersysteem).

Voorbeeld: Een betrokkene vraagt om de persoonsgegevens die hij heeft ingevuld op een formulier van de gemeente om een parkeerticket te kopen. Deze gegevens worden verwerkt op basis van de grondslag 'overeenkomst'. De parkeerticket wordt door het systeem van de gemeente opgeslagen in PDF-formaat dat niet machine-leesbaar is. De betrokkene wil de persoonsgegevens in het machineleesbare CSV-formaat (Excel) verkrijgen. De gemeente dient de gegevens van het formulier in CSV-formaat te verstrekken, volgens het recht op dataportabiliteit.

De betrokkene vraagt of de gemeente de persoonsgegevens rechtstreeks kan overdragen aan een privaat parkeerbedrijf in CSV-formaat. Om te voldoen aan het recht op dataportabiliteit, draagt de gemeente de persoonsgegevens over.

5.6 Recht van bezwaar tegen gegevensverwerking (artikel 21 AVG)

Er bestaan twee rechten van bezwaar tegen verwerking tegen persoonsgegevens: een algemeen recht van bezwaar, en een rechts van bezwaar tegen direct marketing. **Let op**: dit is dus wat anders dan het indienen van een bezwaarschrift onder de Algemene wet bestuursrecht (Awb).

5.6.1 Algemeen bezwaar

De betrokkene heeft te allen tijde het recht om vanwege met zijn specifieke situatie verband houdende redenen bezwaar te maken tegen de verwerking van hem betreffende persoonsgegevens, met inbegrip van profilering. Dit geldt echter alleen voor verwerkingen op basis van een van de volgende grondslagen:

- 'algemeen belang/ openbaar gezag'; of

- ‘gerechtvaardigd belang’

De verwerkingsverantwoordelijke staakt de verwerking van de persoonsgegevens, tenzij hij dwingende gerechtvaardigde gronden voor de verwerking aanvoert die zwaarder wegen dan de belangen, rechten en vrijheden van de betrokkene of die verband houden met de instelling, uitoefening of onderbouwing van een rechtsvordering.

Er moet dus een belangenafweging worden gemaakt naar aanleiding van het verzoek van betrokkene. Indien de belangen van de betrokkene zwaarder wegen, dient de verwerking te worden gestopt. Dit kan ook betekenen dat de persoonsgegevens dienen te worden verwijderd. Schakel hierbij met de privacy officer.

Voorbeeld: De gemeente wil een AI-systeem trainen met gegevens over parkeerbewegingen, inclusief kentekens, met als doel om burgers te adviseren over waar zij het best kunnen parkeren. Een betrokkene maakt bezwaar tegen het opnemen van zijn persoonsgegevens (kenteken) in de trainingsdata voor het AI-systeem. Na het uitvoeren van een belangenafweging, concludeert de gemeente dat deze verwerking van de persoonsgegevens van betrokkene dient te worden gestaakt. De persoonsgegevens van betrokkene mogen dan dus niet meer worden opgenomen in de trainingsdata. Indien de gegevens al zijn opgenomen in de trainingsdata dienen deze ook te worden verwijderd. Deel dit mee in het besluit zodat de betrokkene op de hoogte is van de verwijdering.

5.6.2 Bezwaar tegen direct marketing

Wanneer persoonsgegevens voor direct marketing worden verwerkt, heeft de betrokkene altijd het recht bezwaar te maken tegen de verwerking van hem betreffende persoonsgegevens voor dergelijke marketing, met inbegrip van profilering die betrekking heeft op direct marketing.

Wanneer de betrokkene bezwaar maakt tegen verwerking ten behoeve van direct marketing, worden de persoonsgegevens niet meer voor deze doeleinden verwerkt.

Dit geldt voor alle verwerkingen voor direct marketing. De grondslag die hierbij gebruikt wordt, is niet relevant. Ook hoeft er geen belangenafweging te worden gemaakt, omdat het bezwaar altijd dient te worden ingewilligd.

Direct marketing is een breed begrip. Het omvat het overbrengen van communicatie aan de betrokkene voor commerciële, ideële of charitatieve doeleinden.

Voorbeeld: Een betrokkene vraagt de gemeente om geen direct marketing over schone voertuigen van partnerbedrijven per email te sturen. Om te voldoen aan het recht op bezwaar, stopt de gemeente met het versturen van zulke marketing naar deze betrokkene per email.

6. Input versturen naar loket

De directie koppelt de uitkomst van het verzoek terug aan het loket.

De stukken met persoonsgegevens moeten gelakt en in PDF-format moeten worden aangeleverd in de aangewezen map op de Sharepoint omgeving. De verdere informatie rondom de verwerking, zoals een verwijzing naar de privacyverklaring, of beantwoording van het verzoek kunnen via een Wordbestand aangeleverd worden. Plaats de stukken in de map voor jouw directie.

In geval van een geheel of gedeeltelijke afwijzing van een verzoek, moet in het schriftelijke antwoord aan de verzoeker gemotiveerde reden(en) vermeld staan. De directie levert de gemotiveerde reden(en) aan bij het loket. Stem de motivatie af met je privacy officer.

Let op: Het loket beoordeelt de stukken niet inhoudelijk en zal ontvangen (ongelakte) documenten niet lakken. Als je dus twijfelt over de invulling van het recht op inzage, neem dan contact op met de privacy officer van je directie.

Voor lak-instructies, zie:5.1, 2, i
5.1, 2, i

6.1 Loket neemt besluit

De contactpersoon levert binnen de vastgestelde termijn, zie de tabel in hoofdstuk 2.1, de stukken aan. Voorafgaand is de inhoud van de stukken getoetst binnen het organisatieonderdeel.

Het Loket Persoonsgegevens stelt het besluit op aan de hand van de verzamelde informatie en het sjabloon uit de bijlagen bij deze instructie. Dit besluit wordt ondertekend door de directeur van Dienstverlening. Deze persoon heeft op basis van ondertekeningsmandaat de bevoegdheid besluiten te tekenen voor de directies.

De beslissingen van een bestuursorgaan met betrekking tot de verzoeken worden aangemerkt als een besluit in de zin van de Awb op grond van artikel 34 Uitvoeringswet Algemene verordening gegevensbescherming (UAVG).

6.2 Loket Persoonsgegevens stuurt het besluit op

Het kan voorkomen dat de informatie een inzageverzoek bij verschillende directies/ afdelingen moet worden opgehaald alvorens een besluit door het Loket Persoonsgegevens kan worden gemaakt. De betreffende directie levert de informatie uiterlijk op dag 20, of bij verlenging uiterlijk op dag 70 aan het Loket Persoonsgegevens.

7. Dwangsommen, bezwaar en beroep

7.1 Ingebrekestelling en dwangsommen

Op grond van artikel 29 Wpg /artikel 34 UAVG, is de Awb van toepassing op beslissingen naar aanleiding van de uitoefening van rechten van betrokkenen op grond van artikel 15-22 AVG. Als de gemeente te laat reageert op een verzoek, kan de verzoeker de gemeente in gebreke stellen en onder voorwaarden dwingen een dwangsom te betalen. De dwangsommen dienen betaald te worden door de desbetreffende directie(s) die te laat reageerden op het verzoek. Dit is ook gepubliceerd op de website van de Gemeente: Gemeente te laat met beslissing (ingebrekestelling) | Gemeente Amsterdam

7.2 Bezwaar, beroep en hoger beroep

De beslissing (of het uitblijven van een tijdige beslissing) is een besluit waartegen bezwaar kan worden gemaakt en beroep kan worden ingesteld onder de Awb. Een verzoeker kan binnen zes weken na ontvangstdatum van de beslissing bezwaar aantekenen. Komt een bezwaarschrift na deze termijn van 6 weken binnen, stuurt dit alsnog door aan de desbetreffende afdeling.

Het bezwaarschrift kan op verschillende manieren binnenkomen. Vaak gebeurt dit via het online bezwaarformulier, maar het kan ook via de post. Het is zaak dat het bezwaar landt bij de directie die bezwaren behandelt. Stuur het bezwaarschrift zo nodig door aan de desbetreffende directie. Dit is afhankelijk van het onderwerp van het besluit. Zie onderstaande tabel.

Afdeling/directie	Mailadres	Onderwerpen
Juridische Zaken (JZ)	DJZ Griffie Bezwaar- en beroepschriften 5.1, 2, i @amsterdam.nl	OOV, Treiteraanpak (*tot dat er een nieuw convenant is, daarna naar JB)*, Burgemeester, Kabinet, Politiek gevoelige onderwerpen, Politie/Veiligheid [Directie overstijgend]
Juridisch Bureau (JB)	Juridischbureau.bezwaren 5.1, 2, i @amsterdam.nl	Stadsdelen, overige directies
Basisinformatie	Bezwaarcommissie Basisinformatie 5.1, 2, i @amsterdam.nl	Alle BRP-gerelateerde bezwaren (adresonderzoek, protocollijst)
Juridisch bureau Sociaal (SIS)	BezwaarenBeroep.sociaal 5.1, 2, i @amsterdam.nl	Alle bezwaren in het Sociaal Domein (muv GGD)
GGD	Privacy GGD Amsterdam 5.1, 2, i @ggd.amsterdam.nl	GGD

Belastingen	Vraag het Loket Persoonsgegevens voor de contactpersoon	Belastingen behandelt zelf

Deze directie is dan in de lead. Zij zijn namelijk verantwoordelijk voor het uiteindelijke besluit op bezwaar. Hiervoor kan informatie nodig zijn vanuit de directie. Vragen over de inhoud van het verzoek dienen beantwoord te worden door de directie die de inhoud heeft behandeld. Hiervoor wordt de Teams omgeving van het desbetreffende verzoek door het Loket opnieuw geopend. Hierbij kan het voorkomen dat ongelakte stukken moeten worden geüpload voor beoordeling van de beperkingen van het verzoek.

Beroep, hoger beroep
Na de beslissing op bezwaar staat beroep, en daarna hoger beroep open bij de bestuursrechter. Hierbij kunnen weer inhoudelijke vragen gesteld worden aan de directie. Zorg dus voor voldoende capaciteit, niet alleen voor het afhandelen van de verzoeken, maar ook voor het mogelijke gevolg.

Voorbeeld: Persoon X heeft een besluit op diens inzageverzoek ontvangen en is het niet eens met de toepassing van de beperkingsgronden. Diegene tekent bezwaar aan en stelt dat de beperkingsgronden niet van toepassing horen te zijn. De bezwaarcommissie vraagt vervolgens de ongelakte stukken op en vraagt aan de directie waarom bepaalde woorden zijn gelakt.