Autoriteit
Consument & Markt

Openbaar

Consultatieversie Leidraad

Leidraad Data Delen

Data delen van verbonden producten en gerelateerde diensten

Samenvatting

Doel Dataverordening

Hoofddoel en achtergrond
De Autoriteit Consument en Markt (hierna: ACM) publiceert deze leidraad in het kader van de Dataverordening, die op 12 september 2025 in werking treedt. Deze verordening maakt onderdeel uit van de Europese datastrategie, gericht op het creëren van een interne datamarkt waar gegevens vrij kunnen stromen. Het belangrijkste uitgangspunt is dat de gebruiker zeggenschap krijgt over gegevens die worden verzameld door verbonden producten en gerelateerde diensten. Verbonden producten zijn apparaten die verbinding kunnen maken met het internet en gegevens uitwisselen. Voorbeelden zijn een slimme thermostaat, een moderne auto of een melkrobot. Vaak kunnen deze apparaten op afstand worden bediend en verzamelen zij, via sensoren, gegevens. Een gerelateerde dienst is een digitale dienst die gekoppeld is aan een verbonden product en waarmee de functionaliteit, het gedrag of de bediening van het verbonden product kan worden beïnvloed, bijvoorbeeld via een app.

Alle ondernemingen die verbonden producten of gerelateerde diensten aanbieden, vallen onder de Dataverordening. Ook ondernemingen buiten de Europese Unie (hierna: EU) vallen hieronder als zij verbonden producten in de EU in de handel brengen of gerelateerde diensten in de EU aanbieden.

Deze leidraad richt zich primair op organisaties die verplichtingen uit de Dataverordening krijgen opgelegd: fabrikanten, leveranciers, verkopers, verhuurders en leasegevers van verbonden producten en gerelateerde diensten binnen de EU.

Toezicht
De ACM wordt naar verwachting aangewezen als toezichthouder op een groot deel van de Dataverordening en als datacoördinator voor Nederland. Ook de Autoriteit Persoonsgegevens (hierna: AP) krijgt een aantal toezichtstaken. Organisaties met hun (Europese) hoofdkantoor in Nederland vallen onder het toezicht van deze Nederlandse autoriteiten. De uitvoeringswet die dit regelt wordt in de komende periode in het parlementair proces behandeld.

Belangrijkste partijen en termen

Belangrijkste partijen
De Dataverordening heeft invloed op veel verschillende partijen. De belangrijkste spelers in de Dataverordening zijn:

- **Gebruiker**: de persoon of organisatie die het recht heeft om een verbonden product te gebruiken;
- **Gegevenshouder**: de partij die het recht of de verplichting heeft om gegevens beschikbaar te stellen;
- **Gegevensontvanger**: de partij die gegevens ontvangt voor professionele doeleinden;
- **Derde partij**: een partij die toegang tot gegevens kan krijgen als de gebruiker dat wil;
- **Verkoper**: een partij die handelt in het kader van een commerciële activiteit;
- **Houder van een bedrijfsgeheim**: een partij die beschikt over vertrouwelijke bedrijfsinformatie.

Type gegevens
De Dataverordening verplicht gegevenshouders om in bepaalde gevallen gegevens te delen met gebruikers en derde partijen. Hierbij zijn verschillende type gegevens relevant:

- **Eenvoudig beschikbare gegevens**: Productgegevens en gegevens van een gerelateerde dienst die een gegevenshouder gemakkelijk en rechtmatig verkrijgt of kan krijgen, zonder dat daar een grote inspanning voor hoeft te worden geleverd.

- **Gebruikersgegevens**: Gegevens die voortkomen uit de interactie tussen de gebruiker en een verbonden product of gerelateerde dienst. Deze gebruikersgegevens zijn onder te verdelen in drie soorten:
  - **Productgegevens**: Ruwe, onbewerkte gegevens die rechtstreeks door het verbonden product worden verzameld door gebruik van het product, de prestaties ervan, of het milieu waarin het product zich bevindt. Productgegevens kunnen door een gebruiker, gegevenshouder of derde partij, waaronder de fabrikant, worden opgevraagd via een elektronische communicatiedienst, fysieke verbinding of directe toegang tot het product. Beschrijvende gegevens over het product, gebruikshandleidingen en verpakkingsinformatie zijn geen productgegevens.
  - **Gegevens van een gerelateerde dienst**: Gegevens die worden gegenereerd door de handelingen van de gebruiker met het verbonden product of het verlenen van de gerelateerde dienst zelf.
  - **Metagegevens**: Gegevens die extra informatie geven over de productgegevens, waardoor de gerelateerde dienst deze correct kan interpreteren en gebruiken.

Samenloop met andere wetgeving
- De AVG blijft volledig van toepassing op persoonsgegevens. Bij conflict heeft de AVG voorrang.
- De Dataverordening doet geen afbreuk aan intellectueel eigendomsrecht, consumentenrecht en contractenrecht.
- Sectorale regelgeving, zoals de NIS2-richtlijn, blijft onverminderd van toepassing.

Thema 1 Informatieverplichting

De Dataverordening legt specifieke informatieverplichtingen op aan aanbieders van verbonden producten of gerelateerde diensten. Deze verplichtingen gelden voorafgaand aan het sluiten van een overeenkomst voor de aankoop, huur of leasing van een verbonden product, of voor het verlenen van een gerelateerde dienst.

Informatievereisten voor verbonden producten
Bij een verbonden product rust de informatieverplichting op de verkoper, verhuurder, leasegever of fabrikant van het product. Er moet informatie worden gegeven over de volgende zaken:
- Het type productgegevens dat door het verbonden product wordt gegenereerd;
- Het formaat en het geschatte volume van productgegevens, evenals informatie over de mogelijkheid tot continue en realtime generatie van gegevens;
- Waar het verbonden product gegevens kan opslaan en hoe lang deze gegevens worden bewaard;
- Hoe de gebruiker gegevens kan raadplegen, opvragen of wissen. Hierbij hoort ook informatie over de benodigde technische middelen, inclusief gebruikersvoorwaarden en kwaliteitsinformatie van deze middelen.

Informatievereisten voor gerelateerde diensten
Bij een gerelateerde dienst is de leverancier van de dienst verantwoordelijk voor het verstrekken van informatie. Er moet informatie worden gegeven over de volgende zaken:
- De aard van de productgegevens die de gegevenshouder verzamelt, het geschatte volume daarvan en de frequentie van verzameling. Daarnaast moet worden aangegeven welke gegevens door de gerelateerde dienst zelf worden gegenereerd en in welke hoeveelheid;
- Transparantie over het gebruik van gegevens. Dit betreft zowel het verwachte gebruik van eenvoudig beschikbare gegevens door de gegevenshouder zelf als door derde partijen. De identiteit van de gegevenshouder en andere gegevensverwerkende partijen moet daarbij worden verstrekt;
- De beschikbare communicatiemiddelen;

- Hoe de gebruiker gegevens met een derde partij kan delen of dit delen kan stopzetten;
- Het recht van de gebruiker om klachten in te dienen bij de bevoegde autoriteit;
- Eventuele bedrijfsgeheimen die onderdeel zijn van de toegankelijke gegevens en wie daarvan de houder is;
- De duur van de overeenkomst en beëindigingsregelingen, inclusief wat met de gegevens gebeurt bij beëindiging van het contract.

Algemene vereisten
- De te verstrekken informatie moet duidelijk en begrijpelijk zijn, en in een voor Nederlandse gebruikers begrijpelijke taal worden opgesteld.
- Wanneer informatie wijzigt tijdens de levensduur van het verbonden product of de contractperiode van de gerelateerde dienst, moet deze gewijzigde informatie opnieuw aan de gebruiker worden verstrekt.

Thema 2 Toegangsverplichting

De Dataverordening voorziet in een uitgebreid regime voor gebruikerstoegang tot gegevens die worden gegenereerd door een verbonden product of gerelateerde dienst. Toegang kan op twee manieren worden gegeven: via directe toegang (access-by-design) of indirecte toegang op verzoek.

Directe toegang (access-by-design)
De verplichting geldt voor de partij die verantwoordelijkheid draagt voor het ontwerp en de productie van een verbonden product of gerelateerde dienst, doorgaans de fabrikant of ontwerper. Soms zijn dit meerdere partijen.
- De primaire verplichting rust op de fabrikant om een verbonden product en gerelateerde dienst zodanig te ontwerpen dat productgegevens, gegevens van een gerelateerde dienst en bijbehorende metagegevens rechtstreeks toegankelijk zijn voor de gebruiker, voor zover dit relevant en technisch haalbaar is.
- Directe toegang betekent dat de gebruiker de gegevens kan exporteren zonder tussenkomst van andere partijen en beschikt over de technische middelen om dit te doen, ongeacht of gegevens lokaal of op externe servers worden opgeslagen.

De technische haalbaarheid wordt beoordeeld aan de hand van beschikbare technologie, middelen en kennis, waarbij rekening wordt gehouden met factoren zoals ontwikkelingskosten, bescherming van bedrijfsgeheimen en intellectueel eigendom, en beveiligingsvereisten. Met relevant wordt bedoeld dat de fabrikant rekening mag houden met de specifieke omstandigheden en kenmerken van verschillende verbonden producten of gerelateerde diensten.

Indirecte toegang op verzoek
De verplichting rust op de gegevenshouder, zijnde een persoon of organisatie die op basis van een contract het recht of de verplichting heeft gegevens te gebruiken of beschikbaar te stellen. De gegevenshouder mag de gebruiker verifiëren maar niet verder gaan dan nodig. Het verificatieproces verloopt bij voorkeur automatisch, zonder handmatige beoordeling.
- Wanneer directe toegang niet mogelijk of relevant is, moet de gegevenshouder gegevens beschikbaar stellen op verzoek van de gebruiker. Dit geldt zowel voor verzoeken van de gebruiker zelf als voor verzoeken om gegevens te delen met een derde. De gebruiker kan toegang aanvragen via eenvoudige elektronische verzoeken.
- Bij indirecte toegang moet de gegevenshouder de gebruiker onmiddellijk toegang verlenen met dezelfde kwaliteit als waarover hijzelf beschikt over de gegevens. Voor toegang aan een derde partij moet de gegevenshouder met de derde partij voorwaarden en een mogelijke vergoeding

overeenkomen. Een derde partij mag de gegevens uitsluitend gebruiken voor expliciet met de gebruiker overeengekomen doeleinden, niet voor ontwikkeling van concurrerende producten of diensten.

Reikwijdte en kwaliteit van gegevens
Hoewel de Dataverordening verschillende terminologie hanteert voor directe en indirecte toegang, betreft het in beide gevallen hetzelfde type gegevens. In principe moeten alle gegevens die voortkomen uit het gebruik van een verbonden product of gerelateerde dienst beschikbaar worden gesteld. De toegangsverplichting omvat gegevens die niet substantieel zijn gewijzigd, zoals ruwe, bron- of primaire gegevens, alsmede voorbewerkte gegevens die zijn verwerkt om ze begrijpelijk en bruikbaar te maken. Uitgesloten zijn gegevens waarvoor de gegevenshouder aanzienlijke investeringen moet doen om ze bruikbaar te maken.

Wijze van toegangverlening
- Toegang moet gemakkelijk en intuïtief zijn, met een duidelijke en toegankelijke presentatie, zodat de gebruiker zonder technische vaardigheden eenvoudig gegevens kan raadplegen via gebruiksvriendelijke interfaces.
- Toegang moet veilig worden verleend, met passende implementatie van beveiligingsmaatregelen tegen ongeautoriseerde toegang, manipulatie of misbruik.
- Toegang moet kosteloos zijn voor de gebruiker, zowel direct als indirect, zonder verborgen kostenposten.
- Gegevens moeten worden verstrekt in alomvattende, gestructureerde, algemeen gebruikte en machineleesbare formaten. Het formaat moet compleet, logisch gestructureerd, gangbaar binnen Europa, en inleesbaar zijn door dataverwerkingsprogramma's.

Uitzonderingsgronden: beveiligingsrisico's en bedrijfsgeheimen
De Dataverordening kent twee uitzonderingsgronden waarbij het delen van gegevens kan worden geweigerd.

Bij ernstige beveiligingsrisico's die de beveiligingsvereisten van een verbonden product kunnen verzwakken met negatieve gevolgen voor de gezondheid, veiligheid of beveiliging van personen, kunnen de gegevenshouder en gebruiker contractueel afspraken maken om toegang te beperken.

Betreffende bedrijfsgeheimen zoekt de verordening een evenwicht tussen de toegangsverplichting en bescherming van vertrouwelijke informatie. Bedrijfsgeheimen worden alleen bekendgemaakt indien alle noodzakelijke maatregelen worden genomen om de vertrouwelijkheid te waarborgen, met name richting derde partijen. De gegevenshouder moet alle bedrijfsgeheimen identificeren en met de gebruiker of een derde partij maatregelen overeenkomen ter waarborging van de vertrouwelijkheid. In uitzonderlijke gevallen kan toegang worden geweigerd wanneer het delen van bedrijfsgeheimen zeer waarschijnlijk leidt tot ernstige, onherstelbare economische schade. Deze weigering moet uitgebreid worden onderbouwd met objectieve elementen en schriftelijke bewijsvoering aan de gebruiker.

In beide situaties kan de gebruiker klachten indienen bij de ACM, geschilbeslechtingsaanvragen doen bij gecertificeerde organen, of de zaak voorleggen aan de rechter.

Thema 3 — Voorschriften, voorwaarden en overeenkomsten

De Dataverordening richt zich uitgebreid op de contractuele relatie tussen de gegevenshouder en gegevensontvanger. De verordening bevat specifieke voorschriften voor alle betrokken partijen over het toegestane gebruik van gegevens en reguleert welke afspraken partijen onderling mogen maken.

Voorschriften voor gegevenshouders

- De gegevenshouder blijft volledig gebonden aan de AVG. Dit betekent dat persoonsgegevens alleen mogen worden verwerkt op basis van een geldige rechtsgrond.
- De gegevenshouder heeft gebruiksvrijheid, maar mag niet-persoonsgebonden gegevens niet gebruiken om de commerciële positie van de gebruiker of een derde partij te schaden.
- De gegevenshouder mag gegevens alleen aan een derde partij verstrekken voor doeleinden die in de overeenkomst met de gebruiker zijn vastgesteld.
- Technische beschermingsmaatregelen ter voorkoming van ongeoorloofde toegang tot de gegevens zijn toegestaan. Deze maatregelen moeten proportioneel en non-discriminatoir zijn.

Voorschriften voor gebruikers en derde partijen

- Gegevens mogen niet worden gebruikt voor de ontwikkeling van concurrerende verbonden producten.
- Gegevens mogen niet worden gebruikt om inzicht te verkrijgen in de economische situatie van een fabrikant, om druk uit te oefenen voor gegevenstoegang, of om technische beschermingsmaatregelen te wijzigen.

Specifieke voorschriften voor derde partijen

- Een derde partij mag ontvangen gegevens uitsluitend gebruiken voor doeleinden waarvoor de gebruiker toestemming heeft gegeven en binnen de overeengekomen voorwaarden.
- Gegevens moeten worden gewist zodra deze niet langer nodig zijn voor het overeengekomen doel.
- Het gebruik van misleidende ontwerpkeuzes (*dark patterns*) is uitdrukkelijk verboden.
- Het moet voor de gebruiker even gemakkelijk zijn toegang te weigeren of te stoppen als om toegang te verlenen.
- Gebruik van gegevens dat negatieve gevolgen heeft voor de veiligheid van het verbonden product of de gerelateerde dienst is niet toegestaan.
- Beschermingsmaatregelen voor bedrijfsgeheimen moeten worden nageleefd en mogen de vertrouwelijkheid daarvan niet ondermijnen.

Herstelmaatregelen

De Dataverordening voorziet in vergaande herstelmaatregelen bij inbreuken door een derde partij of gegevensontvanger. Deze maatregelen kunnen worden ingeroepen door de gegevenshouder, gebruiker, of houder van een bedrijfsgeheim wanneer sprake is van valse informatie, misleidende middelen, ongeoorloofd gebruik, onrechtmatige gegevensdeling, of niet-naleving van beveiligingsmaatregelen. Herstelmaatregelen omvatten:

- Het wissen van gegeven en kopieën;
- Het staken van productie en handel;
- Het informeren van gebruikers over ongeoorloofd gebruik;
- Het vorderen van een schadevergoeding voor geleden schade.

Voorwaarden voor gegevensdeling met derde partijen

Wanneer de gegevenshouder verplicht is gegevens te delen met een derde partij, moet daarvoor een overeenkomst worden opgesteld met eerlijke, redelijke, niet-discriminerende en transparante voorwaarden (FRAND-normen). Daarnaast stelt de Dataverordening dat bepaalde eenzijdig opgelegde contractuele bepalingen als oneerlijk worden beschouwd en daarom niet bindend zijn. Voorbeelden hiervan zijn exclusieve afspraken (behalve wanneer deze op verzoek van gebruikers worden gemaakt) en informatievereisten die verder gaan dan nodig voor de controle op naleving van contractuele verplichtingen.

Tarieven

De gegevenshouder en gegevensontvanger kunnen een vergoeding overeenkomen voor het beschikbaar stellen van gegevens, waarbij deze vergoeding niet mag worden opgevat als betaling voor de gegevens

zelf. Vergoedingen moeten non-discriminerend en redelijk zijn en kunnen een marge bevatten, gebaseerd op objectieve criteria zoals technische kosten voor het beschikbaar stellen van gegevens en investeringen in gegevensverzameling en -productie. De gegevenshouder moet voldoende gedetailleerde informatie verstrekken over de grondslag voor vergoedingsberekening, zodat de ontvanger kan beoordelen of aan redelijkheidsvereisten is voldaan.

Standaardcontracten
De Europese Commissie ontwikkelt modelcontractvoorwaarden (*Model Contractual Terms* – hierna: MCT's) om partijen te ondersteunen bij de implementatie van de voorschriften. Deze MCT's bieden sjablonen voor eerlijke, redelijke en niet-discriminerende contractuele rechten en plichten, inclusief bescherming van bedrijfsgeheimen.

Er zijn vier verschillende sets beschikbaar:
- Set 1: voor contracten tussen de gegevenshouder en de gebruiker, waarbij de gegevenshouder gegenereerde gegevens wil gebruiken;
- Set 2: voor contracten tussen de gebruiker en de gegevensontvanger, waarbij de gebruiker verzoekt om gegevensdeling;
- Set 3: voor contracten tussen de gegevenshouder en de gegevensontvanger bij verplichte gegevensdeling op verzoek van de gebruiker;
- Set 4: voor vrijwillige gegevensdeling tussen de gegevensdeler en een bedrijf.

Het gebruik van de MCT's is niet verplicht, maar zij bieden praktische ondersteuning voor naleving van de Dataverordening in verschillende typen commerciële relaties.

Inhoudsopgave

1 Inleiding

1. Dit is de Leidraad Data delen van verbonden producten en gerelateerde diensten (hierna: de leidraad). Met deze leidraad verschaft de ACM duidelijkheid aan bedrijven die een verbonden product of gerelateerde dienst aanbieden over de verplichtingen uit de Dataverordening[1] waaraan zij moeten voldoen. Deze leidraad richt zich op de verplichtingen zoals vastgelegd in hoofdstuk 2 en 3 van de Dataverordening. Deze hoofdstukken hebben met name betrekking op het recht op toegang tot en het gebruik van gegevens uit verbonden producten en gerelateerde diensten.

1.1 De Dataverordening

2. Op 12 september 2025 treedt de Dataverordening in werking. De Dataverordening is onderdeel van de Europese datastrategie. Met deze strategie neemt de Europese Unie (hierna: EU) het voortouw in de datagedreven economie en werkt zij aan een interne markt voor data, zodat gegevens vrij kunnen stromen tussen alle sectoren en binnen de gehele EU.[2] Toegang tot gegevens en de mogelijkheid om deze te gebruiken zijn daarvoor essentieel. Dit bevordert innovatie en economische groei.[3]

3. De Dataverordening regelt verschillende zaken om deze doelen te bereiken. Een belangrijk uitgangspunt is dat de gebruiker zeggenschap krijgt over de gegevens die worden verzameld door het gebruik van verbonden producten, ook wel slimme apparaten genoemd.[4] Dit zijn apparaten die verbinding kunnen maken met het internet en gegevens kunnen uitwisselen. Voorbeelden hiervan zijn een slimme thermostaat, een moderne auto of een melkrobot. Vaak kunnen deze apparaten op afstand worden bediend en verzamelen zij, via sensoren, gegevens. Bij het gebruik van een dergelijk product of dienst worden veel gegevens gegenereerd. Op dit moment heeft de gebruiker vaak geen toegang tot deze gegevens en kan hij deze ook niet delen met een derde partij. Meestal heeft alleen de fabrikant, of in sommige gevallen een andere partij, toegang tot de gegevens. De gebruiker is hiervan vaak niet op de hoogte en heeft hier geen controle over. Met de Dataverordening krijgt de gebruiker meer zeggenschap en desgewenst ook toegang tot deze gegevens.

4. Om goed te kunnen begrijpen welke gegevens worden verzameld bij het gebruik van een verbonden product, moet de gebruiker hierover informatie ontvangen wanneer hij een verbonden product koopt, leaset of huurt. Vervolgens moet de gebruiker toegang tot deze gegevens kunnen krijgen. De gegevenshouder – vaak de fabrikant of producent van een verbonden product – is verantwoordelijk voor het verlenen van die toegang. De gebruiker kan de gegevens gebruiken voor bijvoorbeeld eigen analyses, maar kan er ook voor kiezen deze gegevens te delen met een derde. Daarnaast kan hij de fabrikant verzoeken om een derde partij rechtstreeks toegang te geven tot de gegevens die door zijn gebruik van het product zijn gegenereerd.

5. Deze regels gelden niet alleen voor verbonden producten, maar ook voor gerelateerde diensten. Een gerelateerde dienst is een digitale dienst die is gekoppeld aan een verbonden product en waarmee de functionaliteit, het gedrag of de bediening van het verbonden product kan worden beïnvloed.[5]

[1] Verordening (EU) 2023/2854 van het Europees Parlement en de Raad van 13 december 2023 betreffende geharmoniseerde regels inzake eerlijke toegang tot en eerlijk gebruik van data en tot wijziging van Verordening (EU) 2017/2394 en Richtlijn (EU) 2020/1828 (*Dataverordening*).
[2] Europese Commissie, *Europese datastrategie – een Europa dat klaar is voor het digitale tijdperk*, beschikbaar via: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_nl.
[3] Overweging 119 Dataverordening.
[4] Verbonden producten worden ook wel slimme of verbonden apparaten genoemd omdat zij, voor het verzamelen van gegevens, draadloos of via een kabel zijn verbonden met sensoren. Zie voor meer informatie randnummer 42 van deze leidraad.
[5] Zie voor meer informatie randnummer 43 van deze leidraad.

6. De Dataverordening geeft in belangrijke mate invulling aan de wijze waarop deze verplichtingen moeten worden toegepast, bijvoorbeeld om welke typen gegevens het gaat en op welke manier toegang moet worden verleend. Daarnaast bevat de verordening verschillende waarborgen en uitzonderingen om fabrikanten en producenten – ondanks de verplichting om gegevens te delen wanneer de gebruiker daarom verzoekt – toch bescherming te bieden. In deze leidraad licht de ACM deze regels en voorwaarden toe.

7. De Dataverordening bevat ook een lijst met bepalingen over toegang tot en het gebruik van gegevens die als oneerlijk worden beschouwd als deze eenzijdig worden opgelegd door een onderneming. In dat geval worden zij als niet bindend en ongeldig aangemerkt.[6]

8. De Dataverordening geldt vanaf 12 september 2025. Vanaf die datum moet een gegevenshouder voldoen aan de regels uit deze verordening en ervoor zorgen dat de producten die hij verkoopt hiermee in overeenstemming zijn.[7]

9. Naast de hiervoor beschreven verplichtingen zijn er nog andere regels in de Dataverordening. Bijvoorbeeld over het overstappen naar een andere cloudaanbieder en waarborgen tegen onrechtmatige internationale overdracht van gegevens.[8] Daarnaast zijn er ook nog andere wetten die onder de Europese datastrategie vallen, zoals bijvoorbeeld de Datagovernanceverordening,[9] die onder meer regels geeft voor databemiddelingsdiensten zodat mensen kunnen vertrouwen op dergelijke partijen.[10] Al deze regels komen in deze leidraad niet aan bod.

1.2 Het doel van deze leidraad

10. In het wetsvoorstel voor de uitvoering van de Dataverordening, dat bij de Tweede Kamer is ingediend, is de ACM aangewezen als toezichthouder op een groot deel van de Dataverordening en als datacoördinator voor Nederland.[11] Vanuit deze rollen zal de ACM zich inzetten om het delen van gegevens in Nederland te bevorderen. De ACM vindt het belangrijk dat de gebruiker zeggenschap krijgt over zijn of haar gegevens en zich bewust is van de kansen die ontstaan als gegevens worden gedeeld.

11. De ACM hecht veel waarde aan naleving van de Dataverordening. Bij het toezicht op overtredingen kan de ACM overgaan tot handhaving. Handhaving is echter geen doel op zich; het effect van het optreden staat centraal. Dit betekent dat de ACM bij overtredingen van de Dataverordening zal beoordelen welke interventie het meest geschikt is. Bij deze afweging houdt de ACM onder andere rekening met de ernst van de overtreding en de mogelijke schade die daardoor kan ontstaan.

12. Deze leidraad is bedoeld als hulpmiddel voor organisaties bij het voldoen aan de voorschriften uit de Dataverordening. Daarnaast kan de leidraad ook bruikbaar zijn voor consultants, juristen en brancheorganisaties. De toelichting van de ACM bestaat uit het uiteenzetten van de relevante overwegingen van de Dataverordening, het verwijzen naar aanverwante wetgeving en leidraden van de ACM, en het geven van enkele voorbeelden.

[6] Hoofdstuk 4 Dataverordening.
[7] Uitzonderingen op deze regel en het overgangsrecht worden besproken in paragraaf 2.2 van deze leidraad.
[8] Hoofdstuk 6, 7 en 8 Dataverordening.
[9] Verordening (EU) 2022/868 van het Europees Parlement en de Raad van 30 mei 2022 betreffende Europese datagovernance en tot wijziging van Verordening (EU) 2018/1724 (*Datagovernanceverordening*).
[10] Zie voor meer informatie ACM, *Databemiddelingsdiensten*, beschikbaar via: https://www.acm.nl/nl/digitale-economie/data/databemiddelingsdiensten. Zie ook Europese Commissie, *Uitleg over de datagovernanceverordening*, beschikbaar via: https://digital-strategy.ec.europa.eu/nl/policies/data-governance-act-explained.
[11] Wetsvoorstel Uitvoeringswet Dataverordening (verwijzend naar Verordening (EU) 2023/2854), Kamerstuk 36733.

13. Op dit moment is nog weinig officieel gepubliceerd over de interpretatie van de Dataverordening. Ook is nog geen jurisprudentie beschikbaar. Om die reden heeft de ACM zoveel mogelijk aansluiting gezocht bij wat in de verordening zelf wordt beschreven. Daarnaast is voor deze leidraad gebruikgemaakt van het document "*Frequently Asked Questions about the Data Act*" dat door de Europese Commissie is gepubliceerd.[12]

14. Naast de ACM wordt ook de Autoriteit Persoonsgegevens (hierna: AP) belast met het toezicht op een deel van de Dataverordening. Voor elke bepaling is altijd één toezichthouder aangewezen. De ACM en de AP werken in het toezicht nauw samen, bijvoorbeeld door informatie met elkaar te delen en meldingen aan elkaar door te geven. De samenwerking is vastgelegd in formele afspraken.[13] Deze leidraad is geschreven door de ACM[14] en geeft daarom uitsluitend uitleg op de bepalingen waarop de ACM toezicht houdt. De bepalingen waar de AP toezicht op houdt, worden uit oogpunt van volledigheid wel kort besproken, maar de ACM geeft hier geen uitgebreide toelichting op. In de verordening wordt aangegeven wanneer het een bepaling betreft waarop de AP toezicht houdt.

15. Let op: Met deze Leidraad geeft de ACM extra uitleg over de verplichtingen die gelden volgens de Dataverordening. Deze leidraad is een hulpmiddel voor bedrijven die een verbonden product of gerelateerde dienst aanbieden. Het blijft de eigen verantwoordelijkheid van deze organisaties om te voldoen aan de voorschriften uit de Dataverordening en andere wet- en regelgeving. Het is daarbij belangrijk om op te merken dat de Europese data-economie volop in ontwikkeling is. Dit betekent ook dat wet- en regelgeving kan wijzigen na publicatie van deze leidraad, of dat rechterlijke uitspraken de interpretatie van specifieke artikelen kunnen wijzigen. De ACM streeft ernaar om de leidraad na verloop van tijd te actualiseren op basis van ervaringen met het toezicht op de Dataverordening, eventuele wetswijzigingen en rechterlijke uitspraken. Ook internationale afspraken met andere toezichthouders over de interpretatie van de verordening zullen in de leidraad worden verwerkt.

1.3 Voor wie is deze leidraad bedoeld?

16. Deze leidraad is in het bijzonder bedoeld voor organisaties die voorschriften krijgen opgelegd door de Dataverordening. Het gaat om alle organisaties die een verbonden product of gerelateerde dienst in de EU in de handel brengen, of deze leveren aan gebruikers binnen de EU.[15] Dit betreft een brede groep bedrijven, zoals fabrikanten van slimme auto's, leveranciers van een applicatie om deze auto's voor te verwarmen, of verkopers, verhuurders, of leasegevers van dergelijke voertuigen.

17. Deze leidraad is dus niet primair gericht op bedrijven en personen die rechten ontlenen aan de verordening. Uiteraard staat het hen vrij om gebruik te maken van de informatie in deze leidraad. Op de website van de ACM staat uitgebreide informatie over deze rechten en de wijze waarop zij kunnen worden ingeroepen.[16]

1.4 Leeswijzer

18. Deze leidraad volgt niet de volgorde van de artikelen zoals opgenomen in de Dataverordening. De reden daarvoor is dat de opbouw van verplichtingen en rechten in de verordening niet altijd aansluit

[12] Europese Commissie, *Frequently Asked Questions Data Act Version 1.2*, beschikbaar via: https://digital-strategy.ec.europa.eu/en/library/commission-publishes-frequently-asked-questions-about-data-act.
[13] Er wordt op moment van schrijven van deze leidraad gewerkt aan een Samenwerkingsprotocol Dataverordening.
[14] De ACM heeft een conceptversie van deze leidraad afgestemd met AP.
[15] Artikel 1, lid 3 Dataverordening.
[16] Zie ACM, *Data uit slimme apparaten*, beschikbaar via: https://www.acm.nl/nl/digitale-economie/data/data-uit-slimme-apparaten.

bij een praktijkgerichte benadering. Daarom is ervoor gekozen om de hoofdstukken en paragrafen thematisch en logisch te ordenen.

19. Hoofdstuk 2 van deze leidraad biedt algemene informatie over de Dataverordening. Het behandelt de werkingssfeer van de Dataverordening, waaronder op wie de verplichtingen van toepassing zijn en vanaf welk moment deze gelden. Daarnaast worden de belangrijkste rollen in de Dataverordening toegelicht, zoals welke partijen verplicht zijn informatie of toegang te verstrekken. Ook worden de kernbegrippen uit de verordening uitgelegd en wordt de relatie met andere wetgeving besproken.

20. In hoofdstuk 3 worden de diverse informatieverplichtingen behandeld met betrekking tot de verzameling en toegang tot gegevens uit verbonden producten en gerelateerde diensten.

21. Hoofdstuk 4 gaat in op de verplichtingen inzake het verschaffen van toegang tot gegevens uit verbonden producten en gerelateerde diensten. Er wordt uitleg gegeven over de verschillende vormen van toegang, tot welke gegevens toegang moet worden verleend, en op welke wijze de toegang moet plaatsvinden. Ook wordt ingegaan op de uitzondering die van toepassing kunnen zijn.

22. In hoofdstuk 5 komen de contractuele en financiële voorwaarden voor het delen van gegevens aan bod. Er wordt onder meer besproken welke afspraken partijen mogen en moeten maken bij het uitwisselen van gegevens, hoe tarieven voor toegang tot gegevens op een eerlijke wijze kunnen worden vastgesteld, en welke bescherming geldt tegen oneerlijke contractvoorwaarden.

23. Aan het begin van elk hoofdstuk wordt een specifiekere leeswijzer gegeven.

2 Reikwijdte en begrippen

2.1 Inleiding

24. In dit hoofdstuk wordt toegelicht wat de reikwijdte is van de Dataverordening, welke actoren daarin een centrale rol spelen en welke kernbegrippen van belang zijn voor een goed begrip van de wetgeving. In paragraaf 2.2 komt eerst aan bod op wie en wat de verordening van toepassing is, zowel geografisch als materieel. Daarna wordt in paragraaf 2.3 besproken vanaf welk moment partijen moeten voldoen aan de verplichtingen uit de verordening. In paragraaf 2.4 worden de belangrijkste betrokken actoren toegelicht. Paragraaf 2.2.55 bevat de definities die als fundament dienen voor het verdere begrip en de interpretatie van de bepalingen in de verordening. Daarna volgt in paragraaf 2.6 een nadere toelichting op de samenloop tussen de Dataverordening en de Algemene verordening gegevensbescherming (hierna: AVG).[17] Tot slot gaat paragraaf 2.7 kort in op de samenloop met andere relevante wetgeving.

2.2 Voor wie gelden de regels uit de Dataverordening?

25. De Dataverordening is een verordening. Dat betekent dat deze wet algemene toepassing heeft en in al haar onderdelen verbindend en rechtstreeks van toepassing is in alle landen van de EU.[18] De verordening geldt bovendien voor zowel natuurlijke personen als rechtspersonen (zoals bedrijven en organisaties) binnen de EU.[19]

26. Onder bepaalde voorwaarden is de Dataverordening ook van toepassing voor ondernemingen buiten de EU. De verordening heeft daarmee een extraterritoriale werking. Dit wil zeggen dat de wet ook gevolgen heeft buiten de grenzen van de EU. Dit is bijvoorbeeld het geval wanneer een buiten de EU gevestigde onderneming goederen of digitale diensten levert aan gebruikers binnen de EU.[20]

27. Een verbonden product moet voldoen aan de Dataverordening als het "in de EU in de handel wordt gebracht". Dit betekent dat het product voor het eerst op de Europese markt wordt aangeboden.[21] Dit is bijvoorbeeld het geval als het product voor het eerst wordt verkocht in een lidstaat. Een verbonden product wordt slechts één keer in de handel gebracht. Alle daaropvolgende stappen, zoals doorverkoop of distributie, gelden als "op de markt aanbieden".[22]

28. Een gerelateerde dienst valt onder de reikwijdte van de Dataverordening als deze dienst wordt aangeboden in een lidstaat.[23]

29. Het toezicht op de Dataverordening is gebaseerd op het land-van-oorsprongsbeginsel.[24] Dit betekent dat een organisatie die onder de verordening valt, primair onder het toezicht staat van de autoriteit van de lidstaat waar zij is gevestigd.[25] Deze toezichthouder is verantwoordelijk voor het toezicht op de naleving van de verordening, ongeacht in welke andere lidstaten de apparaten of diensten worden aangeboden, of waar de persoon of organisatie die de gegevens opvraagt zich bevindt. Dit beginsel bevordert de rechtszekerheid en voorkomt dubbel toezicht. Tegelijkertijd bestaat er binnen de EU een systeem van samenwerking en informatie-uitwisseling tussen nationale toezichthouders en de

[17] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (*AVG*).
[18] Zie ook Europese Commissie, *Verordening*, beschikbaar via: https://eur-lex.europa.eu/NL/legal-content/glossary/regulation.html.
[19] Artikel 1, lid 3 Dataverordening.
[20] Artikel 1, lid 3 Dataverordening.
[21] Artikel 2, punt 22 Dataverordening.
[22] Artikel 2, punt 21 Dataverordening.
[23] Artikel 1, lid 3, punt a Dataverordening.
[24] Artikel 37, lid 10 Dataverordening.
[25] Zie ook artikel 37, lid 10 t/m 13 Dataverordening.

Europese Commissie, met als doel een consistent toezicht en gelijke toepassing van de regels op de interne markt te waarborgen.

30. Voor micro- en kleine ondernemingen geldt een uitzondering op bepaalde verplichtingen uit de Dataverordening.[26] Zij zijn niet gebonden aan de informatieverplichtingen uit hoofdstuk 3 en de toegangsverplichtingen uit hoofdstuk 4 van deze leidraad. Deze uitzondering is bedoeld om innovatie te stimuleren, zonder kleine of startende ondernemingen te zwaar te belasten. De Dataverordening bevat echter ook algemene bepalingen over oneerlijke contractuele bedingen. Deze regels zijn wél van toepassing op micro- en kleine ondernemingen.

2.3 Vanaf wanneer gelden de regels uit de Dataverordening?

31. De Dataverordening is van toepassing met ingang van 12 september 2025. Vrijwel alle verplichtingen uit de verordening gelden vanaf die datum. Verkopers moeten dus vanaf dat moment voldoen aan de informatieverplichtingen (zie hoofdstuk 3 van deze leidraad) en gegevenshouders moet vanaf dat moment in staat zijn om toegangsverzoeken van gebruikers te honoreren (zie hoofdstuk 4 van deze leidraad).

32. Er geldt een uitzondering voor de directe toegangsverplichting: de verplichting om verbonden producten en gerelateerde diensten op zo'n manier vorm te geven of te maken dat gegevens direct voor de gebruiker op te vragen zijn (de acces-by-design verplichting, zie paragraaf 4.2), is pas van toepassing op verbonden producten en gerelateerde diensten die na 12 september 2026 op de markt worden gebracht.[27]

33. De bepalingen met betrekking tot eenzijdig opgelegde bedingen (zie randnummer 159) zijn van toepassing op overeenkomsten die zijn gesloten na 12 september 2025.[28]

    Met ingang van 12 september 2027 gelden deze bepalingen ook voor overeenkomsten die op of vóór 12 september zijn gesloten mits zij:
    a) van onbepaalde tijd zijn, of
    b) ten minste 10 jaar na 11 januari 2024 aflopen.

2.4 De hoofdrolspelers in de Dataverordening

34. Hieronder volgen een aantal relevante definities uit de Dataverordening ten behoeven van de verdere bespreking van de verplichtingen in de leidraad.

35. **Gebruiker**:[29] De persoon of organisatie die het recht heeft om een verbonden product te gebruiken of die een gerelateerde dienst ontvangt. Een recht tot gebruik van een verbonden product kan ook tijdelijk zijn. De gebruiker kan een consument zijn, maar ook een bedrijf of een overheidsinstantie. Een gebruiker kan eigenaar zijn van het product, maar kan het product ook huren of leasen. In sommige gevallen kunnen meerdere personen hetzelfde product gebruiken, zoals bij het delen van een auto.[30] Een voorbeeld van een gebruiker is een consument die een eigen slimme thermostaat in

[26] Artikel 7 Dataverordening. Zie artikel 2, lid 2 van de bijlage bij Aanbeveling 2003/351/EG voor de definities. U bent een kleine onderneming als uw onderneming minder dan 50 werknemers telt en een omzet genereert van minder dan 10 miljoen euro per jaar en een micro-onderneming als uw onderneming minder dan 10 werknemers telt en een omzet genereert van minder dan 2 miljoen euro per jaar. Bij het tellen van het aantal werknemers of het bepalen van uw omzet moet u ook rekening houden met de omzet en de werknemers bij eventuele andere rechtspersonen in uw groep.
[27] Artikel 50 Dataverordening.
[28] *Idem*.
[29] Artikel 2, punt 12 Dataverordening.
[30] Overweging 18 Dataverordening. Zie ook vraag 16 FAQ Europese Commissie.

huis heeft, een ziekenhuis die eigenaar is van een MRI, of een loonwerker die een slimme tractor huurt.

36. **Gegevenshouder**:[31] De persoon of organisatie die, veelal op basis van een contract, het recht of de verplichting heeft om gegevens te gebruiken of beschikbaar te stellen. Dit is vaak de fabrikant van het verbonden product of een organisatie die een gerelateerde dienst aanbiedt, maar het kan ook een andere partij zijn. De verordening maakt het mogelijk dat fabrikanten de rol van gegevenshouder contractueel overdragen aan een andere partij.[32]

37. **Gegevensontvanger**:[33] Een persoon of organisatie die gegevens ontvangt van een gegevenshouder, handelt voor professionele, niet-privédoeleinden, en geen gebruiker is in de zin van de Dataverordening. Dit kan bijvoorbeeld een organisatie zijn die de gegevens gebruikt voor het ontwikkelen van een gerelateerde dienst, wetenschappelijk onderzoek, of voor het verlenen van adviesdiensten.

38. **Derde partij**: Deze term is niet gedefinieerd in de Dataverordening. De ACM verstaat onder een derde partij een persoon of organisatie die toegang tot gegevens kan krijgen, indien de gebruiker daarvoor kiest. In de meeste gevallen zal een derde partij ook een gegevensontvanger zijn in de zin van de verordening. Een voorbeeld van een derde partij is een serviceverlener zoals een onderhoudsmonteur voor een slimme thermostaat, een energieadviseur of een onderzoeksinstelling.

39. **Datasubject**:[34] een betrokkene zoals bedoeld in artikel 4, punt 1 van de AVG. Dit is een identificeerbaar 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.[35]

40. **Verkoper**: Deze term is niet gedefinieerd in de DA. De ACM sluit voor de interpretatie aan bij het consumentenrecht: een partij die handelt in het kader van zijn handels-, bedrijfs-, ambachts- of beroepsactiviteit.[36] Voor een **leasegever** of **verhuurder** geldt hetzelfde binnen hun respectieve activiteiten.

41. **Houder van een bedrijfsgeheim**:[37] De persoon of organisatie die over bedrijfsgeheimen beschikt.[38] In de context van de Dataverordening kan dit bijvoorbeeld gaan om algoritmes voor data-analyse of machine learning, of de systemen die worden gebruikt om op basis van gegevens uit sensoren te voorspellen wanneer onderhoud nodig is.

[31] Artikel 2, punt 13 Dataverordening.
[32] Voor meer uitleg over de rol van de gegevenshouder, Zie ook vraag 21 FAQ Europese Commissie.
[33] Artikel 2, punt 14 Dataverordening.
[34] Artikel 2, punt 11 Dataverordening.
[35] Artikel 4, punt 1 AVG.
[36] Artikel 2, lid 3 Richtlijn (EU) 2019/771 van het Europees Parlement en de Raad van 20 mei 2019 betreffende bepaalde aspecten van overeenkomsten voor de verkoop van goederen, tot wijziging van Verordening (EU) 2017/2394 en Richtlijn 2009/22/EG, en tot intrekking van Richtlijn 1999/44/EG en artikel 2, lid 2 Richtlijn 2011/83/EU van het Europees Parlement en de Raad van 25 oktober 2011 betreffende consumentenrechten, tot wijziging van Richtlijn 93/13/EEG van de Raad en van Richtlijn 1999/44/EG van het Europees Parlement en de Raad en tot intrekking van Richtlijn 85/577/EEG en van Richtlijn 97/7/EG van het Europees Parlement en de Raad (*EU-richtlijn consumentenkoop*).
[37] Artikel 2, punt 19 Dataverordening. Hierin wordt verwezen naar artikel 2, lid 2 van Richtlijn (EU) 2016/943 van het Europees Parlement en de Raad van 8 juni 2016 betreffende de bescherming van niet-openbaar gemaakte knowhow en bedrijfsinformatie (bedrijfsgeheimen) tegen het onrechtmatig verkrijgen, gebruiken en openbaar maken daarvan (*Richtlijn bedrijfsgeheimen*).
[38] Een bedrijfsgeheim zoals gedefinieerd in artikel 2, lid 1 van de Richtlijn Bedrijfsgeheimen.

2.5 Belangrijkste definities

2.5.1 Slimme apparaten en diensten

42. **Verbonden product**:[39] Een verbonden product wordt gebruikt voor het uitvoeren van een specifieke taak en verkrijgt, genereert of verzamelt daarbij gegevens. Een verbonden product wordt ook wel een slim of verbonden apparaat genoemd, omdat het voor het verzamelen van gegevens draadloos of via een kabel verbonden is met sensoren. Een verbonden product is niet alleen een product dat continu verbonden is, maar ook een product dat ad hoc extern gegevens communiceert (bijvoorbeeld tijdens onderhoud).[40] Voorbeelden van verbonden producten zijn smartphones, digitale camera's, slimme thermostaten of temperatuurregelingen, slimme huishoudelijke apparaten, voertuigen, medische apparatuur en industriële machines.[41] Een verbonden product valt niet onder de definitie in de zin van de Dataverordening als de hoofdfunctie het opslaan, verwerken of doorgeven van gegevens voor een andere partij dan de gebruiker zelf is. Zo kan een server wel als verbonden product worden beschouwd als deze gegevens opslaat, verwerkt of doorgeeft namens de gebruiker, maar niet als de server dit namens derde partijen doet.[42]

43. **Gerelateerde dienst**:[43] Een gerelateerde dienst is een digitale dienst die gekoppeld is aan een verbonden product en waarmee de functionaliteit, het gedrag of de bediening van het verbonden product kan worden beïnvloed. Dit kan bijvoorbeeld een app zijn waarmee een gebruiker de omgevingstemperatuur regelt, of software die de prestaties van een verbonden product optimaliseert. Gerelateerde diensten kunnen gegevens uitwisselen tussen verbonden producten en de dienstverlener. Een digitale dienst die gegevens eenzijdig (uni-directioneel)[44] verzendt, valt niet onder deze definitie.[45] Ondersteunende digitale diensten, zoals onderhouds- en analysediensten, vallen hier ook niet onder.

44. **Virtuele assistent**:[46] Een virtuele assistent is een type gerelateerde dienst. Dit is software die opdrachten, taken of vragen kan verwerken en op basis daarvan toegang biedt tot andere diensten of een verbonden product kan besturen. Een voorbeeld van een virtuele assistent is de boordcomputer in een auto die via een gesproken opdracht, door middel van een smartphone, een tekstbericht naar iemand anders kan versturen. Een virtuele assistent kan ook bijvoorbeeld de omgevingstemperatuur beïnvloeden. Gegevens die door een virtuele assistent zijn geproduceerd en die geen verband houden met het gebruik van een verbonden product of gerelateerde dienst, vallen niet onder de Dataverordening.[47]

2.5.2 Gegevens

45. **Persoonsgegevens**:[48] Dit zijn persoonsgegevens zoals gedefinieerd in artikel 4, punt 1 van de AVG. Dit gaat om alle informatie die een natuurlijke persoon direct of indirect kunnen identificeren, zoals naam, locatiegegevens of een IP-adres.

46. **Bijzondere persoonsgegevens**: Dit zijn persoonsgegevens zoals bedoeld in artikel 9, lid 1 van de AVG. Bijzondere persoonsgegevens zijn gegevens die zó privacygevoelig zijn dat het grote(re) impact op iemand kan hebben als deze gegevens worden verwerkt. Voorbeelden van bijzondere persoonsgegevens zijn persoonsgegevens waaruit iemands ras of etnische afkomst blijkt,

[39] Artikel 2, lid 5 Dataverordening. Voor meer uitleg, zie ook vraag 7 en 8 in FAQ Europese Commissie.
[40] Vraag 7 in FAQ Europese Commissie.
[41] Overweging 14 Dataverordening.
[42] Vraag 7 in FAQ Europese Commissie.
[43] Artikel 2, lid 6 Dataverordening. Voor meer uitleg, zie ook vraag 10 FAQ Europese Commissie.
[44] Dat wil zeggen dat de communicatie of stroom aan gegevens enkel één richting opgaat (van verzender naar ontvanger) Het tegenovergestelde is bi-directioneel, wat tweerichtingsverkeer is en betekent dat de communicatie of stroom aan gegevens in beide richtingen plaatsvindt.
[45] Vraag 10 FAQ Europese Commissie.
[46] Artikel 2, lid 31 Dataverordening. Zie ook overweging 23 Dataverordening.
[47] Artikel 1, lid 4 Dataverordening.
[48] Artikel 2, punt 3 Dataverordening.

biometrische en genetische gegevens, en gegevens over iemands gezondheid en seksuele geaardheid.

47. **Niet persoonsgebonden gegevens**:[49] Gegevens die geen betrekking hebben op een identificeerbare natuurlijke persoon. Dit zijn dus alle andere gegevens, dan persoonsgegevens.

48. **Bedrijfsgeheimen**:[50] Informatie die niet algemeen bekend of gemakkelijk toegankelijk is, vanwege dit geheime karakter een handelswaarde heeft en die wordt beveiligd tegen ongeoorloofde toegang.

49. **Eenvoudig beschikbare gegevens**:[51] Productgegevens en gegevens van een gerelateerde dienst die een gegevenshouder gemakkelijk en rechtmatig krijgt of kan krijgen, zonder dat daar een grote inspanning voor hoeft te worden geleverd.

50. **Gebruikersgegevens**: Gegevens die voortvloeien uit de interactie tussen de gebruiker en een verbonden product of gerelateerde dienst. Deze gebruikersgegevens zijn onder te verdelen in drie soorten:
    1. **Productgegevens**:[52] Ruwe, onbewerkte gegevens die rechtstreeks door het verbonden product worden verzameld door gebruik van het product, de prestaties van het product, of het milieu waarin het product zich bevindt. Productgegevens kunnen door een gebruiker, gegevenshouder of derde partij, waaronder de fabrikant, worden opgevraagd via een elektronische communicatiedienst, fysieke verbinding of toegang tot het product. Beschrijvende gegevens over het product, gebruikshandleidingen en verpakkingsinformatie zijn geen productgegevens.[53]
    2. **Gegevens van een gerelateerde dienst**:[54] Gegevens die worden gegenereerd door de handelingen van de gebruiker met het verbonden product of het verlenen van de gerelateerde dienst zelf.
    3. **Metagegevens**: Gegevens die extra informatie geven over de productgegevens, waardoor de gerelateerde dienst deze correct kan interpreteren en gebruiken.

51. Om het onderscheid tussen de verschillende soorten gegevens te verduidelijken, zijn in tabel 1 ter illustratie voorbeelden opgenomen van de verschillende gegevens, gekoppeld aan de functionaliteiten van een slimme thermostaat of temperatuurregeling.

Tabel 1: Voorbeelden soorten gegevens

Soort gegevens	Geregistreerde gegevens
Persoonsgegevens	• Naam van de gebruiker • Straat, huisnummer en woonplaats • IP-adres van het thuisnetwerk
Niet persoonsgebonden gegevens Bedrijfsgeheime gegevens	• Gemiddelde temperatuur per maand • Beveiligingsinstellingen in de thermostaat of in een app die voorkomen dat een hacker de toegang tot de thermostaat kan overnemen
Productgegevens	• Huidige kamertemperatuur: 21,5°C • Luchtvochtigheid: 45%

[49] Artikel 2, punt 2 Dataverordening.
[50] Artikel 2, punt 18 Dataverordening. Dit zijn bedrijfsgeheimen zoals gedefinieerd in artikel 2, punt 1 van de Richtlijn Bedrijfsgeheimen.
[51] Artikel 2, punt 17 Dataverordening.
[52] Artikel 2, punt 15 Dataverordening.
[53] Vraag 4 in FAQ Europese Commissie.
[54] Artikel 2, punt 16 Dataverordening.

Gegevens van een gerelateerde dienst	• Energieverbruik: 2,3 kWh vandaag • Verwarming aan/uit status: Uit • Schema-instelling: Verwarming aan om 18:00 uur • Koppelstatus met app zoals “Verbonden met smartphone van gebruiker”
Metagegevens	• Locatie van de thermostaat: Woonkamer • Tijdstip van meting: 10 maart 2025, 14:05 • Product-ID: THRM-2025-XYZ123 • Firmware versie van het product: 3.2.1 • Software versie: 09.2.1 • Wifi-signaalsterkte: 78%
Eenvoudig beschikbare gegevens	De gegevens die zijn opgeslagen en zich kenmerken als productgegevens, gegevens van een gerelateerde dienst, en metagegevens.

2.6 Samenloop AVG

52. Bij het gebruik van een verbonden product en een gerelateerde dienst kunnen persoonsgegevens worden verwerkt, zoals een IP-adres. De AVG blijft volledig van toepassing op alle verwerkingen van persoonsgegevens binnen de reikwijdte van de Dataverordening.[55] Ook een gemixte dataset, bestaande uit persoonsgegevens en niet-persoonsgegevens, valt onder de AVG wanneer deze gegevens onlosmakelijk met elkaar verbonden zijn.[56] In sommige gevallen vult de Dataverordening de AVG aan, bijvoorbeeld met bepalingen over de overdraagbaarheid van persoonsgegevens uit verbonden producten of door beperkingen aan te brengen in het hergebruik van persoonsgegevens door derde partijen.[57]

53. De toepasselijkheid van de AVG betekent dat de verwerkingsverantwoordelijke aan de verplichtingen uit die verordening moet voldoen.[58] Zij moet dus, naast de Dataverordening, ook altijd de voorschriften van de AVG naleven wanneer persoonsgegevens worden verwerkt. Bij eventuele tegenstrijdigheden tussen beide wetgevingen heeft de AVG voorrang.[59] De Dataverordening laat de AVG dan ook onverlet: verplichtingen tot het delen van gegevens ontslaan verwerkingsverantwoordelijken niet van hun verplichtingen onder de AVG bij het delen van persoonsgegevens. Evenmin doet de Dataverordening afbreuk aan bestaande AVG-rechten van betrokkenen, zoals het recht op overdraagbaarheid van persoonsgegevens (art. 20 AVG) en het recht op inzage (art. 15 AVG).[60]

54. De Dataverordening erkent de bevoegdheid van de gegevensbeschermingsautoriteiten (zoals de AP in Nederland) om toezicht te houden op de naleving van de AVG en voorziet in een samenhangend handhavings- en samenwerkingsmechanisme tussen deze autoriteiten en andere bevoegde

[55] Artikel 1, lid 5 Dataverordening.
[56] Overweging 34 Dataverordening.
[57] Artikel 1, lid 5 Dataverordening. Zie ook vraag 18 FAQ Europese Commissie en overweging 34 en 35 Dataverordening.
[58] Een verwerkingsverantwoordelijke wordt gedefinieerd in artikel 2, punt 7) van de AVG. Dit 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.
[59] Artikel 1, lid 5 Dataverordening. Daarnaast verwijst artikel 1, lid 5 Dataverordening en overweging 36 Dataverordening naar Verordening (EU) 2018/1725 van het Europees Parlement en de Raad van 23 oktober 2018 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie en betreffende het vrije verkeer van die gegevens, en tot intrekking van Verordening (EG) nr. 45/2001 en Besluit nr. 1247/2002/EG, en naar Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (*Richtlijn betreffende privacy en elektronische communicatie).*
[60] Zie ook overweging 31 en 35 Dataverordening.

instanties.[61] Zo zijn de gegevensbeschermingsautoriteiten ook binnen het kader van de Dataverordening bevoegd om toezicht te houden op de verwerking van persoonsgegevens. Hiermee wordt gewaarborgd dat betrokkenen zich niet tot meerdere instanties hoeven te wenden bij geschillen over hun persoonsgegevens.[62] Deze samenwerking tussen de ACM en AP wordt verankerd in de Uitvoeringswet Dataverordening.[63] De ACM en AP hebben een samenwerkingsprotocol en verdere samenwerkingsafspraken om deze samenwerking te concretiseren.[64] Hierin worden ook afspraken specifiek gericht op het toezicht op de Dataverordening opgenomen.

2.7 Samenloop overige wetgeving

55. De Dataverordening bevat horizontale regels en heeft een breed toepassingsbereik. Daarnaast is de verordening relevant in zowel de context van relaties tussen ondernemingen onderling als tussen ondernemingen en consumenten. Daarom raakt de verordening aan diverse andere Europese en nationale wetgeving. Het zou te ver voeren om in deze leidraad de samenloop met al deze wetgeving in detail te bespreken. Voor een uitgebreidere analyse verwijst de ACM graag naar Memorie van toelichting op de Uitvoeringswet Dataverordening.[65]

56. De verordening bevat algemene regels en bepaalt expliciet dat zij geen afbreuk doet aan, of een aanvulling vormt op, Europees recht op bijvoorbeeld het gebied van intellectueel eigendomsrecht,[66] consumentenrecht[67], en contractenrecht.[68] Daarnaast doet zij ook geen afbreuk aan Europees recht met betrekking tot fysiekontwerp en gegevensvereisten, tenzij de verordening daar uitdrukkelijk in voorziet.[69]

57. Er bestaat substantiële overlap met consumentenwetgeving, die van fundamenteel belang is voor de bescherming van consumenten bij de aankoop en het gebruik van slimme apparaten. Zo legt het consumentenrecht uitgebreide informatieverplichtingen op aan handelaren, waaronder vergaande transparantieverplichtingen over de aard van de verzamelde gegevens en het gebruik daarvan.[70] Deze verplichtingen zijn complementair aan de transparantie- en toegangsvereisten zoals neergelegd in de Dataverordening. Daarnaast bestrijkt het consumentenrecht onderwerpen als eerlijke contractvoorwaarden, bescherming tegen misleidende handelspraktijken, en het verbod op zogenoemde '*dark patterns*' – misleidende ontwerpkeuzes die gebruikers manipuleren om bepaalde handelingen te verrichten of juist te vermijden.[71] De Dataverordening en het consumentenrecht dienen daarom in samenhang te worden toegepast.

[61] De Europese Commissie stimuleert samenwerking tussen handhavingsinstanties via o.a. de Europese Data-innovatie Raad, waarin ook de EDPS (European Data Protection Supervisor) en de EDPB (European Data Protection Board) participeren.
[62] Een betrokkene wordt gedefinieerd in artikel 4, punt 1 van de AVG. Dit is een identificeerbaar 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.
[63] Zie artikel 6 Voorstel van Wet Uitvoeringswet Dataverordening.
[64] Samenwerkingsprotocol tussen Autoriteit Consument en Markt en Autoriteit Persoonsgegevens, Staatcourant 2025, 3534.
[65] Hoofdstuk 5, Memorie van toelichting (Uitvoeringswet Dataverordening), Kamerstuk 36733, nr. 3.
[66] Artikel 1, lid 8 Dataverordening en overweging 13 Dataverordening.
[67] Artikel 1, lid 9 Dataverordening en overweging 9 Dataverordening.
[68] Artikel 1, lid 10 Dataverordening en overweging 9 Dataverordening.
[69] Overweging 11 Dataverordening.
[70] Burgerlijk Wetboek Boek 6, Afdeling 3a.
[71] In overweging 38 Dataverordening, de DSA leidraad en de Leidraad Bescherming online consument van de ACM wordt meer informatie gegeven over '*dark patterns*'. Zie voor de DSA Leidraad, ACM, *Leidraad over Digital Service Act (DSA) voor aanbieder van online diensten*, beschikbaar via: https://www.acm.nl/nl/publicaties/leidraad-over-digital-service-act-dsa-voor-aanbieder-van-online-diensten. Zie voor de Leidraad bescherming online consument ACM, *Leidraad Bescherming online consument*, beschikbaar via: https://www.acm.nl/nl/publicaties/leidraad-bescherming-online-consument.

58. De verordening sluit niet uit dat, op basis van specifieke behoeften van een sector, aanvullende vereisten worden vastgesteld in Europees recht. Echter, deze sectorale vereisten dienen in overeenstemming te zijn met de Dataverordening.

59. Specifieke sectorale vereisten kunnen bijvoorbeeld betrekking hebben op technische eisen voor de toegang tot gegevens, of op beperkingen dan wel uitbreidingen van het recht op toegang tot of gebruik van bepaalde gegevens. Het kan hier bijvoorbeeld gaan om beveiligingsvereisten zoals beschreven in de NIS2-richtlijn[72] of in bijlage I van de Verordening cyberweerbaarheid.[73] Ook sectorale productregelgeving zoals bijvoorbeeld de machineverordening[74] of de verordening voor medische hulpmiddelen[75] kunnen eisen stellen aan het verwerken of beveiligen van gegevens. Daarnaast bestaat er ook andere sectorale wetgeving die raakt aan de uitwisseling van gegevens, die binnen de reikwijdte van de verordening valt. Denk bijvoorbeeld PSD2-richtlijn,[76] de Motorverordening,[77] en de Elektriciteitsrichtlijn.[78]

60. Omdat de Dataverordening geen afbreuk doet aan Europees recht, geldt ook dat de betreffende toezichthouders op Europese wetgeving, of daarop gebaseerde nationale wetgeving, bevoegd blijven voor de respectieve bepalingen uit deze wetgeving. Dit betekent bijvoorbeeld dat bij één en hetzelfde verbonden product of gerelateerde dienst meerdere toezichthouders bevoegd kunnen zijn om toezicht te houden, ieder op verschillende onderdelen daarvan. Zo kan de ACM toezicht houden op consumentenwetgeving en de Dataverordening, de AP op het onderdeel persoonsgegevens, en de Rijksinspectie Digitale Infrastructuur (hierna: RDI), Inspectie Gezondheidszorg en Jeugd (hierna: IGJ) of de Nederlandse Voedsel- en Warenautoriteit (hierna: NVWA) op productveiligheid. De ACM streeft ernaar het toezicht zo goed mogelijk af te stemmen met andere toezichthouders, bijvoorbeeld binnen het Samenwerkingsplatform Digitale Toezichthouders (SDT).[79]

[72] Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (*NIS 2-richtlijn*).
[73] Verordening (EU) 2024/1847 van het Europees Parlement en de Raad van 23 oktober 2024 betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen en tot wijziging van Verordeningen (EU) nr. 168/2013 en (EU) 2019/1020 en Richtlijn (EU) 2020/1828 (*Verordening cyberweerbaarheid*).
[74] Verordening (EU) 2023/1230 van het Europees Parlement en de Raad van 14 juni 2023 betreffende machines en tot intrekking van Richtlijn 2006/42/EG van het Europees Parlement en de Raad en Richtlijn 73/361/EEG van de Raad.
[75] Verordening (EU) 2017/745 van het Europees Parlement en de Raad van 5 april 2017 betreffende medische hulpmiddelen, tot wijziging van Richtlijn 2001/83/EG, Verordening (EG) nr. 178/2002 en Verordening (EG) nr. 1223/2009, en tot intrekking van Richtlijnen 90/385/EEG en 93/42/EEG van de Raad.
[76] Richtlijn (EU) 2015/2366 van het Europees Parlement en de Raad van 25 november 2015 betreffende betalingsdiensten in de interne markt, houdende wijziging van de Richtlijnen 2002/65/EG, 2009/110/EG en 2013/36/EU en Verordening (EU) nr. 1093/2010 en houdende intrekking van Richtlijn 2007/64/EG
[77] Verordening (EU) 2024/1257 van het Europees Parlement en de Raad van 24 april 2024 betreffende de typegoedkeuring van motorvoertuigen en motoren en van systemen, onderdelen en technische eenheden die voor dergelijke voertuigen zijn bestemd, met betrekking tot hun emissies en de duurzaamheid van batterijen (Euro 7), tot wijziging van Verordening (EU) 2018/858 van het Europees Parlement en de Raad en tot intrekking van de Verordeningen (EG) nr. 715/2007 en (EG) nr. 595/2009 van het Europees Parlement en de Raad, Verordeningen (EU) nr. 582/2011, (EU) 2017/1151 en (EU) 2017/2400 van de Commissie en Uitvoeringsverordening (EU) 2022/1362 van de Commissie.
[78] Richtlijn (EU) 2019/944 van het Europees Parlement en de Raad van 5 juni 2019 betreffende gemeenschappelijke regels voor de interne markt voor elektriciteit en tot wijziging van Richtlijn 2012/27/EU (herschikking).
[79] Voor meer informatie over hoe de ACM samenwerkt, zie ACM, *Nationale samenwerking*, beschikbaar via: https://www.acm.nl/nl/over-de-acm/organisatie/samenwerkingen/nationale-samenwerking.

3 Informatieverplichting

3.1 Inleiding

61. In dit hoofdstuk wordt stilgestaan bij de informatieverplichtingen die voortvloeien uit de Dataverordening. Allereerst wordt in paragraaf 3.2 toegelicht wat deze verplichtingen precies inhouden en op welke situaties zij van toepassing zijn. Vervolgens wordt in paragraaf 3.3 nader bekeken welke informatie moet worden verstrekt met betrekking tot een verbonden product. Tot slot komt in paragraf 3.4 aan bod welke gegevens moeten worden verschaft bij het leveren van een gerelateerde dienst.

3.2 Wat houdt de verplichting in?

62. Voordat een overeenkomst wordt gesloten voor de aankoop, huur of leasing van een verbonden product, of voor het verlenen van een gerelateerde dienst, moet de aanbieder hiervan informatie verstrekken aan de gebruiker.[80] Bij een verbonden product is de verkoper, de verhuurder of leasegever van het product degene die verplicht is bepaalde informatie te verstrekken.[81] Dit kan ook de fabrikant zelf zijn. Bij een gerelateerde dienst is de leverancier van de dienst verantwoordelijk voor het verstrekken van de informatie.[82]

63. Als de informatie tijdens de levensduur van het verbonden product of gedurende de contractperiode van de gerelateerde dienst wijzigt, moet die (gewijzigde) informatie opnieuw aan de gebruiker worden verstrekt.

64. De informatie moet op een duidelijke en begrijpelijke wijze worden verstrekt. Dit houdt in dat dat de informatie specifiek, gedetailleerd en niet vaag is. Daarnaast is het van belang dat de informatie is opgesteld in een taal die voor de meeste Nederlandse gebruikers begrijpelijk is. Afhankelijk van het product zal dit doorgaans Nederlands en/of Engels zijn.

65. De informatie kan bijvoorbeeld worden verstrekt via een link op het internet, door opname in een offline of online handleiding, of door middel van een QR-code bij het product of dienst die verwijst naar de relevante informatie. De gebruiker moet de mogelijkheid hebben om de informatie op te slaan, zodat deze in de toekomst toegankelijk blijft om in te zien, te raadplegen, en in ongewijzigde vorm te reproduceren. Welke informatie precies moet worden verstrekt, is afhankelijk van de vraag of het gaat om informatie over een verbonden product of een gerelateerde dienst. Dit wordt toegelicht in de volgende paragrafen.

3.3 Te verschaffen informatie over een verbonden product

66. In onderstaande tabel staat welke informatie aan de gebruiker moet worden verstrekt wanneer het gaat om de aankoop, huur of lease van een verbonden product. Daarbij worden ook voorbeelden gegeven gerelateerd aan een slimme thermostaat.

[80] Deze verplichting staat geformuleerd in artikel 3, lid 2 en 3 Dataverordening. Zie ook overweging 24 en 25 Dataverordening.
[81] Artikel 3, lid 2 Dataverordening.
[82] Artikel 3, lid 2 Dataverordening.

Tabel 2: Overzicht van de vereiste informatie verbonden product

Vereiste informatie	Toelichting	Voorbeelden slimme thermostaat
Type van productgegevens[83]	Het type productgegevens dat door het product wordt gegenereerd	Temperatuurmetingen, aan/uit-status, tijdstip van interacties met product
Formaat van productgegevens[84]	Informatie over de structuur of het formaat waarin de productgegevens worden vastgelegd	Datastructuren, dataformaten vocabularia, classificatieschema's, taxonomieën, codelijsten JSON, XML, CSV, Dublin Core, SKOS, Schema.org, DCAT, etc.
Geraamde volume van productgegevens[85]	De geschatte hoeveelheid productgegevens die wordt gegenereerd	200 MB over dagelijks energieverbruik en 5 MB over gebruikersinstellingen
Mogelijkheid continu en in realtime generatie van gegevens[86]	Of het verbonden product continu (ononderbroken) en in realtime (onmiddellijk) gegevens kan generen	Generatie vindt elke minuut plaats, elk uur, of bij wijziging van temperatuurinstelling
Mogelijkheid opslaan gegevens en bewaringstermijn[87]	Of het verbonden product gegevens op het product zelf of op afstand kan opslaan en hoe lang gegevens worden bewaard	Opslag: Op het product zelf, in de cloud (bijv. in EU-datacenters of in een derde land) Bewaringstermijn: 1 jaar, 6 maanden, totdat de gebruiker de gegevens verwijdert
Mogelijkheid raadplegen, opvragen of wissen van gegevens[88, *a]	Hoe de gebruiker de gegevens kan raadplegen, opvragen of wissen	Vanuit de instellingen van een product kan de gebruiker inzicht en toegang krijgen tot de gegenereerde gegevens en deze zelfstandig gebruiken of delen

Ad a: Hierbij hoort ook de informatie over de technische middelen die nodig zijn om gegevens te raadplegen of te wissen. Denk hierbij aan een API of een software ontwikkelingskit. De gebruikersvoorwaarden en informatie over de kwaliteit van deze middelen moet ook worden verstrekt.[89]

3.4 Te verschaffen informatie over een gerelateerde dienst

67. In onderstaande tabel staat welke informatie aan de gebruiker moet worden verstrekt wanneer het gaat om de verlening van een gerelateerde dienst. Daarbij worden ook voorbeelden gegeven gerelateerd aan een slimme thermostaat.

[83] Artikel 3, lid 2, punt a Dataverordening.
[84] Artikel 3, lid 2, punt a Dataverordening.
[85] Artikel 3, lid 2, punt a Dataverordening.
[86] Artikel 3, lid 2, punt b Dataverordening.
[87] Artikel 3, lid 2, punt c Dataverordening.
[88] Artikel 3, lid 2, punt d Dataverordening.
[89] Overweging 24 Dataverordening.

Tabel 3: Overzicht van de vereiste informatie gerelateerde dienst

Vereiste informatie	Toelichting	Voorbeelden gerelateerde dienst slimme thermostaat
Aard van productgegevens die gegevenshouder verzamelt[90, *a]	Het soort productgegevens waarvan wordt aangenomen dat de potentiële gegevenshouder deze verkrijgt	Dagelijks energieverbruik, buitentemperatuur versus binnentemperatuur, gebruikersinstellingen, handmatige aanpassingen
Geraamde volume van productgegevens die gegevenshouder verzamelt[91, *a]	De geschatte hoeveelheid productgegevens waarvan wordt aangenomen dat de potentiële gegevenshouder deze verkrijgt	200 MB over dagelijks energieverbruik en 5 MB over gebruikersinstellingen
Frequentie van verzameling van productgegevens die gegevenshouder verzamelt[92, *a]	De hoeveelheid productgegevens die wordt verzameld over een bepaalde periode en waarvan wordt aangenomen dat de potentiële gegevenshouder deze verkrijgt	Verzameling vindt elke minuut plaats, elk uur, of bij wijziging van temperatuurinstelling
Aard van gegevens die worden gegeneerd door gerelateerde dienst[93, *a]	Het soort gegevens dat wordt gegenereerd door een gerelateerde dienst	Analyse van verwarmingspatronen, schema's voor wanneer verwarming aan of uit moet
Geraamde volume van gegevens die worden gegenereerd door gerelateerde dienst[94, *a]	De geschatte hoeveelheid gegevens die wordt gegeneerd door een gerelateerde dienst	2 GB over analyse van verwarmingspatronen
Verwacht gebruik eenvoudig beschikbare gegevens door gegevenshouder[95]	Of de potentiële gegevenshouder verwacht eenvoudig beschikbare gegevens te gebruiken en met welke doeleinden	De fabrikant gebruikt de gegevens om het algoritme voor energiebesparing te verbeteren
Verwacht gebruik eenvoudig beschikbare gegevens door derde partijen[96]	Of de potentiële gegevenshouder verwacht derde partijen toe te staan de eenvoudig beschikbare gegevens te gebruiken voor met de gebruiker overeengekomen doeleinden	Gegevens worden ook gedeeld met een energieleverancier indien de gebruiker hiervoor toestemming heeft gegeven
Identiteit van de gegevenshouder en van andere gegevensverwerkende partijen[97, *b]	De identiteit van de potentiële gegevenshouder of andere partijen die de gegevens verwerken. Denk hierbij aan handelsnaam en adres van iedere entiteit die betrokken is bij gegevensverwerking	ThermoSmart Technology B.V., Voorbeeldstraat 123, 1234 AB in Voorbeeldstad

[90] Artikel 3, lid 3, punt a Dataverordening.
[91] Artikel 3, lid 3, punt a Dataverordening.
[92] Artikel 3, lid 3, punt a Dataverordening.
[93] Artikel 3, lid 3, punt b Dataverordening.
[94] Artikel 3, lid 3, punt b Dataverordening.
[95] Artikel 3, lid 3, punt c Dataverordening.
[96] Artikel 3, lid 3, punt c Dataverordening.
[97] Artikel 3, lid 3, punt d Dataverordening.

Communicatiemiddelen voor snelle en efficiënte communicatie[98]	De communicatiemiddelen die de gebruiker kan gebruiken om snel en efficiënt contact op te zoeken met de potentiële gegevenshouder	Klantenservice bereikbaar via e-mail, telefoon en live chat op werkdagen tussen 08:00-18:00
Manier waarop gebruiker gegevens met derde partijen kan delen of het delen kan stopzetten[99]	De wijze waarop de gebruiker kan beginnen met het delen van gegevens met een derde partij, of hiermee kan stoppen	Instellingen in de app bevatten een optie om gegevensdeling aan/uit te zetten; gebruiker kan op elk moment toestemming intrekken om gebruikersgegevens voor hergebruik wel of niet te delen met derde partijen
Recht om klacht in te dienen bij de daarvoor bevoegde autoriteit[100]	De gebruiker kan bij vermoeden van misbruik of schending van zijn of haar rechten onder de Dataverordening een klacht indienen bij de ACM	Disclaimer waarin de gebruiker op zijn of haar rechten wordt gewezen
Gegevens over bedrijfsgeheimen en wie daarvan de houder is[101, *c]	Of een potentiële gegevenshouder houder is van een bedrijfsgeheim die onderdeel is van de gegevens die toegankelijk zijn via het verbonden product of de gerelateerde dienst	Verzamelde algoritmische analyse bevat bedrijfsgevoelige informatie; houder is ThermoSmart Technology B.V.
Duur van de overeenkomst en beëindigingsregelingen[102]	Over de duur van de overeenkomst tussen de gebruiker en potentiële gegevenshouder en over regelingen voor het beëindigen van de overeenkomst	Contract loopt door totdat gebruiker het account opzegt; bij beëindiging van het contract worden gegevens binnen 30 dagen verwijderd, tenzij wettelijk anders vereist

Ad a: Hierbij horen ook de methodes voor de gebruiker om toegang te krijgen tot deze gegevens of deze op te vragen. De methodes van de potentiële gegevenshouder voor gegevensopslag en de termijn van bewaring moeten ook worden verstrekt.[103]
Ad b: Hierbij hoort ook de identiteit van andere gegevensverwerkende partijen.[104]
Ad c: Wanneer een ander dan de potentiële gegevenshouder de houder is van een bedrijfsgeheim in de zin van dit vereiste, dient zijn identiteit te worden vermeld.[105]

[98] Artikel 3, lid 3, punt e Dataverordening.
[99] Artikel 3, lid 3, punt f Dataverordening.
[100] Artikel 3, lid 3, punt g Dataverordening.
[101] Artikel 3, lid 3, punt h Dataverordening.
[102] Artikel 3, lid 3, punt i Dataverordening.
[103] Artikel 3, lid 3, punt b Dataverordening.
[104] Artikel 3, lid 3, punt d Dataverordening.
[105] Artikel 3, lid 3, punt h Dataverordening.

4 Toegang tot gegevens uit een verbonden product of gerelateerde dienst

4.1 Inleiding

68. In dit hoofdstuk staat de toegang tot gegevens centraal. Volgens de Dataverordening moet de gebruiker toegang krijgen tot de gegevens die worden gegenereerd met het gebruik van zijn verbonden product of de gerelateerde dienst. In het algemeen is het de fabrikant die ervoor moet zorgen dat deze gegevens beschikbaar komen. Er zijn twee manieren om deze toegang te regelen: de directe en de indirecte variant.[106]

69. De fabrikant of gegevenshouder kan de gebruiker op directe of indirecte manier toegang geven tot de gegevens die worden gegenereerd met het gebruik van een verbonden product of een gerelateerde dienst. In beginsel moet de fabrikant op directe wijze (ofwel, rechtstreeks) toegang geven.[107] De fabrikant moet het product dan zo ontwerpen dat de gegevens rechtstreeks toegankelijk zijn voor de gebruiker. [108] Dit noemt de ACM de **access-by-design-verplichting**.

70. Er zullen situaties zijn waarin het niet mogelijk of niet logisch is om rechtstreekse toegang te verlenen. Bijvoorbeeld wanneer dit een te grote technische inspanning vergt, of als het ontwerp van het product directe toegang niet toelaat zonder ingrijpende aanpassingen. In dat geval moet de gegevenshouder de toegang zo spoedig mogelijk verlenen via de **indirecte variant**. [109]

71. Indirecte toegang betekent dat de gebruiker de gegevens niet zelf rechtstreeks uit het product of van een website kan verkrijgen, maar een verzoek moet indienen bij de gegevenshouder. Deze moet de gevraagde gegevens dan actief en in begrijpelijke vorm beschikbaar stellen binnen een redelijke termijn. Als de gebruiker geen rechtstreekse toegang heeft, is de gegevenshouder dus verplicht om de gegevens op verzoek te verstrekken. Dit noemt de ACM **indirecte toegang op verzoek**. De gebruiker kan ook verzoeken dat een derde partij, zoals een adviesbureau, toegang krijgt. Beide situaties worden hierna verder toegelicht.

72. De gegevens moeten rechtstreeks toegankelijk zijn voor de gebruiker, voor zover dit **relevant** en **technisch haalbaar** is.[110] Wanneer dit dus niet het geval is, mag gebruik worden gemaakt van de indirecte variant.[111]

73. **Technisch haalbaar** betekent dat het vanuit technisch oogpunt mogelijk is om de toegang te realiseren. Dit houdt in dat de benodigde technologie, middelen en kennis beschikbaar zijn om het product zodanig te ontwikkelen en te implementeren. Het kan voor de fabrikant bijvoorbeeld niet technisch haalbaar zijn:
    1. als de kosten van de benodigde technische aanpassingen onevenredig hoog zijn;
    2. als het beschermen van bedrijfsgeheimen of intellectuele eigendomsrechten daardoor in het geding komt; of
    3. als de beveiliging van het verbonden product of gerelateerde dienst daardoor onvoldoende gewaarborgd kan worden.[112]

[106] De Dataverordening spreekt van rechtstreekse toegang, zie artikel 3, lid 1 en artikel 4, lid 1 Dataverordening.
[107] Deze verplichting staat geformuleerd in artikel 3, lid 1 Dataverordening. Zie ook overweging 20 Dataverordening.
[108] Artikel 3, lid 1 Dataverordening.
[109] Artikel 4, lid 1 Dataverordening.
[110] Artikel 3, lid 1 Dataverordening.
[111] Voor meer uitleg over het onderscheid tussen directe en indirecte toegang, zie ook vraag 22 in FAQ Europese Commissie.
[112] Zie ook vraag 22 in FAQ Europese Commissie.

Bij al deze elementen moet rekening worden gehouden met de huidige stand van de techniek.[113]

74. Met **relevant** wordt bedoeld dat de fabrikant rekening mag houden met de specifieke omstandigheden en kenmerken van verschillende verbonden producten of gerelateerde diensten.[114] De fabrikant kan daarbij ook een afweging maken vanuit het perspectief van de gebruiker. Kort gezegd zullen er situaties zijn waarin het niet voor de hand ligt, niet passend is, of werkbaar is om directe toegang te verlenen tot gegevens uit een verbonden product of gerelateerde dienst.[115]

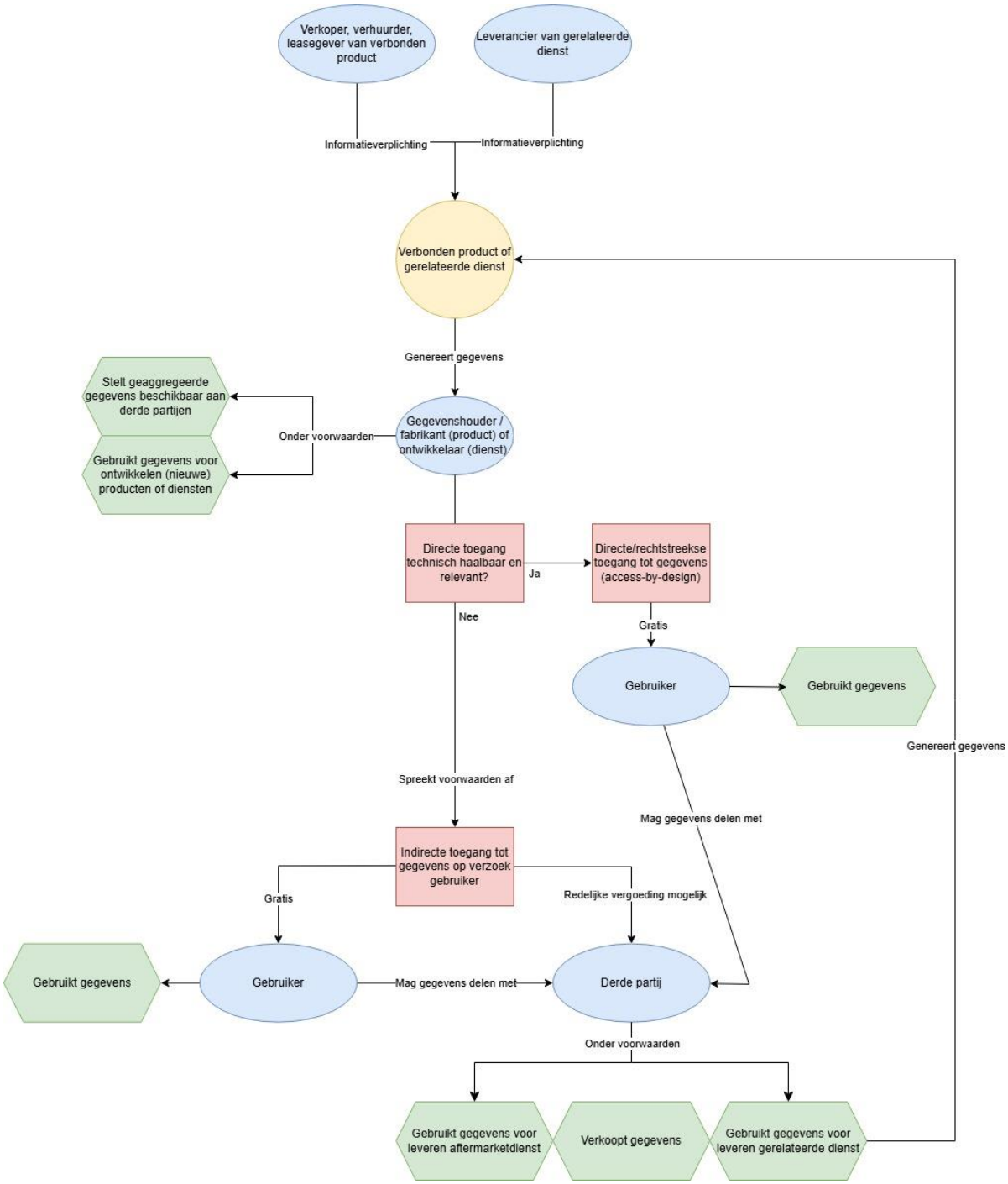
75. Het is aan de fabrikant om zorgvuldig af te wegen of voor zijn product directe of indirecte toegang tot de gegevens het meest passend is. De Europese Commissie geeft in de FAQ aan dat de Dataverordening daarbij enige flexibiliteit biedt, doordat fabrikanten – waar relevant en technisch haalbaar – zelf kunnen beslissen of zij al dan niet ontwerpen voor directe toegang. Tegelijkertijd stimuleert de Dataverordening gegevenshouders om oplossingen te implementeren die het beste bij hen passen wanneer zij moeten voldoen aan de verplichting om gegevens beschikbaar te stellen aan de gebruiker.[116]

76. De keuze voor directe of indirecte toegang heeft invloed op de voorwaarden waaraan de toegang moet voldoen. Beide varianten brengen verschillende verplichtingen met zich mee. Bij de directe variant krijgt de gebruiker rechtstreeks toegang tot de gegevens. De gebruiker kan deze gegevens zelf delen met een derde partij. Bij de indirecte variant kan een gebruiker een verzoek doen aan de gegevenshouder om toegang tot de gegevens te verkrijgen of deze te (laten) delen met een derde partij.

77. Deze en andere voorschriften rondom het verlenen van toegang worden toegelicht in de volgende twee paragrafen. De verhouding tussen deze beide varianten en het bijbehorende proces wordt hieronder ook schematisch weergegeven.

78. Dit hoofdstuk biedt een systematische behandeling van de toegangsregeling voor gegevens onder de Dataverordening. Allereerst worden de twee hoofdvarianten van gegevenstoegang – direct en indirect – uiteengezet in respectievelijk paragraaf 4.2 en 4.3. Hierbij wordt verduidelijkt hoe deze zich tot elkaar verhouden en wanneer welke variant van toepassing is. In paragraaf 4.2 wordt ingegaan op de directe toegang. In paragraaf 4.3 komt de indirecte toegang aan bod, met een onderscheid tussen toegangsverzoeken door de gebruiker zelf en door derde partijen. Deze paragraaf behandelt ook het toepassingsbereik van de verplichting en de eisen voor identiteitsverificatie van verzoekers. Aansluitend wordt in paragaaf 4.4 toegelicht welke gegevens precies onder de regeling vallen en aan welke kwaliteitseisen deze moeten voldoen. De wijze van toegangverlening komt aan bod in paragraaf 4.5, waarin zowel algemene principes als variant-specifieke regels worden besproken. Het hoofdstuk besluit in paragraaf 4.6 met een bespreking van de uitzonderingsgronden, zoals beveiligingsrisico's en bedrijfsgeheimen, gevolgd door een uiteenzetting van de verplichtingen en gedragsregels die gelden voor gebruikers en derde partijen bij toegangverlening.

[113] De term stand der techniek wordt vaak gebruikt om aan te geven wat op een bepaald moment de meest geavanceerde en algemeen geaccepteerde technologie, methode of praktijk is binnen een specifiek vakgebied. Bij producten en systemen verwijst de stand der techniek naar de best beschikbare en breed toegepaste technologieën die op dat moment als norm gelden.
[114] Vraag 17 in FAQ Europese Commissie.
[115] Vraag 22 in FAQ Europese Commissie.
[116] Vraag 17 en vraag 22 in FAQ Commissie.



Figuur 1: schematische weergave van toegang op directe en indirecte wijze. Deze figuur is gebaseerd op de figuur uit de FAQ van de Europese Commissie en geeft alle stappen weer die in dit hoofdstuk worden toegelicht.

4.2 Directe toegang tot gegevens (access-by-design)

4.2.1 Wat houdt de verplichting in?

79. Het verbonden product en de gerelateerde dienst moeten zo worden vormgegeven of gemaakt dat productgegevens, gegevens van een gerelateerde dienst, en bijbehorende metagegevens

rechtstreeks toegankelijk zijn voor de gebruiker, voor zover dit relevant en technisch haalbaar is.[117] Dit noemt de ACM de **access-by-design-verplichting**.

80. Onder rechtstreekse toegang wordt verstaan dat de toegang onmiddellijk en in realtime wordt verleend, zonder dat dit de gebruiker onnodig moeilijk wordt gemaakt. Zo mag de toegang niet onnodig worden bemoeilijkt door de gebruiker te confronteren met allerlei extra handelingen als voorwaarde voor toegang. Er is sprake van rechtstreekse toegang als:
    1. de gebruiker de mogelijkheid heeft om de gegevens zonder tussenkomst van een andere partij uit het verbonden product te exporteren; én
    2. de gebruiker over de technische middelen beschikt om de gegevens uit het verbonden product te exporteren, doordat het verbonden product op deze wijze is ontworpen en vervaardigd. Daarbij maakt het niet uit of de gegevens worden opgeslagen op het verbonden product zelf of op een (externe) server.[118]

81. Meer informatie over hoe toegang moet worden verleend, bijvoorbeeld tot welke gegevens en wat wordt verstaan onder realtime, is te vinden in paragraaf 4.5 en verder.

4.2.2 Voor wie geldt de verplichting?

82. De verplichting geldt voor partijen die de verantwoordelijkheid dragen voor het ontwerp en de productie van het verbonden product of de gerelateerde dienst. In de praktijk betreft dit in de meeste gevallen de fabrikant of ontwerper van het verbonden product.[119] Er kunnen echter ook andere partijen zijn die zeggenschap hebben over het technische ontwerp van het product. In het geval van een gerelateerde dienst is dit vaak de ontwikkelaar.[120]

83. Een verbonden product bevat vaak verschillende onderdelen die gegevens genereren en die niet afkomstig zijn van de fabrikant van het verbonden product zelf. Daarnaast komt het regelmatig voor dat het ontwerp en de assemblage van een verbonden product door verschillende partijen wordt uitgevoerd. Hetzelfde geldt voor de ontwikkeling van een gerelateerde dienst, waarbij vaak meerdere partijen samenwerken aan de ontwikkeling. Deze aspecten ontslaan partijen niet van de toegangsverplichting uit de verordening. In elk individueel geval moet worden vastgesteld welke partij daadwerkelijk controle en invloed heeft op het ontwerp en de productie. Wanneer meerdere partijen in gelijke mate verantwoordelijkheid zijn, kan de access-by-design-verplichting op al deze partijen rusten.[121]

Voorbeeld van directe toegang: een app voor energiebesparing

Een energieleverancier ontwikkelt een applicatie die klanten inzicht geeft in hun gas- en stroomverbruik. De app leest gegevens uit de slimme meter uit en biedt daarnaast de mogelijkheid om te koppelen met andere slimme apparaten, zoals bepaalde typen thermostaten, wasmachines en zonnepanelen. De energieleverancier heeft zelf toegang tot de gegevens in de app, omdat zij de applicatie op deze manier heeft ontworpen.

De energieleverancier is verplicht om de applicatie zodanig te ontwerpen dat de gegevens die worden gegenereerd door het gebruik ervan – de zogenaamde “gegevens van de gerelateerde dienst” – ook rechtstreeks toegankelijk zijn voor de gebruikers.

[117] Artikel 3, lid 1 Dataverordening.
[118] Vraag 22 FAQ Europese Commissie. Zie ook overweging 22 Dataverordening.
[119] Zie ook overweging 20 Dataverordening.
[120] Ter behoeve van de leesbaarheid zal deze groep vanaf nu enkel worden aangeduid als “fabrikanten”.
[121] Vraag 21 FAQ Europese Commissie. Zie ook overweging 20 Dataverordening.

4.3 Indirecte toegang op verzoek

84. Indien de gebruiker geen rechtstreekse toegang heeft, moet de gegevenshouder de gegevens op verzoek van de gebruiker beschikbaar stellen.[122] Dit noemt de ACM **indirecte toegang op verzoek**. De gebruiker kan ook verzoeken dat een derde partij toegang krijgt tot de gegevens. Zo'n derde partij kan bijvoorbeeld een adviesbureau zijn. Beide situaties worden hierna besproken.

4.3.1 Indirecte toegang aan de gebruiker

85. Een gebruiker kan een verzoek indienen om toegang te krijgen tot gegevens. De gegevenshouder stelt deze gegevens dan onmiddellijk beschikbaar. De kwaliteit van de gegevens moet gelijk zijn aan de kwaliteit waarin de gegevenshouder zelf over deze gegevens beschikt.[123]

86. Uitgangspunt is dat de gebruiker dit verzoek eenvoudig elektronisch moet kunnen indienen,[124] bijvoorbeeld via een webportaal[125] of een applicatie die hoort bij het verbonden product.

87. De gegevenshouder moet de gebruiker toegang geven tot de eenvoudig beschikbare gegevens, evenals tot de metagegevens die nodig zijn om deze gegevens te interpreteren en te gebruiken.[126] Nadere toelichting hierover is te vinden in paragraaf 4.4.

88. De toegang tot de gegevens moet, voor zover relevant en technisch haalbaar, continu en in realtime zijn. Dit moet op een gemakkelijke, veilige en voor de gebruiker kosteloze wijze gebeuren. De gegevens moeten beschikbaar worden gesteld in een alomvattende, gestructureerde en algemeen gebruikte en machineleesbaar formaat.[127] Deze aspecten worden verder toegelicht in paragraaf 4.5.

4.3.2 Indirecte toegang aan een derde partij

89. Een gebruiker kan de gegevenshouder verzoeken om gegevens te delen met een derde partij. In dat geval stelt de gegevenshouder de gegevens ter beschikking aan deze derde partij. De toegang moet onmiddellijk worden verleend en de gegevens moeten van dezelfde kwaliteit zijn als waarin de gegevens beschikbaar zijn voor de gegevenshouder zelf.[128]

90. Als een gegevenshouder verplicht is gegevens beschikbaar te stellen aan een derde partij, moet hij met deze derde partij afspraken maken over de voorwaarden waaronder gegevens worden gedeeld, evenals een eventuele vergoeding.[129] Meer informatie hierover wordt gegeven vanaf paragraaf 5.3.

91. De gegevenshouder is niet verplicht gegevens beschikbaar te stellen aan een derde partij als het gaat om het testen van een nieuw verbonden product, of om stoffen of processen die nog niet in de handel zijn gebracht.[130] De uitzondering hierop is als het gebruik door een derde partij contractueel is toegestaan.[131]

92. Een derde partij mag geen poortwachter zijn zoals bedoeld in de Verordening digitale markten (hierna: DMA).[132] Onder de DMA worden de grootste aanbieders van digitale platformen aangewezen als 'poortwachters'.[133] Een partij die als poortwachter is aangewezen, kan geen derde partij zijn zoals

[122] Deze verplichting staat geformuleerd in artikel 4, lid 1 Dataverordening. Zie ook overweging 26 Dataverordening.
[123] Artikel 4, lid 1 Dataverordening.
[124] *Idem*.
[125] Vraag 17 FAQ Europese Commissie.
[126] Artikel 4, lid 1 Dataverordening.
[127] *Idem*.
[128] Artikel 5, lid 1 Dataverordening.
[129] Artikel 5, lid 1 Dataverordening en artikel 8 en 9 Dataverordening.
[130] Artikel 5, lid 2 Dataverordening.
[131] *Idem*.
[132] Verordening (EU) 2022/1925 van het Europees Parlement en de Raad van 14 september 2022 over betwistbare en eerlijke markten in de digitale sector, en tot wijziging van Richtlijnen (EU) 2019/1937 en (EU) 2020/1828 (*Digitalemarktenverordening*)
[133] Voor een actuele lijst van poortwachters, zie Europese Commissie, *Gatekeepers*, beschikbaar via: https://digital-markets-act.ec.europa.eu/gatekeepers_en?prefLang=nl.

bedoeld in dit hoofdstuk van de leidraad. Een poortwachter mag ook geen gegevens ontvangen van de gebruiker, die de gebruiker op een andere wijze heeft gekregen op basis van zijn of haar rechten onder de Dataverordening.[134]

93. De gegevenshouder moet toegang verlenen tot eenvoudig beschikbare gegevens, en ook tot de metagegevens die nodig zijn om die gegevens te interpreteren en te gebruiken.[135] Hierover staat meer toelichting in paragraaf 4.4.

94. Toegang tot de gegevens moet, voor zover relevant en technisch haalbaar, continu en in realtime plaatsvinden. Dit moet op een gemakkelijke, veilige en voor de gebruiker kosteloze wijze gebeuren. De gegevens moeten beschikbaar worden gesteld in een alomvattende, gestructureerde en algemeen gebruikte en machineleesbaar formaat.[136] Deze aspecten worden allemaal toegelicht in paragraaf 4.5.

95. De derde partij mag de gegevens alleen gebruiken voor doeleinden die expliciet met de gebruiker zijn overeengekomen. Daarnaast mag de derde partij de gegevens niet gebruiken voor het ontwikkelen van concurrerende producten of diensten.[137] De verplichtingen van derde partijen die op verzoek van de gebruiker gegevens ontvangen worden nader besproken in paragraaf 5.2

4.3.3 Voor wie geldt de verplichting?

96. De verplichting om gegevens te delen rust op de gegevenshouder. Een gegevenshouder is de persoon of organisatie die, veelal op basis van een contract, het recht of de verplichting heeft om gegevens te gebruiken of beschikbaar te stellen.[138]

4.3.4 Verifiëren van gebruikers door de gegevenshouder

97. De gegevenshouder moet toegang verlenen aan de gebruiker. De gegevenshouders mag een verificatieproces inrichten om te verifiëren of degene die een toegangsverzoek doet, daadwerkelijk gebruiker is van het verbonden product en dus recht heeft op toegang tot de gegevens.[139] Dit proces mag echter niet verder gaan dan strikt noodzakelijk. De gegevenshouder mag niet meer informatie over de gebruiker, zoals loggegevens, bewaren dan nodig is voor de uitvoering van het toegangsverzoek en voor de beveiliging en onderhoud van de data-infrastructuur.[140]

98. De gegevenshouder is vrij om het verificatieproces zelf vorm te geven. Daarbij kan rekening worden gehouden met aspecten zoals:
    - wat het best past bij het soort product;
    - het type gebruiker (bijv. een consument t.o.v. een zakelijke gebruiker);
    - het aantal te verwachten gebruikers (bijv. in het geval van een lift of autoverhuur);
    - het bestaan van verschillende mechanismen om eigenaarschap aan te tonen (bijv. registratie van een auto op naam);
    - de kosten voor het opzetten van verschillende gebruikersaccounts;
    - het gebruiksgemak van een gebruikersaccount voor de gebruiker.[141]

99. Het verificatieproces bestaat bij voorkeur uit een eenvoudig aanvraagmechanisme dat automatisch wordt uitgevoerd, en waarvoor geen beoordeling of goedkeuring van de gegevenshouder nodig is.[142]

[134] Artikel 5, lid 3 Dataverordening.
[135] Artikel 5, lid 1 Dataverordening.
[136] *Idem*.
[137] Zie artikel 6, lid 2, punt e Dataverordening.
[138] Artikel 2, punt 13 Dataverordening. Zie ook randnummer 36.
[139] Artikel 4, lid 5 en artikel 5, lid 4. Zie ook overweging 29 Dataverordening.
[140] Vraag 30 in FAQ Europese Commissie.
[141] *Idem*.
[142] Overweging 21 en vraag 30 FAQ Europese Commissie.

100. Wanneer een verbonden product meerdere gebruikers heeft, ligt het voor de hand dat de gegevenshouder mechanismen implementeert om het verificatieproces per gebruiker toe te passen. Dit kan bijvoorbeeld door het mogelijk te maken om meerdere gebruikersaccounts aan te maken. Deze accounts stellen gebruikers ook in staat om hun rechten op grond van de verordening op individueel niveau te benutten.[143]

101. Persoonsgegevens mogen alleen worden opgevraagd door de verwerkingsverantwoordelijke of door een datasubject.[144] Dat betekent dat alleen degene over wie de gegevens gaan, deze kan opvragen. Voor de verwerking van persoonsgegevens blijft de AVG leidend. Indien door een gebruiker persoonsgegevens worden opgevraagd van een ander datasubject, moet er een geldige rechtsgrond voor de verwerking bestaan op grond van artikel 6 van de AVG, of als gaat om bijzondere categorieën van persoonsgegevens, artikel 9, lid 2 van de AVG. Ook voor het delen van persoonsgegevens met een derde partij is een grondslag vereist. De Dataverordening vormt geen grondslag voor het verwerken van persoonsgegevens die door het gebruik van een verbonden product of een gerelateerde dienst zijn gegenereerd.[145] De AP zal toezicht houden op deze verplichting.

4.4 Tot welke gegevens toegang moet worden verschaft

4.4.1 Welke gegevens: type gegevens, zelfde kwaliteit als voor gegevenshouder

102. Voor de gegevens die ter beschikking moeten worden gesteld, gebruikt de Dataverordening verschillende termen bij directe en indirecte toegang. Bij directe toegang wordt gesproken over "productgegevens en gegevens van een gerelateerde dienst", terwijl bij indirecte toegang de termen "eenvoudig beschikbare gegevens en relevante metagegevens" worden gebruikt. Ondanks dit terminologische verschil gaat de ACM ervan uit dat in beide gevallen hetzelfde type gegevens wordt bedoeld. Voor een uitgebreide toelichting op deze terminologie en bijbehorende voorbeelden wordt verwezen naar paragraaf 2.5.2.

103. In beginsel moeten alle gegevens die voortkomen uit het gebruik van een verbonden product of een gerelateerde dienst beschikbaar worden gesteld. Dit omvat meer dan alleen informatie óf een product is gebruikt. Het gaat om alle gegevens die het gebruik genereert, waaronder:
- Automatisch gegenereerde sensorgegevens
- Gegevens over storingen en afwijkingen
- Gegevens die worden vastgelegd tijdens stand-by of uitgeschakelde toestand[146]

104. De toegangsverplichting heeft betrekking op gegevens die niet substantieel zijn gewijzigd – ook wel ruwe, bron- of primaire gegevens genoemd. Daarnaast vallen ook voorbewerkte gegevens onder de toegangsverplichting als deze zijn verwerkt om ze begrijpelijk en bruikbaar te maken voorafgaand aan verdere verwerking en analyse. Denk hierbij aan sensorgegevens die zijn omgerekend naar fysieke grootheden zoals temperatuur, snelheid of druk, vergezeld van metagegevens, basiscontext en tijdstempels. Niet onder de toegangsverplichting vallen afgeleide gegevens die nieuwe, waardevolle inzichten vertegenwoordigen en die verder gaan dan de aard en reikwijdte van de ruwe of voorbewerkte gegevens. De verordening verduidelijkt dat het hierbij gaat om "informatie die is afgeleid van dergelijke gegevens".[147] Dit is bijvoorbeeld nieuwe informatie die is gegenereerd door aanvullende investeringen, bedrijfseigen algoritmen of andere analytische processen. Dit onderscheid beschermt de innovaties van de gegevenshouder en zorgt er tegelijkertijd voor dat de gebruiker

[143] Vraag 16 FAQ Europese Commissie.
[144] Artikel 4, lid 12 Dataverordening.
[145] Zie overweging 7 Dataverordening.
[146] De definitie van 'direct beschikbare gegevens' verwijst niet naar het tijdstip waarop ze zijn gegeneerd of verzameld. Alleen de gegevens die zijn gegenereerd/verzameld na de inwerkingtreding van de Dataverordening vallen binnen de scope. Zie ook vraag 4 in FAQ Europese Commissie.
[147] Overweging 15 Dataverordening.

toegang behoudt tot de onderliggende gegevens die zijn gegenereerd door het gebruik van het verbonden product of de gerelateerde dienst.[148]

4.5 De wijze van het geven van toegang

105. De verordening geeft diverse aanwijzingen over de manier waarop de toegang aan een gebruiker of een derde partij moet worden verleend. Daarbij wordt onderscheid gemaakt tussen de wijze van toegang: directe toegang (access-by-design) en indirecte toegang (toegang op verzoek). Een aantal vereisten met betrekking tot de wijze van toegang geldt voor beide vormen van toegang. Deze gemeenschappelijke elementen worden eerst toegelicht. Vervolgens worden de specifieke vereisten besproken die uitsluitend van toepassing zijn op directe toegang (access-by-design) of juist op indirecte toegang (toegang op verzoek).

4.5.1 Voor zowel direct (access-by-design) als indirect (toegang op verzoek)

106. Voor alle vormen van toegang tot gegevens geldt dat deze toegang **gemakkelijk en intuïtief** moet zijn, **veilig** moet zijn, en dat de gegevens **kosteloos** toegankelijk moeten zijn. Daarnaast gelden er eisen aan het **formaat** waarin gegevens worden verstrekt.[149] De Dataverordening biedt geen nadere toelichting op deze begrippen. De ACM geeft daarom hieronder een algemene uitleg per term om partijen op weg te helpen met de toepassing hiervan.

107. De toegang tot gegevens moet voor de gebruiker **gemakkelijk en intuïtief** zijn. Dit houdt in dat de gegevens op een duidelijke en toegankelijke manier worden gepresenteerd, zodat de gebruiker – zonder technische vaardigheden – zijn gegevens eenvoudig kan raadplegen en beheren. Dit moet mogelijk zijn met minimale inspanning, bijvoorbeeld door middel van een eenvoudige handeling binnen gebruiksvriendelijke interfaces.

108. De toegang tot gegevens moet **veilig** worden verleend. Dit betekent dat gegevens en metagegevens op een veilige manier toegankelijk zijn voor de geautoriseerde gebruikers en dat zij beschermd worden tegen ongeoorloofde toegang, manipulatie of misbruik. Hiervoor moeten passende beveiligingsmaatregelen worden getroffen en moeten geldende wettelijke normen worden nageleefd.[150] De gebruiker mag door het verkrijgen van toegang tot de gegevens niet worden blootgesteld aan nieuwe risico's. Toegang tot de verbruiksgegevens van slimme verlichting mag er bijvoorbeeld niet toe leiden dat onbevoegden ook toegang krijgen tot de aansturing van die verlichting.

109. Gegevens moeten **kosteloos** toegankelijk zijn voor de gebruiker. Dit betekent dat er geen vergoeding mag worden gevraagd voor het verlenen van toegang. Dit mag niet op directe wijze door een financiële of andere vergoeding te vragen, maar mag ook niet op indirecte wijze door de kosten via andere kostenposten door te berekenen. Een voorbeeld hiervan zou bijvoorbeeld zijn dat een gebruiker enkel toegang krijgt tot zijn gegevens op voorwaarde dat de gegevenshouder deze ook mag delen met andere partijen, of dat er een toeslag wordt toegevoegd aan een offerte.

110. De Dataverordening stelt algemene eisen aan het **formaat** waarin gegevens toegankelijk moeten worden gemaakt. Gegevens moeten worden verstrekt in een **alomvattend**, **gestructureerd**, **algemeen gebruikt** en **machineleesbaar** formaat. Hieronder wordt toegelicht wat hieronder wordt verstaan.

[148] Zie overweging 15 Dataverordening en vraag 5 FAQ Europese commissie.
[149] Artikel 3, lid 1, artikel 4, lid 1 en artikel 5, lid 1 Dataverordening.
[150] Denk bijvoorbeeld aan relevante cyberbeveiligingsvereisten die zijn vastgelegd in Europese cybersecurity certificeringsschema's, zoals het EUCC (European Common Criteria-based cybersecurity certification scheme), gebaseerd op Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 betreffende ENISA (het Agentschap van de Europese Unie voor cyberbeveiliging) (*Cybersecurity Act*).

a) **Alomvattend formaat**: het formaat moet compleet zijn. Dit betekent dat de gegevens in één uniform formaat moeten worden gedeeld, en niet als een combinatie van meerdere datasets in verschillende bestandsformaten.
b) **Gestructureerd formaat**: het formaat moet zodanig zijn dat de gegevens logisch en duidelijk van elkaar te scheiden zijn. De ontvanger moet gericht betekenis kunnen geven aan de gegevens. Het is bijvoorbeeld niet gestructureerd als alle gegevens in één lange rij worden aangeleverd zonder structuur of scheiding.
c) **Algemeen gebruikt formaat**: het formaat moet breed geaccepteerd en gangbaar zijn, in ieder geval binnen Europese context. Voorbeelden van algemeen gebruikte formaten zijn .xls, .xml, .csv of .json. Voor verschillende sectoren en doelgroepen kunnen specifieke formaten gangbaar zijn.
d) **Machineleesbaar formaat**: het formaat moet geschikt zijn voor automatische verwerking door software. Dit betekent dat een dataverwerkingsprogramma de gegevens moet kunnen lezen. Een PDF-formaat is dat bijvoorbeeld niet.

4.5.2 Voor enkel directe toegang

111. Als directe, rechtstreekse toegang tot gegevens wordt verleend, moet deze toegang **standaard** worden verschaft. Met standaard toegang, ook wel toegang *by default* genoemd, wordt bedoeld dat de fabrikant het verbonden product of de gerelateerde dienst zo ontwerpt dat de gebruiker zonder onevenredige inspanning toegang heeft tot de gegevens. De wijze waarop deze standaardtoegang (technisch) wordt gerealiseerd, wordt overgelaten aan de fabrikant.[151] Het gaat er bijvoorbeeld om dat de toegang niet zit verborgen achter meerdere schermen of instellingen, of dat de gebruiker op een andere manier wordt ontmoedigd of verhinderd in het verkrijgen van toegang. In het voorbeeld van een slimme thermostaat kan de gebruiker standaard toegang krijgen tot de gegevens die door het verbonden product worden verzameld via een mobiele app of webportaal.

4.5.3 Voor enkel indirecte toegang

112. Als indirecte toegang wordt verleend, dus toegang op verzoek, moet deze toegang **onmiddellijk**, **continu** en in **realtime** zijn. Ook mag de gegevenshouder het de gebruiker niet **onnodig moeilijk** maken om toegang te verkrijgen. In deze paragraaf worden deze begrippen nader toegelicht.

113. De toegang tot gegevens moet **onmiddellijk** worden verleend. Dit betekent dat de gegevenshouder de gebruiker zonder onnodige vertraging toegang moet geven tot de verzochte gegevens. De gegevenshouder mag het proces niet onnodig vertragen en de gebruiker moet zo snel als mogelijk over de gegevens kunnen beschikken.

114. De toegang zelf moet in beginsel **continu** en **in realtime** zijn. Dit betekent dat een gebruiker niet telkens opnieuw toegang hoeft te vragen, maar op een doorlopende wijze toegang heeft tot de gegevens, zonder onderbrekingen of (onnodige) vertraging. Deze vorm van toegang is echter alleen vereist voor zover dit **relevant** en **technisch haalbaar** is. Wanneer het verbonden product bijvoorbeeld slecht incidenteel gegevens verzamelt, is continue toegang mogelijk niet relevant. Indien de gegevenshouder van mening is dat realtime en continue toegang technisch niet haalbaar is, dient hierover overleg met de gebruiker plaats te vinden. Zie voor nadere toelichting op de begrippen relevant en technisch haalbaar randnummer 72 en verder.

115. De gegevenshouder mag het de gebruiker niet **onnodig moeilijk** maken om zijn keuzes of rechten uit te oefenen op grond van de verordening.[152] Zo is het niet toegestaan om keuzemogelijkheden op een niet-neutrale manier te presenteren, of om de autonomie, besluitvorming of vrije keuze van de gebruiker te ondermijnen of te belemmeren door de structuur, het ontwerp, de

[151] Overweging 22 Dataverordening.
[152] Hiermee worden specifiek de rechten bedoeld die zijn neergelegd in artikel 4 Dataverordening.

functionaliteit of het gebruik van de digitale gebruikersinterface (of een deel daarvan) aan te passen. Het gebruik van zogenaamde '*dark patterns*' (misleidende ontwerpkeuzes die gebruikers manipuleren om bepaalde handelingen te verrichten of juist te vermijden) is daarom eveneens niet toegestaan.[153]

4.6 Uitzonderingsgevallen waarin het is toegestaan om het delen van gegevens te weigeren vanwege beveiligingsrisico's of bedrijfsgeheimen

116. De Dataverordening beschrijft twee situaties waarin het in uitzonderlijke situaties is toegestaan om het delen van gegevens te weigeren: vanwege ernstige beveiligingsrisico's of vanwege bedrijfsgeheimen. Beide uitzonderingen mogen niet lichtvaardig worden ingeroepen en kennen daarom een aantal voorwaarden en waarborgen. Deze worden in de volgende paragraaf beschreven. Op het eind van dit hoofdstuk wordt dit schematisch weergegeven.

4.6.1 Beveiligingsrisico's

117. In bepaalde gevallen kan toegang tot of het delen van gegevens de beveiligingsvereisten van een verbonden product verzwakken, met als gevolg ernstige risico's voor de gezondheid, veiligheid of beveiliging van natuurlijke personen. Het gaat hierbij om beveiligingsvereisten zoals vastgelegd in Europese wetgeving of nationaal recht, bijvoorbeeld de Verordening cyberweerbaarheid,[154] de NIS2-richtlijn[155] of de Cybersecurity Act.[156]

118. In dergelijke situaties kunnen de gebruiker en de gegevenshouder contractueel afspraken maken om de toegang tot gegevens, of het gebruik of het verder delen daarvan, te beperken of verbieden.[157]

119. Als de gegevenshouder en de gebruiker geen overeenstemming bereiken over de toegang tot gegevens, en de gegevenshouder besluit om de toegang te weigeren of beperkingen op te leggen, dan moet hij de ACM hiervan op de hoogte brengen. Vanaf het moment dat de uitvoeringswet in werking treedt, kan deze melding worden gedaan via een speciaal formulier op onze website: www.acm.nl.[158]

120. Als een gebruiker het niet eens is met de weigering om toegang tot gegevens te verlenen, kan hij een aanvraag indienen voor geschilbehandeling bij een gecertificeerd orgaan voor geschilbeslechting. De ACM zal in Nederland, specifiek voor de toepassing van de Dataverordening, dergelijke organen certificeren. Organisaties kunnen hiervoor een aanvraag indienen om gecertificeerd te worden, mits zij voldoen aan de voorwaarden zoals vastgesteld in de Dataverordening. Een actuele lijst van gecertificeerde geschilbeslechtingsorganen in Nederland zal te vinden zijn op www.acm.nl. Daarnaast zal de Europese Commissie op haar website een overzicht publiceren van geschilbeslechtingsorganen in andere lidstaten.[159] Een gebruiker heeft ook het recht om een klacht in

[153] Artikel 6, lid 1 en 2, punt a) Dataverordening en overweging 37 en 38 Dataverordening. In overweging 38 Dataverordening, de DSA leidraad en de Leidraad Bescherming online consument van de ACM wordt meer informatie gegeven over 'dark patterns'. Zie voor de DSA Leidraad, ACM, *Leidraad over Digital Service Act (DSA) voor aanbieder van online diensten*, beschikbaar via: https://www.acm.nl/nl/publicaties/leidraad-over-digital-service-act-dsa-voor-aanbieder-van-online-diensten. Zie voor de Leidraad bescherming online consument ACM, *Leidraad Bescherming online consument*, beschikbaar via: https://www.acm.nl/nl/publicaties/leidraad-bescherming-online-consument.
[154] Verordening (EU) 2024/2847 van het Europees Parlement en de Raad van 23 oktober 2024 betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen en tot wijziging van Verordeningen (EU) nr. 168/2013 en (EU) 2019/1020 en Richtlijn (EU) 2020/1828 (*Verordening cyberweerbaarheid*).
[155] Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gemeenschappelijk niveau van cyberbeveiliging in de hele Unie (*NIS2-richtlijn*).
[156] Cybersecurity Act.
[157] Artikel 4, lid 2 Dataverordening. Zie ook vraag 25 FAQ Europese Commissie.
[158] *Idem*.
[159] De link naar deze pagina is op het moment van schrijven nog onbekend. Wanneer deze bekend is zal de ACM op haar website naar de lijst van de Europese Commissie verwijzen.

te dienen bij de ACM. Tot slot staat het de gebruiker altijd vrij om de zaak voor te leggen aan de rechter.[160]

4.6.2 Bedrijfsgeheimen

121. Het kan voorkomen dat gegevens uit een verbonden product of gerelateerde dienst bedrijfsgeheimen bevatten (zie ook randnummer 48 voor een definitie van bedrijfsgeheimen). In dergelijke gevallen streeft de Dataverordening naar een evenwicht tussen twee belangen: enerzijds de verplichting van de gegevenshouder om gegevens beschikbaar te stellen, en anderzijds de bescherming van diens bedrijfsgeheimen. De verordening bepaalt daarom dat bedrijfsgeheimen enkel bekend worden gemaakt indien alle noodzakelijke maatregelen worden genomen om de vertrouwelijkheid ervan te waarborgen, met name richting derde partijen.[161]

122. Richting derde partijen mogen bedrijfsgeheimen uitsluitend worden gedeeld voor zover dit strikt noodzakelijk is om het tussen de gebruiker en derde partij overeengekomen doel te verwezenlijken.[162]

123. De gegevenshouder is verantwoordelijk voor het identificeren van alle gegevens, inclusief metagegevens, die als bedrijfsgeheim moeten worden aangemerkt. Indien de gegevenshouder niet zelf de houder is van het bedrijfsgeheim, dan moet de feitelijke houder deze identificatie uitvoeren.[163]

124. Op basis van deze identificatie maken de gegevenshouder en de gebruiker of derde partij afspraken over de noodzakelijke maatregelen om de vertrouwelijkheid van de bedrijfsgeheimen te waarborgen. Deze maatregelen kunnen zowel technisch als organisatorisch van aard zijn, zoals het hanteren van modelcontractvoorwaarden, het afsluiten van vertrouwelijkheidsovereenkomsten, het instellen van strikte toegangsprotocollen, het toepassen van technische normen, en de toepassing van gedragscodes.[164]

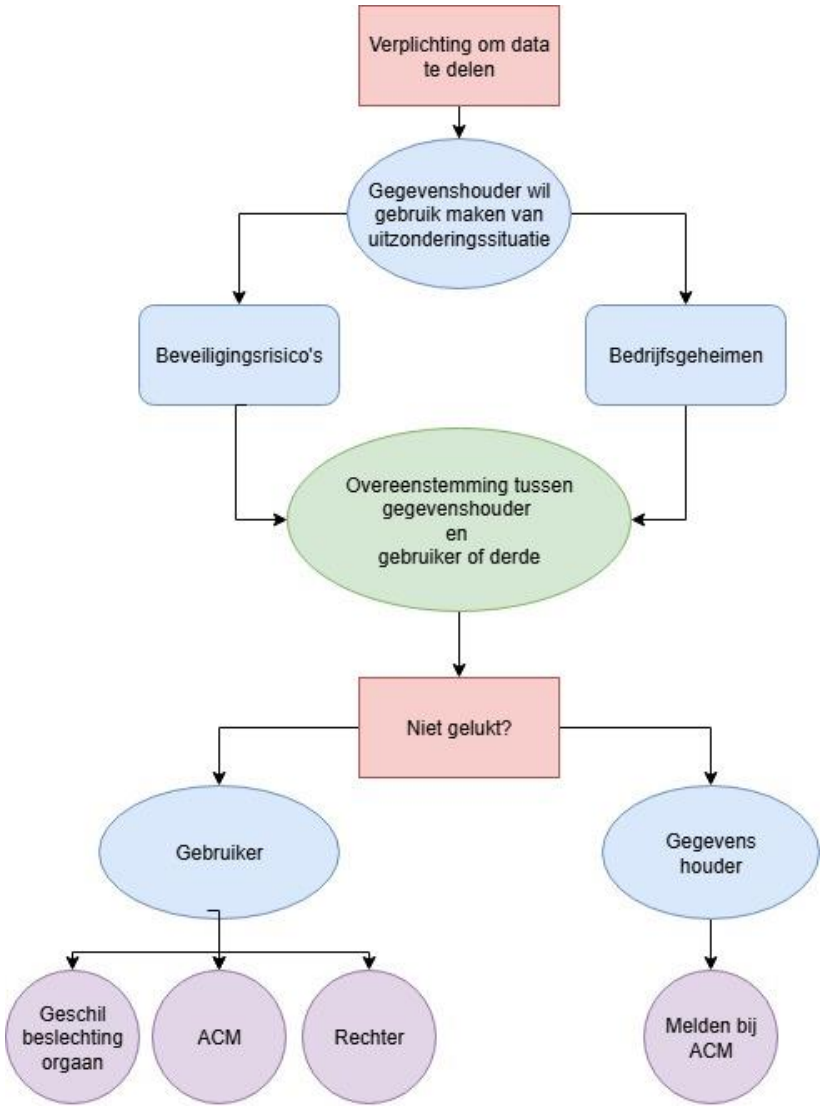
125. Wanneer geen overeenstemming wordt bereikt, de gebruiker of derde partij de afspraken niet nakomt, of de gebruiker de vertrouwelijkheid van bedrijfsgeheimen ondermijnt, dan kan de gegevenshouder het delen van de betreffende gegevens tegenhouden of opschorten. [165] De gegevenshouder moet dit besluit zo snel mogelijk schriftelijk aan de gebruiker mededelen, inclusief een deugdelijke motivering. Tevens moet de ACM hiervan op de hoogte worden gesteld, waarbij wordt vermeld welke maatregelen niet zijn overeengekomen of nageleefd, en welke bedrijfsgeheimen mogelijk zijn gecompromitteerd.

126. In uitzonderlijke gevallen kan de gegevenshouder toegang tot specifieke gegevens weigeren wanneer het delen van bedrijfsgeheimen, ondanks alle genomen maatregelen, zeer waarschijnlijk leidt tot ernstige economische schade.[166] Deze schade moet bestaan uit een serieus en onherstelbaar economisch verlies. De gegevenshouder moet dit risico uitgebreid onderbouwen met objectieve elementen, zoals de afdwingbaarheid van bescherming van bedrijfsgeheimen in derde landen, de aard en het niveau van vertrouwelijkheid van de gevraagde gegevens, en de mate waarin het gaat om een uniek en nieuw verbonden product.

127. Het bewijs moet schriftelijk en zo snel mogelijk aan de gebruiker worden verstrekt, en ook aan de ACM worden gemeld.

[160] Artikel 4, lid 3 Dataverordening.
[161] Artikel 4, lid 6 Dataverordening.
[162] Artikel 5, lid 9 Dataverordening. Zie ook overweging 31 Dataverordening.
[163] Artikel 4, lid 6 en artikel 5, lid 9 Dataverordening.
[164] *Idem*. Overweging 31 Dataverordening.
[165] Artikel 4, lid 7 en artikel 5, lid 10 Dataverordening.
[166] Artikel 4, lid 8 en artikel 5, lid 11 Dataverordening.

128. In beide bovengenoemde situaties, dus bij geen overeenstemming of schending van afspraken, of wanneer de gegevenshouder zich beroept op het risico op ernstige economische schade, heeft de gebruiker het recht om een klacht in te dienen bij de ACM. De ACM zal in dat geval zo spoedig mogelijk beoordelen of en onder welke voorwaarden gegevens alsnog moeten worden gedeeld. De ACM zal hiervoor een aparte klachtenprocedure opzetten, inclusief een klachtenformulier op de website. Daarnaast heeft de gebruiker ook de mogelijkheid om een geschilbeslechtingsaanvraag te doen bij een gecertificeerd geschillenbeslechtingsorgaan onder de Dataverordening, of de zaak voor te leggen bij de rechter.[167]



Figuur 2: Schematische weergave proces rondom het inroepen van uitzonderingen

[167] Artikel 4, lid 9 en artikel 5, lid 12 Dataverordening.

5 Voorschriften, voorwaarden en overeenkomsten

5.1 Inleiding

129. Naast de informatieverplichtingen in de precontractuele fase, zoals uiteengezet in hoofdstuk 3 van deze leidraad, richt de Dataverordening zich ook op de contractuele relatie tussen de gegevenshouder en de gegevensontvanger. De Dataverordening geeft voorschriften voor zowel gegevenshouders, gebruikers als derde partijen, over wat zij wel en niet met (de verkregen) gegevens mogen doen. Ook stelt de Dataverordening regels over wat partijen met elkaar mogen afspreken ten aanzien van het gebruik van gegevens. In dit hoofdstuk geeft de ACM hier uitleg over.

130. Het hoofdstuk opent in paragraaf 5.2 met een toelichting op de specifieke voorschriften voor de gegevenshouder, waarbij wordt ingegaan op zijn verplichtingen bij het verstrekken van gegevens en de waarborgen die hij daarbij moet bieden. In paragraaf 5.3 worden vervolgens de gedragsregels besproken die gelden voor de gebruiker en derde partij, waaronder de beperkingen ten aanzien van het gebruik van verkregen gegevens. Aansluitend komen in paragraaf 5.4 de voorwaarden aan bod voor het delen van gegevens met een derde partij, met bijzondere aandacht voor de extra waarborgen en verantwoordelijkheden die hierbij komen kijken. Paragraaf 5.5 behandelt de tariefstructuur die de gegevenshouder mag hanteren voor toegang tot gegevens. Tot slot wordt in paragraaf 5.6 ingegaan op de standaardcontracten die kunnen worden gebruikt om de wederzijdse rechten en verplichtingen juridisch vast te leggen.

5.2 Voorschriften voor gegevenshouders

131. Zoals uitgelegd in paragraaf 2.6 blijft de AVG volledig van toepassing op alle verwerkingen van persoonsgegevens binnen de reikwijdte van de Dataverordening.[168] Dit betekent dat wanneer een gebruiker persoonsgegevens opvraagt van iemand anders dan zichzelf, of deze wil laten delen met een derde partij,[169] de gegevenshouder deze informatie alleen ter beschikking mag stellen als er een geldige rechtsgrond voor verwerking bestaat op grond van de AVG.[170] De AP zal toezicht houden op deze verplichting.

132. Een gegevenshouder is in principe vrij om eenvoudig beschikbare gegevens die géén persoonsgegevens zijn te gebruiken, mits:

a) Dit is overeengekomen met de gebruiker en het voor de gebruiker duidelijk is dat zijn gegevens gebruikt worden; [171] en
b) hij deze gegevens niet gebruikt om inzichten te verkrijgen over de gebruiker die nadelig kunnen werken voor zijn commerciële positie op de markten waar hij actief is. Dingen die in ieder geval niet mogen worden gebruikt zijn: informatie over de economische situatie van de gebruiker, zijn activa of productiemethoden, of het gebruik van het verbonden product of de gerelateerde dienst door de gebruiker.[172]

133. De gegevenshouder mag eenvoudig beschikbare gegevens eveneens niet gebruiken om inzichten te verkrijgen in de economische situatie, activa, productiemethoden of het gebruik van een verbonden product of gerelateerde dienst door een derde partij, als dat het risico met zich meebrengt dat de commerciële positie van die derde partij wordt verzwakt op de markten waar hij actief is. Dit

[168] Artikel 1, lid 5 Dataverordening.
[169] Artikel 5, lid 7 Dataverordening. Zie ook overweging 35 Dataverordening.
[170] Artikel 4, lid 12 Dataverordening en overweging 34 Dataverordening. De rechtsgronden voor verwerking staan in artikel 6 AVG. Daarnaast verwijst artikel 4, lid 12 Dataverordening naar artikel 9 van de AVG en artikel 5, lid 3 van de Richtlijn betreffende privacy en elektronische communicatie.
[171] Artikel 4, lid 13 Dataverordening.
[172] Artikel 4, lid 13 Dataverordening.

mag alleen als de derde partij daarvoor duidelijk toestemming heeft gegeven én op elk moment op een eenvoudige manier die toestemming kan intrekken.[173]

134. De gegevenshouder mag niet-persoonsgebonden productgegevens niet beschikbaar stellen aan een derde partij voor andere doeleinden dan welke in de overeenkomst met de gebruiker zijn vastgelegd.[174]

135. Als één of meerdere derde partijen toegang krijgen tot niet-persoonsgebonden productgegevens van een gegevenshouder, dan moet de gegevenshouder in het contract duidelijk vastleggen dat deze derde partijen de gegevens niet verder mogen doorgeven aan anderen.[175]

136. De gegevenshouder kan technische beschermingsmaatregelen implementeren, zoals het gebruik van slimme contracten en encryptie voor authenticatie- en autorisatiedoeleinden, om ongeoorloofde toegang tot gegevens en metagegevens te voorkomen en om ervoor te zorgen dat alle partijen zich houden aan de wettelijke verplichtingen op grond van de Dataverordening en de overeengekomen contractvoorwaarden.[176]

137. Deze maatregelen moeten proportioneel en non-discriminatoir zijn: de gegevenshouder mag geen onderscheid maken tussen verschillende gegevensontvangers en mag de fundamentele rechten van de gebruiker niet belemmeren. Dit betekent dat de gebruiker nog steeds onbelemmerd toegang moet hebben tot zijn gegevens, een kopie daarvan moet kunnen verkrijgen, de gegevens moet kunnen gebruiken of raadplegen, en deze conform de wettelijke bepalingen aan een derde partij moet kunnen verstrekken. Ook de rechten van een derde partij op grond van Europese wetgeving of nationale wetgeving die overeenkomstig het Europees recht is vastgesteld, moeten volledig worden gerespecteerd.[177]

5.3 Voorschriften voor gebruikers en derde partijen

5.3.1 Voorschriften voor gebruikers en derde partijen

138. De gebruiker of derde partij die toegang heeft gekregen tot gegevens door middel van een verzoek op grond van de Dataverordening, mag deze gegevens niet gebruiken om een verbonden product te ontwikkelen dat concurreert met het verbonden product waarvan de gegevens afkomstig zijn.[178] Het is hen ook niet toegestaan om met dit doel gegevens te delen met een andere derde partij. De vraag of een verbonden product concurreert met het verbonden product waar de gegevens vandaan komen hangt af van of ze concurreren op dezelfde productmarkt.[179]

139. Let op: dit verbod geldt uitdrukkelijk niet voor het ontwikkelen van een gerelateerde dienst die mogelijk concurreert met die van de gegevenshouder. Het stimuleren van innovatie op *aftermarkets* is immers een expliciet doel van de Dataverordening.[180] Ook maakt de verordening duidelijk dat het gebruik van de gegevens voor reverse engineering is toegestaan, zolang wordt voldaan aan de regels in de verordening en in Europese of nationale wetgeving. Denk hierbij aan reparatiedoeleinden, de verlenging van de levensduur van een verbonden product, of de verlening van *aftermarketdiensten*.[181]

[173] Artikel 5, lid 6 Dataverordening.
[174] Artikel 4, lid 14 Dataverordening.
[175] Artikel 4, lid 14 Dataverordening.
[176] Artikel 11, lid 1 Dataverordening. Zie ook overweging 57 Dataverordening.
[177] Artikel 11, lid 1 Dataverordening. Zie ook overweging 57 Dataverordening.
[178] Artikel 4, lid 10 en 6, lid 2, punt e Dataverordening.
[179] Zie ook overweging 32 Dataverordening. De relevante productmarkt moet worden gedefinieerd aan de hand van de gevestigde beginselen van het mededingingsrecht van de EU.
[180] Overweging 32 Dataverordening. Zie ook vraag 26 FAQ Europese Commissie.
[181] Overweging 25 Dataverordening.

140. Daarnaast is het voor de gebruiker en derde partij niet toegestaan om de gegevens te gebruiken om inzicht te krijgen in de economische situatie, activa, productiemethoden of het gebruik door, de fabrikant of gegevenshouder.[182]

141. Een gebruiker of derde partij mag geen druk uitoefenen of misbruik maken van zwakke plekken in de techniek die een gegevenshouder gebruikt om gegevens te beveiligen, om zo toegang te krijgen tot die gegevens.[183]

142. In randnummer 136 en 137 staat beschreven dat de gegevenshouder technische beschermingsmaatregelen mag implementeren om ongeoorloofde toegang tot gegevens en metagegevens te voorkomen en om ervoor te zorgen dat alle partijen zich houden aan de wettelijke verplichtingen op grond van de Dataverordening en de overeengekomen contractvoorwaarden. De gebruiker, derde partij of andere gegevensontvanger mag deze technische beschermingsmaatregelen niet wijzigen of verwijderen zonder expliciete toestemming van de gegevenshouder.[184]

5.3.2 Specifieke voorschriften voor enkel derde partijen

143. Een derde partij mag de ontvangen gegevens uitsluitend gebruiken voor het doel waarvoor de gebruiker toestemming heeft gegeven, en binnen de voorwaarden die met de gebruiker zijn overeengekomen. Vanzelfsprekend moet de derde partij zich daarbij ook houden aan Europese en nationale wetgeving over gegevensbescherming, zoals voorgeschreven in de AVG. De gegevens moeten worden gewist zodra ze niet langer nodig zijn voor het overeengekomen doel, tenzij anders is afgesproken in het geval van niet-persoonsgegevens.[185]

144. Het moet voor de gebruiker even gemakkelijk zijn om toegang van de derde partij tot de gegevens te weigeren of stop te zetten als het voor de gebruiker is om toegang te verlenen.[186] De derde partij mag het de gebruiker niet onnodig moeilijk maken om zijn keuzes of rechten uit te oefenen op basis van de verordening.[187] Zo is het niet toegestaan om keuzemogelijkheden op een niet-neutrale manier te presenteren, of om de autonomie, besluitvorming of vrije keuze van de gebruiker te ondermijnen of te belemmeren door de structuur, het ontwerp, de functionaliteit of het gebruik van de digitale gebruikersinterface (of een deel daarvan) aan te passen. Het gebruik van *'dark patterns*' (misleidende ontwerpkeuzes die gebruikers manipuleren om bepaalde handelingen te verrichten of juist te vermijden) is daarom eveneens niet toegestaan.[188]

145. De derde partij mag de ontvangen gegevens niet gebruiken om personen te profileren. De AP zal toezicht houden op deze verplichting. Met profilering wordt elke vorm van geautomatiseerde verwerking van persoonsgegevens bedoeld, waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd.[189] Profilering mag wel indien

[182] Artikel 4, lid 10 Dataverordening.
[183] Artikel 4, lid 11 en artikel 5, lid 5 Dataverordening.
[184] Artikel 11, lid 1 Dataverordening. Zie ook overweging 57 Dataverordening. Deze bepaling creëert zo een evenwicht tussen de beveiligingsbehoeften van gegevenshouders en de toegangsrechten van gebruikers en derde partijen, waarbij technische innovatie wordt aangemoedigd zonder de doelstellingen van de Dataverordening te ondermijnen.
[185] Artikel 6, lid 1 Dataverordening. Zie ook overweging 38 en 39 Dataverordening. De verplichting om gegevens te verwijderen zodra ze niet meer nodig zijn voor het afgesproken doel met de gebruiker – tenzij er iets anders is afgesproken voor niet-persoonsgegevens – komt bovenop het recht van de betrokkene om zijn of haar gegevens te laten wissen volgens artikel 17 van de AVG.
[186] Overweging 38 Dataverordening.
[187] Hiermee worden specifiek de rechten bedoeld die zijn neergelegd in artikel 5 en 6 Dataverordening.
[188] Artikel 6, lid 1 en 2, punt a Dataverordening en overweging 37 en 38 Dataverordening. In overweging 38 Dataverordening, de DSA leidraad en de Leidraad Bescherming online consument van de ACM wordt meer informatie gegeven over '*dark patterns*'. Zie voor de DSA Leidraad, ACM, *Leidraad over Digital Service Act (DSA) voor aanbieder van online diensten*, beschikbaar via: https://www.acm.nl/nl/publicaties/leidraad-over-digital-service-act-dsa-voor-aanbieder-van-online-diensten. Zie voor de Leidraad bescherming online consument ACM, *Leidraad Bescherming online consument*, beschikbaar via: https://www.acm.nl/nl/publicaties/leidraad-bescherming-online-consument.
[189] Artikel 2, punt 20 Dataverordening. Zie ook artikel 4, punt 4 AVG.

dergelijke verwerkingsactiviteiten strikt noodzakelijk zijn om de door de gebruiker gevraagde dienst te verlenen. Dit kan bijvoorbeeld het geval zijn in de context van geautomatiseerde besluitvorming.[190]

146. De derde partij mag de ontvangen gegevens niet doorgeven aan een andere derde partij, tenzij dat gebeurt op basis van een overeenkomst met de gebruiker. Daarbij geldt wel dat die andere partij alle noodzakelijke maatregelen moet nemen, zoals afgesproken tussen de gegevenshouder en de derde partij, om de vertrouwelijkheid van bedrijfsgeheimen te beschermen.[191]

147. De derde partij mag de ontvangen gegevens niet doorgeven aan bedrijven die zijn aangemerkt als poortwachter zoals bedoeld in de DMA. Zie ook randnummer 92 voor meer toelichting.[192]

148. De derde partij mag de ontvangen gegevens niet gebruiken als dat negatieve gevolgen heeft voor de veiligheid van een verbonden product of de gerelateerde dienst. Hierbij kan worden gedacht aan het manipuleren van software-updates voor een slimme thermostaat, waardoor oververhitting kan ontstaan, of het verstoren van communicatie tussen een verbonden auto en zijn sensoren, wat kan leiden tot ongelukken.[193]

149. In lijn met datgene wat besproken is in randnummer 124 en 125, wordt van de derde partij verwacht dat zij de specifieke maatregelen naleeft die met de gegevenshouder of de houder van een bedrijfsgeheim zijn overeengekomen. De derde partij wordt bovendien expliciet verboden de vertrouwelijkheid van bedrijfsgeheimen te ondermijnen.[194]

150. De derde partij die gegevens ontvangt, mag de consument niet hinderen om de gegevens met een andere partij te delen.[195]

5.3.3 Herstelmaatregelen

151. De Dataverordening voorziet in vergaande herstelmaatregelen wanneer de derde partij of gegevensontvanger inbreuk maakt op zijn verplichtingen op grond van de verordening. Deze maatregelen kunnen worden ingeroepen door de gegevenshouder, gebruiker, of houder van het bedrijfsgeheim, in de situatie dat een derde partij of gegevensontvanger:

1. om gegevens te verkrijgen, valse informatie aan de gegevenshouder heeft gegeven, misleidende middelen heeft ingezet, of druk heeft uitgeoefend of misbruik heeft gemaakt van zwakke plekken in de techniek die een gegevenshouder gebruikt om de gegevens te beschermen;[196]
2. de ter beschikking gestelde gegevens heeft gebruikt voor ongeoorloofde doeleinden, zoals het ontwikkelen van een concurrerend verbonden product;[197]
3. gegevens onrechtmatig heeft gedeeld met een andere partij;[198]
4. de technische en organisatorische beveiligingsmaatregelen die zijn overeengekomen met de gegevenshouder of de houder van het bedrijfsgeheim niet heeft nageleefd;[199]
5. de technische beschermingsmaatregelen die zijn genomen door een gegevenshouder zonder toestemming van de gegevenshouder heeft geschrapt of gewijzigd.[200]

[190] Artikel 6, lid 2, punt b Dataverordening en overweging 39 Dataverordening. Zie in dit kader ook artikel 2, lid 2, punten a en c van de AVG.
[191] Artikel 6, lid 2, punt c Dataverordening.
[192] Artikel 6, lid 2, punt d Dataverordening.
[193] Artikel 6, lid 2, punt f Dataverordening.
[194] Artikel 6, lid 2, punt g Dataverordening.
[195] Artikel 6, lid 2, punt h Dataverordening.
[196] Artikel 11, lid 3, punt a Dataverordening. Dit verbod wordt aan de derde partij opgelegd in artikel 5, lid 5 Dataverordening en staat verder uitgewerkt in randnummer 141.
[197] Dit verbod blijkt onder andere uit artikel 6, lid 2, punt e Dataverordening en staat verder uitgewerkt in randnummer 95.
[198] Artikel 11, lid 3, punt c Dataverordening.
[199] Dit vereiste staat uitgewerkt in artikel 5, lid 9 Dataverordening en staat verder uitgewerkt in randnummer 124.
[200] Dit vereiste staat uitgewerkt in artikel 11, lid 1 Dataverordening en staat verder uitgewerkt in randnummer 142.

152. Wanneer zich dergelijke inbreuken voordoen, moet de derde partij of gegevensontvanger zo snel mogelijk gehoor geven aan verzoeken van de gegevenshouder, gebruiker, of houder van het bedrijfsgeheim om:
    1. De gegevens die door de gegevenshouder ter beschikking zijn gesteld en kopieën daarvan, te wissen;[201]
    2. In geval van een significant risico dat het onrechtmatige gebruik van de gegevens ernstige schade berokkent aan de gegevenshouder, de gebruiker of de houder van het bedrijfsgeheim, of wanneer een dergelijke maatregel niet onevenredig is in het licht van hun belangen, de volgende maatregelen te nemen:
        a) een einde te maken aan het produceren, aanbieden, in de handel brengen of gebruiken van goederen, of afgeleide gegevens of diensten die zijn geproduceerd op basis van de verkregen gegevens;
        b) het invoeren, uitvoeren of opslaan van inbreukmakende goederen met het oog op de hierboven bedoelde gebruik te staken, en deze goederen te vernietigen;[202]
    3. De gebruiker te informeren over het ongeoorloofd gebruik of de ongeoorloofde openbaarmaking van de gegevens, en over de maatregelen die zijn genomen om dit gebruik of deze openbaarmaking te stoppen;[203]
    4. De partij die schade heeft geleden door het misbruik of de openbaarmaking van de onrechtmatig geraadpleegde of gebruikte gegevens schadeloos te stellen.[204]

153. Deze herstelbepalingen gelden ook:
    1. Wanneer de gebruiker zelf de technische beveiligingsmaatregelen van een gegevenshouder ter bescherming van bedrijfsgeheimen heeft gewijzigd of verwijderd;
    2. Wanneer de gebruiker de technische en organisatorische beveiligingsmaatregelen die zijn overeengekomen met de gegevenshouder of de houder van het bedrijfsgeheim niet heeft nageleefd;
    3. Voor iedere andere partij die gegevens heeft ontvangen van een gebruiker als gevolg van een inbreuk op de Dataverordening.[205]

154. De Dataverordening bepaalt daarnaast dat wanneer een gegevensontvanger inbreuk maakt op de verplichtingen omschreven in randnummer 144 en 145, de gebruiker dezelfde herstelbepalingen mag eisen als de gegevenshouder, zoals deze omschreven zijn in randnummer 152.[206]

5.4 Voorwaarden bij delen van gegevens met een derde partij

155. Als een gegevenshouder op grond van de Dataverordening, of op basis van andere nationale of Europese wetgeving, verplicht is om gegevens te delen met een derde partij, moet daarvoor een overeenkomst worden opgesteld.[207] In deze overeenkomst worden afspraken vastgelegd over de voorwaarden en regelingen die gelden voor het delen van de gegevens. In lijn met het beginsel van contractsvrijheid staat het partijen vrij om te onderhandelen over de precieze voorwaarden voor het beschikbaar stellen van gegevens.[208] Wel moeten deze afspraken eerlijk, redelijk, niet-discriminerend en transparant zijn.[209]

156. De termen ‘eerlijk, redelijk, niet-discriminerend en transparant’ zijn brede, open normen. Vaak worden dit ook de FRAND-normen genoemd, verwijzend naar de Engelse termen ‘*Fair, Reasonable*

[201] Artikel 11, lid 2, punt a Dataverordening.
[202] Artikel 11, lid 2, punt b Dataverordening.
[203] Artikel 11, lid 2, punt c Dataverordening.
[204] Artikel 11, lid 2, punt d Dataverordening.
[205] Artikel 11, lid 4 Dataverordening.
[206] Artikel 11, lid 5 Dataverordening.
[207] Artikel 8, lid 1 Dataverordening.
[208] Overweging 43 Dataverordening.
[209] Artikel 8, lid 1 Dataverordening.

and Non-Discriminatory'. Deze normen komen vaker voor wanneer het gaat om de regulering van toegang, bijvoorbeeld in de regulering van telecommunicatienetwerken, maar ook in de context van bijvoorbeeld technologieën en industriestandaarden.[210] Omdat het open normen zijn, verschilt de precieze invulling van geval tot geval. Het is aan partijen zelf om hier een juiste afweging in te maken. Vervolgens kan dit getoetst worden door de toezichthouder, geschilbeslechtingsorganen en/of de rechter. Hierna volgt een algemene uitleg per term.

- **Eerlijkheid**: Contractvoorwaarden die sterk afwijken van gangbare handelspraktijken en in strijd zijn met de beginselen van goede trouw en eerlijke behandeling, worden als oneerlijk beschouwd.
- **Redelijkheid**: Contractuele bepalingen dienen gebalanceerd te zijn. De partij die de bepalingen heeft opgesteld, moet kunnen aantonen dat deze niet eenzijdig zijn opgelegd en niet onredelijk zijn. Dit is vooral van belang om oneerlijke handelspraktijken te voorkomen en een eerlijke verdeling van de waarde van gegevens binnen de Europese data-economie te waarborgen.
- **Non-discriminatie**: Bedrijven en gebruikers moeten gelijk worden behandeld als het gaat om toegang tot en gebruik van gegevens. Dit omvat het voorkomen van oneerlijke contractuele voorwaarden die door grote of sterke partijen aan kleine of zwakke partijen worden opgelegd, wat kan leiden tot discriminatie.

157. De verordening geeft ook zelf nog wat extra invulling ten aanzien van het vereiste van non-discriminatie. De verordening maakt duidelijk dat een gegevenshouder, met betrekking tot de regelingen voor het delen van gegevens, geen onderscheid mag maken tussen vergelijkbare categorieën gegevensontvangers, ongeacht of gegevensontvangers grote ondernemingen zijn of niet. Of een gegevensontvanger in een vergelijkbare categorie valt zal verschillen van geval tot geval en vraagt om een specifieke analyse.[211] Er is geen sprake van onrechtmatige discriminatie wanneer een gegevenshouder verschillende contractvoorwaarden gebruikt om gegevens beschikbaar te stellen, indien die verschillen om objectieve redenen gerechtvaardigd zijn.[212]

158. Een gegevensontvanger die van mening is dat de voorwaarden voor het beschikbaar stellen van gegevens discriminerend zijn, kan een gemotiveerd verzoek indienen bij de gegevenshouder. In dat geval moet de gegevenshouder zo snel mogelijk informatie verschaffen waaruit blijkt dat geen sprake is van discriminatie.[213]

159. De Dataverordening noemt een aantal bepalingen die niet in contracten mogen voorkomen, omdat deze als oneerlijk worden beschouwd.[214] Deze bepalingen worden dan ook niet als bindend erkend.[215] Het gaat in ieder geval om contractuele bepalingen die de rechten van de gebruiker op grond van de Dataverordening uitsluiten of beperken.[216] Daarnaast introduceert de verordening, voor contractuele bedingen die eenzijdig worden opgelegd,[217] een systematiek waarbij onderscheid wordt gemaakt tussen bepalingen die altijd als oneerlijk worden beschouwd en bepalingen die vermoed worden oneerlijk te zijn – vergelijkbaar met de grijze en zwarte lijst uit het consumentenrecht.[218] Een voorbeeld van een bepaling die altijd als oneerlijk wordt aangemerkt, is wanneer de partij die het beding eenzijdig heeft opgelegd haar aansprakelijkheid uitsluit of beperkt in het geval van opzettelijke

[210] Zie in de context van een standaard-essentieel octrooi bijvoorbeeld het toonaangevende arrest CJEU, C-170/13, ECLI:EU:C:2015:477 (Huawei Technologies Co. Ltd tegen ZTE Corp. en ZTE Deutschland GmbH).
[211] Zie ook vraag 38 FAQ Europese Commissie.
[212] Overweging 45 Dataverordening.
[213] Artikel 8, lid 3 Dataverordening.
[214] Artikel 8, lid 2 Dataverordening.
[215] *Idem.*
[216] *Idem.*
[217] Overweging 59 Dataverordening legt uit wanneer een contractvoorwaarde als eenzijdig opgelegd kan worden beschouwd: "Het gaat om situaties waarin een partij een bepaalde contractvoorwaarde voorstelt en de andere onderneming geen invloed kan uitoefenen op de inhoud van die voorwaarde, ondanks een poging om erover te onderhandelen. Een contractvoorwaarde die door één partij is voorgesteld en door de andere onderneming is aanvaard, of een contractvoorwaarde waarover is onderhandeld en die vervolgens in gewijzigde vorm tussen de contractpartijen is overeengekomen, mag niet worden geacht eenzijdig te zijn opgelegd."
[218] Dit is hoofdstuk IV van de Dataverordening. Voor meer uitleg over hoofdstuk IV, zie ook overweging 58 t/m 62 Dataverordening.

handeling of grove nalatigheid.[219] Een voorbeeld van een bepaling die vermoed wordt oneerlijk te zijn, is wanneer de partij aan wie het beding is opgelegd, wordt belet de overeenkomst binnen een redelijke termijn op te zeggen.[220]

160. Een gegevenshouder mag geen exclusieve afspraken maken met een specifieke gegevensontvanger, behalve als dit verzocht is door de gebruiker op grond van de verordening.[221]

161. Zowel de gegevenshouder als de gegevensontvanger hoeft geen informatie te verstrekken die verder gaat dan wat nodig is om te controleren of zij voldoet aan de contractuele voorwaarden voor het beschikbaar stellen van gegevens, of aan andere verplichtingen die volgen uit de Dataverordening of Europese of nationale wetgeving.[222]

5.5 Tarieven

162. De gegevenshouder en gegevensontvanger kunnen onderling afspraken maken over een vergoeding voor het beschikbaar stellen van gegevens.[223] De vergoeding mag niet discriminerend zijn en moet redelijk zijn. Daarnaast mag de vergoeding een marge bevatten.[224] De Dataverordening stelt geen minimum- of maximumbedrag vast voor de vergoeding. In het algemeen geldt dat de vergoedingen af kunnen hangen van de omvang, het formaat en de aard van de gegevens. Dit kan dus per geval verschillen.[225] De Dataverordening maakt wel duidelijk dat de vergoeding moet worden vastgesteld op basis van een aantal objectieve criteria.[226]

163. Bij het overeenkomen van de vergoedingen moet hoofzakelijk rekening worden gehouden met:
1. De (technische) kosten voor het beschikbaar stellen van gegevens, waaronder, met name, de kosten voor de formattering van gegevens, elektronische verspreiding en opslag.
2. De investeringen in het verzamelen en produceren van gegevens. Hierbij moet ook worden meegenomen in hoeverre andere partijen hebben bijgedragen aan het verkrijgen, genereren of verzamelen van de betreffende gegevens.[227]

164. De vergoeding mag niet worden opgevat als een betaling voor de gegevens zelf.[228] De vergoeding is bedoeld voor het goedmaken van technische kosten, zoals kosten die nodig zijn voor de reproductie, elektronische verspreiding en opslag, maar niet voor het verzamelen en produceren van gegevens. Het gaat hierbij dus om de kosten die gemaakt worden voor het beschikbaar stellen van gegevens. Hieronder kunnen ook de kosten vallen voor het formatteren van gegevens en de kosten voor het faciliteren van concrete verzoeken.[229]

165. De kosten voor het beschikbaar stellen van gegevens kunnen variëren afhankelijk van de omvang van de gegevens en de regelingen die worden getroffen om deze beschikbaar te stellen. Bij regelmatige of herhaalde transacties binnen een zakelijke relatie kunnen de kosten dalen wanneer hierover langetermijnafspraken worden gemaakt, bijvoorbeeld via een abonnementsmodel of het

[219] Artikel 13, lid 4, punt a Dataverordening.
[220] Artikel 13, lid 5, punt d Dataverordening.
[221] Artikel 8, lid 4 Dataverordening.
[222] Artikel 8, lid 5 Dataverordening.
[223] Overweging 48 Dataverordening benadrukt dat ingrijpen niet nodig is bij gegevensdeling tussen grote ondernemingen, of wanneer een kleine of middelgrote onderneming de gegevenshouder is en een grote onderneming de gegevensontvanger, aangezien zij geacht worden in staat te zijn om binnen redelijke en niet-discriminerende grenzen over een vergoeding te onderhandelen.
[224] Artikel 9, lid 1 Dataverordening.
[225] Artikel 9, lid 3 Dataverordening.
[226] Vraag 38 FAQ Europese Commissie. Daarnaast wordt nog opgemerkt dat artikel 9, lid 6 Dataverordening duidelijk maakt dat de Dataverordening niet belet dat ander Europees recht of overeenkomstig het Europese recht vastgestelde nationale wetgeving, een vergoeding voor het beschikbaar stellen van gegevens uitsluit of voorziet in een lagere vergoeding.
[227] Artikel 9, lid 2 Dataverordening.
[228] Overweging 46 Dataverordening.
[229] Overweging 47 Dataverordening.

gebruik van slimme contracten. Kosten die niet specifiek worden gemaakt voor één verzoek, mogen niet worden toegerekend aan een enkele gegevensontvanger.[230]

166. De vergoeding mag ook een marge bevatten. Deze marge kan variëren afhankelijk van het volume, het formaat of de aard van de gegevens. Ook kan de marge afhangen van de hoogte van de investeringen die zijn gedaan voor de gegevensverzameling. Als een gegevenshouder de gegevens heeft verzameld op basis van aanzienlijke investeringen ten behoeve van zijn eigen activiteiten, kan een hogere marge gerechtvaardigd zijn. Zijn de investeringen daarentegen beperkt, dan zal ook de marge lager moeten uitvallen. In sommige gevallen kan de marge beperkt zijn of zelfs geheel zijn uitgesloten, bijvoorbeeld wanneer het gebruik van de gegevens door de gegevensontvanger geen invloed heeft op de eigen activiteiten van de gegevenshouder. Het is aan de gegevenshouder om hierin een zorgvuldige afweging te maken.[231]

167. Micro- en kleine ondernemingen[232] of onderzoeksorganisaties zonder winstoogmerk komen voor een lagere vergoeding in aanmerking als gegevensontvanger. In dat geval mogen alleen de kosten hierboven onder 1 worden meegenomen. Het mag hier uitsluitend gaan om kosten die rechtstreeks verband houden met de kosten die aan individuele verzoeken kunnen worden toegeschreven, met dien verstande dat de gegevenshouder permanent de nodige technische interfaces of bijbehorende software en connectiviteit zal moeten opzetten.[233] De gegevensontvanger met partnerondernemingen of verbonden ondernemingen die niet als micro- of kleine ondernemingen kunnen worden aangemerkt, is niet voor deze uitzondering in aanmerking.[234]

168. De gegevenshouder moet de gegevensontvanger voldoende gedetailleerde informatie geven over de grondslag voor de berekening van de vergoeding, zodat deze kan beoordelen of aan de vereisten van een redelijke vergoeding is voldaan. In het geval dat de gegevensontvanger een micro- of kleine onderneming, of een onderzoeksorganisatie zonder winstoogmerk is, moet uit die informatie ook blijken dat de vergoeding niet hoger is dan de kosten die rechtstreeks verband houden met het beschikbaar stellen van de gegevens aan de ontvanger en kunnen worden toegeschreven aan het individuele verzoek.[235]

169. De Europese Commissie zal richtsnoeren vaststellen voor de berekening van een redelijke vergoeding, waarmee invulling wordt gegeven aan de meer algemene voorschriften in de verordening.[236]

5.6 Standaardcontracten

170. De Europese Commissie gaat modelcontractvoorwaarden, de zogenoemde *"Model Contractual Terms"* (hierna: MCT of MCT's), ontwikkelen en aanbevelen om partijen te helpen bovenstaande voorschriften te implementeren.[237] De Europese Commissie heeft aangegeven de sets te publiceren in alle officiële EU-talen.

[230] *Idem*.
[231] *Idem*.
[232] Voor een uitleg van wanneer een bedrijf een micro- of kleine onderneming is, zie voetnoot 26.
[233] Overweging 49 Dataverordening.
[234] Artikel 9, lid 4 Dataverordening.
[235] Artikel 9, lid 7 Dataverordening en overweging 51 Dataverordening.
[236] Artikel 9, lid 5 Dataverordening. Deze richtsnoeren zijn op het moment van schrijven nog niet gepubliceerd. De ACM kan nu dus alleen informatie geven over de voorschriften die in de verordening staan genoemd, maar de verdere invulling zal duidelijk moeten worden vanuit de nog te verschijnen richtsnoeren.
[237] Artikel 41 Dataverordening. Naast de MCT's heeft de Europese Commissie ook standaard contractuele clausules, de zogenoemde standard contractual clauses (hierna: SCC's) ontwikkeld die als kader kunnen dienen voor de contractuele relatie tussen zakelijke klanten en aanbieders van dataverwerkingsdiensten (clouddiensten). Omdat de SCC's niet gericht zijn op het delen van data, vallen ze buiten de scope van deze Leidraad.

171. De MCT's bieden sjablonen en richtlijnen en zijn ontwikkeld om eerlijke, redelijke en niet-discriminerende contractuele rechten en plichten te waarborgen, waaronder de bescherming van bedrijfsgeheimen. Partijen kunnen de MCT's in onderling overleg gebruiken om een overeenkomst inzake de aankoop, huur of leasing van een verbonden product, of levering van een gerelateerde dienst, in lijn te brengen met de Dataverordening.

172. De MCT's kunnen door de fabrikant van een verbonden product en gerelateerde dienst worden gebruikt bij het opstellen van contracten met een zakelijke gebruiker, maar kunnen ook van toepassing zijn in de contractuele relatie met een gebruiker die consument is. In dat geval moeten de MCT's worden aangepast om in lijn te zijn met de regels voor consumentenbescherming. Het gebruik van de MCT's is niet verplicht volgens de Dataverordening.[238]

173. De MCT's zijn op een modulaire manier opgesteld, wat betekent dat partijen ervoor kunnen kiezen om de hele set of slechts bepaalde onderdelen te gebruiken. De partijen kunnen ervoor kiezen om de MCT's als unieke basis van hun overeenkomsten te hanteren, of om ze in te voegen in de eigen vooraf opgestelde contractuele kaders die zij gewoonlijk gebruiken. Naast de bepalingen heeft de Europese Commissie ook instructies en uitleg gegeven over welke MCT's aandacht verdienen bij aanpassingen en integratie in contracten. Bij sommige bepalingen heeft de Europese Commissie meerdere versies van dezelfde bepaling ontwikkeld, zodat deze toepasbaar is in verschillende typen commerciële relaties.

174. Vier verschillende sets van de MCT's worden beschikbaar, die in verschillende type commerciële relaties kunnen worden toegepast:

- *Set 1: Gegevenshouder – Gebruiker*
  Deze set van MCT's is ontworpen voor contracten tussen een gegevenshouder en een gebruiker van een verbonden product of gerelateerde dienst, waarbij de gegevenshouder gegevens wil gebruiken die zijn gegenereerd met behulp van het product of de dienst.

- *Set 2: Gebruiker - Gegevensontvanger*
  Deze set van MCT's is ontworpen voor contracten tussen een gebruiker van een verbonden product of gerelateerde dienst en een gegevensontvanger, waarbij de gebruiker een gegevenshouder verzoekt om gegevens beschikbaar te stellen aan de gegevensontvanger op basis van artikel 5 van de Dataverordening.

- *Set 3: Gegevenshouder - Gegevensontvanger*
  Deze set van MCT's is ontworpen voor contracten tussen een gegevenshouder en een gegevensontvanger, waarbij een gegevenshouder op grond van de Dataverordening verplicht is om gegevens beschikbaar te stellen aan een gegevensontvanger wanneer daarom wordt gevraagd door een gebruiker van het verbonden product of gerelateerde dienst.[239] Dezelfde set kan, met aanpassingen, worden gebruikt als het delen van gegevens verplicht is op basis van andere Europese of nationale wetgeving.

- *Set 4: 'Vrijwillig' delen van gegevens tussen een gegevensdeler en een bedrijf.*
  Deze set van MCT's is ontworpen voor contracten tussen gegevensdelers en gegevensontvangers, waarbij de gegevensdeler vrijwillig en onafhankelijk van enig verzoek van een gebruiker of soortgelijke partij, gegevens beschikbaar stelt aan een gegevensontvanger. De vrijwilligheid betekent in deze context dat de contractuele relatie niet ontstaat door een aanvraag van een gebruiker, maar op basis van een commercieel belang tussen de gegevensdeler en gegevensontvanger. In deze set van MCT's heeft de Europese Commissie ervoor gekozen om af

[238] Annex I tot en met IV van de "Final Report of the Expert Group on B2B Data Sharing and Cloud Contracts" (2 April 2025).
[239] Dit gaat dus om een verzoek zoals beschreven in artikel 5 Dataverordening.

te wijken van de definities van partijen in de Dataverordening en de term ‘gegevensdeler’ te gebruiken om alle mogelijke scenario’s te kunnen opnemen.