Besluit inzake vergunningaanvraag voor de verwerking van CWT B.V. volgens het Protocol Incidentenwaarschuwingssysteem Veilig Vrachtvervoer

1. Inleiding

CWT Commodity Logistics Rotterdam B.V. (hierna: Aanvrager) heeft ingevolge artikel 33, vierde lid, aanhef en onder c, van de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG) – bij de Autoriteit Persoonsgegevens (AP) een vergunningaanvraag ingediend. Deze aanvraag is bij de AP bekend onder het zaaknummer 2026-028045 en is onderdeel van de vergunningen voor Gebruikers van het Protocol Incidentenwaarschuwingssysteem Veilig Vrachtvervoer. Op het moment van indienen van deze vergunningaanvraag bestond er nog geen goedgekeurd Protocol op basis waarvan een vergunning kon worden afgegeven.

In artikel 10 van de Algemene verordening gegevensbescherming (AVG) is bepaald dat persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen op grond van artikel 6, eerste lid, AVG alleen worden verwerkt onder toezicht van de overheid of indien de verwerking is toegestaan bij Unierechtelijke of lidstaatrechtelijke bepalingen die passende waarborgen voor de rechten en vrijheden van betrokkene bieden. De wetgever heeft van deze ruimte gebruik gemaakt in artikel, 33, vierde lid, aanhef en onder c van de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG). Op grond hiervan mogen persoonsgegevens van strafrechtelijke aard ten behoeve van derden worden verwerkt indien de AP een vergunning voor de verwerking heeft verleend. Ingevolge artikel 33, vijfde lid, UAVG kan een vergunning slechts worden verleend, indien de verwerking noodzakelijk is met het oog op een zwaarwegend belang van derden en bij de uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad. Aan de vergunning kunnen door de AP voorschriften worden verbonden.

In het hiernavolgende besluit wordt geconcludeerd dat de AP een vergunning verleent onder de voorschriften opgenomen onder paragraaf 7.

2. Procedureverloop

Op 21 augustus 2026 heeft de AP tevens de vergunningaanvraag van Aanvrager ontvangen.

3. Feitelijke weergave verwerking

Uit het Protocol volgt de volgende feitelijke weergave van de verwerking van persoonsgegevens (woorden met een hoofdletter zijn in het Protocol gedefinieerd en voor de duidelijkheid hieronder opgenomen):[1]

[1] Pagina 4-5 van het Protocol.

De verwerking wordt in het Protocol als volgt omschreven: "*De kern van de verwerkingen is dat chauffeurs die niet in dienst zijn van de Gebruiker zelf, bij aankomst bij een warehouse of andere afhaallocatie hun identiteitsbewijs en kenteken laten controleren en registreren alvorens er een lading aan hen ter beschikking zal worden gesteld. Hierbij wordt de echtheid van het aangeboden identiteitsbewijs gecontroleerd met scanapparatuur die in staat is om de RFID- en NFC-chips van identiteitsdocumenten uit te lezen en te controleren op echtheid en geldigheid. Daarnaast wordt aan de hand van een door ID Logsecure bijgehouden Incidentenregister gecontroleerd of het kenteken of de chauffeur eventueel betrokken is geweest bij identiteitsfraude of ladingdiefstal, in welk geval het systeem een waarschuwing geeft. Indien bij de controle of gedurende het transport van onregelmatigheden blijkt kan dit leiden tot registratie in het Incidentenregister.*"[2]

Gebruiker: een partij die op basis van een Aansluitovereenkomst de diensten van ID Logsecure gebruikt.

Incidentenregister: het register waarin Incidenten worden opgenomen.

Systeem: het geheel aan door ID Logsecure in opdracht van de Gezamenlijk verwerkingsverantwoordelijken beheerde Persoonsgegevens en bijbehorende metadata die in het kader van Veilig Vrachtvervoer worden verwerkt in de Database en het Incidentenregister alsmede de daarmee samenhangende loggingsgegevens op systeem- en query niveau.

Gezamenlijke verwerkingsverantwoordelijken: de Gebruikers gelden tezamen als gezamenlijk verwerkingsverantwoordelijken voor de centrale verwerking van persoonsgegevens onder dit Protocol. Het Protocol, waaraan alle Gebruikers zich dienen te verbinden overeenkomstig de Aansluitovereenkomst, fungeert als transparante regeling zoals bedoeld in artikel 26 AVG. De Gezamenlijk verwerkingsverantwoordelijken dragen de uitvoering van dit Protocol op aan ID Logsecure.

4. Wettelijk kader

Het relevante wettelijke beoordelingskader staat in de bijlage van dit besluit. De bijlage maakt onderdeel uit van dit besluit.

5. Beoordeling voorgenomen verwerking

Aan de hand van het wettelijk kader wordt de voorgenomen verwerking beoordeeld. De beoordeling is gebaseerd op de aan de verwerking ten grondslag liggende vergunningaanvraag, de gevoerde correspondentie, het Protocol[3], en de gegevensbeschermingseffectbeoordeling[4].

De beoordeling wordt hierna op volgende manier vormgegeven: allereerst wordt er gekeken naar de mate van verwerking van persoonsgegevens van strafrechtelijke aard (paragraaf 5.1). Alleen als er sprake is van persoonsgegevens van strafrechtelijke aard dan kan de verwerking vergunningplichtig zijn. Vervolgens wordt de verwerking getoetst aan artikel 33 UAVG, dat wil zeggen (1) is de verwerking noodzakelijk voor een zwaarwegend belang van derden (paragraaf 5.2) en (2) is in zodanige waarborgen voorzien dat de persoonlijke levenssfeer niet onevenredig worden geschaad (paragraaf 5.3). Tot slot wordt ingegaan op het zorgvuldig ontwerp van een gegevensverwerking (paragraaf 5.4).

[2] Paragraaf 2.1 van het Protocol

[3] Protocol Incidentenwaarschuwingssysteem Veilig Vrachtvervoer van 17 maart 2026, versie 1.25 welke als bijlage 3 was bijgevoegd bij de aanvraag.

[4] Model DPIA behorend bij het Protocol.

5.1 Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen

Chauffeurs die lading trachten af te halen bij een Gebruiker kunnen dit doen door middel van het inzetten van valse documenten. Ook kunnen chauffeur betrokken zijn geweest bij eerdere ladingdiefstal. Het Protocol benoemt als mogelijke incidenten: identiteitsfraude, lading(diefstal), kentekenfraude en documentfraude (valsheid in geschrifte). De AP merkt op dat deze gedragingen zijn beschreven in het Wetboek van Strafrecht of de Wegenverkeerswet 1994 en allen strafbaar zijn mits bewezen. Indien er voldoende aanleiding is om, na het in het Protocol beschreven hoor en wederhoor, over te gaan tot toevoegen van een registratie, kan worden aangenomen dat de feiten en omstandigheden, indien er aangifte en vervolging zou volgen, tot een bewezenverklaring in de zin van art. 350 van het Wetboek van Strafvordering kunnen leiden. Hiermee wordt voldaan aan de geldende jurisprudentie.[5]

De AP is van oordeel dat het Protocol terecht stelt dat er persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen kunnen worden verwerkt.

5.2 Noodzakelijk met het oog op een zwaarwegend belang van derden

5.2.1 Zwaarwegend belang van derden

Een vergunning van de AP kan alleen worden verleend als met de uitwisseling van persoonsgegevens van strafrechtelijke aard een zwaarwegend algemeen belang van derden wordt gediend. In het Protocol wordt aangegeven dat het zwaarwegend algemeen belang in dit geval ziet op het voorkomen en bestrijden van ladingdiefstal. Met dragende verwijzingen naar publicaties en onderzoek wordt de omvang van het probleem van ladingdiefstal onderbouwd.[6] Om ladingdiefstal tegen te gaan moeten private bedrijven in de logistieke sector in staat gesteld worden om data over incidenten en onrechtmatig handelende personen uit te wisselen.

De AP is op basis van de onderbouwing van oordeel dat het zwaarwegend belang van derden voldoende is aangetoond wat betreft de uitwisseling van persoonsgegevens van strafrechtelijke aard ten behoeve van derden.

5.2.2 Noodzakelijk

De verwerking dient noodzakelijk te zijn met het oog op voornoemde zwaarwegende belang. Het is volgens de wetgever aan de AP om vooraf, dat wil zeggen via de vergunningsaanvraag, noodzaak en evenredigheid te toetsen. De noodzakelijkheid van een verwerking moet onder andere worden getoetst aan de proportionaliteit en de subsidiariteit. Met andere woorden: een verwerking dient noodzakelijk te zijn om het vastgestelde doel van de verantwoordelijke te bereiken, waarbij dient te worden nagegaan of het middel opweegt tegen de inbreuk op de persoonlijke levenssfeer en of er geen minder verstrekkend middel is waarmee het doel ook wordt bereikt.

Zoals hiervoor aangegeven is het van belang voor de uitwisseling van gegevens van strafrechtelijke aard met derden een goede afweging van de proportionaliteit te maken. Volgens de wetgever kunnen onder andere de volgende omstandigheden een rol spelen bij de proportionaliteitstoets.[7]

---

[5] HR 29 mei 2009, ECLI:NL:HR:2009:BH4720, r.o. 4.4.
[6] Protocol, pagina 6-7.
[7] Zie Bijlage 2: Relevante Kamerstukken.

De Nederlandse logistieke sector is relatief groot en kwetsbaar voor ladingdiefstal. Hierbij speelt mee dat de Gebruiker die lading afgeeft dit niet altijd doet aan een bekende partij. Ladingbelanghebbenden kunnen bijvoorbeeld een transporteur inhuren die werkt met onderaannemers. Deze keten maakt dat het voor een Gebruiker nu niet goed mogelijk is om te controleren of een persoon die zegt gerechtigd te zijn om lading te halen, dit ook daadwerkelijk is. Zo kan men middels valse documenten trachten lading onrechtmatig te verkrijgen.

Daarnaast is voldoende gemotiveerd dat er geen andere minder verstrekkende middelen voorhanden zijn om het doel van de verwerking te verwezenlijken.

Hoewel het doen van aangifte een evidente reactie lijkt bij ladingdiefstal wordt de ladingdiefstal vaak pas opgemerkt op het moment dat de lading al meerder dagen weg is. Ervaringen leren dat de lading dan ook zelden volledig onbeschadigd wordt aangetroffen.

De AP merkt op dat dit Protocol een ander doel heeft dan de reeds in de logistieke sector aanwezige protocollen. Zo is het doel van het Waarschuwingsregister Logistieke Sector het, kortgezegd, weren van 'criminelen' als werknemer bij een volgende werkgever. Het doel van Gatekeeper is het, kortgezegd, het tegengaan van criminaliteit bij bepaalde (lucht)havens. Er is dan ook ten aanzien van de subsidiariteit geen samenloop met deze protocollen.

De AP merkt op dat, aangezien het bij dit Protocol niet gaat om werknemers van Aanvrager, het aanvragen van een VOG niet kan worden gezien als een passende alternatieve maatregel.

De verwerking uit dit Protocol is noodzakelijk om private partijen de middelen te geven elkaar te waarschuwen en zichzelf te beschermen tegen personen die bij de uitoefening van werkzaamheden voor een Gebruiker zich schuldig heeft gemaakt aan gedragingen zoals bedoeld in paragraaf 5.1 van dit besluit. Daarvoor is in het Protocol een limitatief aantal gedragingen geformuleerd die kunnen leiden tot registratie. Dit maakt de reikwijdte van de verwerking beperkt.

De AP is van oordeel dat voldoende is onderbouwd dat de verwerking noodzakelijk is voor het te dienen doel.

5.2.3 Afweging met de belangen of de grondrechten en fundamentele vrijheden van betrokkenen

Het belang dat met de inbreuk op het recht op bescherming van persoonsgegevens gepaard gaat dient afgewogen te worden tegen de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene.

Met de onderhavige verwerking van persoonsgegevens wordt er bij een chauffeur nagegaan of er sprake is van eerdere betrokkenheid bij ladingdiefstal of dat er sprake is van vervalste documenten. Het doel daarbij is om ladingdiefstal te voorkomen. Het is echter, zelfs als er indicaties van incidenten zijn, aan de Gebruiker om uiteindelijk te besluiten om de lading wel of niet af te geven.

Dit belang is afdoende onderbouwd en raakt ook een maatschappelijk belang. Hierbij betrekt de AP dat de verhouding tussen de chauffeurs en de Deelnemers geen arbeidsrelatie betreft. Ten aanzien van deze chauffeurs hebben Gebruikers en Ladingbelanghebbenden geen of beperkte controle over welke personen

werkzaamheden uitvoeren en lading rechtmatig komen ophalen. Dit stelsel geeft hen via deze vergunning wel de mogelijkheid daar passende invloed op uit te oefenen door een zekere mate van controle uit te oefenen waarmee kwaadwillende chauffeurs kunnen worden geweerd. Daarbij merkt de AP op dat met het stelsel van hoor en wederhoor en de bezwaar- en beroepsmogelijkheden de rechtsbescherming voor betrokkenen goed is ingericht. Van een lichtvaardige of disproportionele opname in de registers is daarmee niet gebleken.

In de afweging tussen deze belangen wordt voldoende onderbouwd dat de belangen van de Gebruikers zwaarder wegen. Hieronder wordt toegelicht welke waarborgen de Gebruikers hanteren ter bescherming van de betrokkenen.

5.3 Zodanige waarborgen dat de persoonlijke levenssfeer van betrokkenen niet onevenredig wordt geschaad

5.3.1 Rechtmatigheid, behoorlijkheid en transparantie

Elke verwerking van persoonsgegevens moet een rechtmatige grondslag in de zin van artikel 6, eerste lid, AVG hebben. De uitwisseling van strafrechtelijke persoonsgegevens in het Protocol is gebaseerd op het gerechtvaardigd belang van partijen om zichzelf en elkaar te beschermen tegen ladingdiefstal. Volgens vaste jurisprudentie moet hiervoor de zogenaamde ‘driestappentoets’ worden doorlopen. In paragraaf 5.2 is deze toets reeds beoordeeld door de AP.

De behoorlijkheid van de gegevensverwerking is onder andere geborgd in de uitgebreide rechtsbescherming en toezicht- en auditverplichtingen die zijn opgenomen in het Protocol. Het recht van hoor en wederhoor voor betrokkenen maakt een belangrijk deel uit van de procedures die volgens het Protocol gevolgd moeten worden.

De transparantie is geborgd door de notificatie van opname in een van de registers aan de betrokkene met daarbij de mogelijkheid om in bezwaar te gaan tegen opname.

5.3.2 Doelbinding

De persoonsgegevens worden verzameld voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. De gegevens mogen krachtens het Protocol niet worden gebruikt voor andere doeleinden.

5.3.3 Minimale gegevensverwerking

De verzamelde persoonsgegevens zijn beperkt tot wat ter zake toereikend is voor het omschreven doel. Er wordt door Gebruiker per geval gekozen of het nodig is om de documenten te controleren. Daaruit volgt, indien er een registratie aanwezig is, alleen een meldcode, icoon en kleurindicatie. Er worden geen andere persoonsgegevens getoond.

5.3.4 Juistheid

De verzamelde persoonsgegevens moeten correct en actueel zijn. Het Protocol voorziet in de eis dat betrokkenen deze kunnen rectificeren indien dat niet het geval is. Ook voorziet het Protocol in de situatie waarin een betrokkene strafrechtelijk is vrijgesproken of ontslagen is van rechtsvervolging, waarna de registratie van betrokkene kan worden geschrapt.

5.3.5 Opslagbeperking

Het Protocol voorziet in een duidelijke en onderbouwde bewaartermijn. De gegevens moeten volgens het Protocol worden gewist zodra de bewaartermijn is verstreken of zodra de betrokkene met succes zijn recht op verwijdering heeft ingeroepen.

5.3.6 Integriteit en vertrouwelijkheid

Het Protocol voorziet in de eis dat slechts daartoe geautoriseerde functionarissen toegang hebben tot de registratie. Deze functionarissen worden nadrukkelijk gewezen op de afspraken uit het Protocol. Verder voorziet het Protocol in technische en organisatorische maatregelen om de verwerking te beveiligen.

5.4 Zorgvuldig ontwerp voorgenomen verwerking

Er is een DPIA opgesteld ten behoeve van Gebruiker die willen deelnemen. In de DPIA worden diverse beheersmaatregelen voorgeschreven om een zorgvuldige verwerking van persoonsgegevens te waarborgen. De Gebruikers moeten deze DPIA onderschrijven en eventuele aan hen toegewezen beheersmaatregelen uitvoeren.

Het Protocol kent een jaarlijkse evaluatie op de werking van het Protocol en de technische en organisatorische maatregelen en de naleving door Gebruikers. Daarnaast zijn er interne controles en zijn er als onderdeel van de beveiligingsmaatregelen certificaten aanwezig die audits omvatten.

In de Model DPIA wordt geconcludeerd dat er geen hoge restrisico's voor betrokken bij de verwerking aanwezig zijn mits alle beheersmaatregelen correct worden uitgevoerd. Een Voorafgaande Raadpleging bij de AP conform artikel 37 AVG is daarom niet nodig. De AP kan deze conclusie volgen.

De AP merkt op dat zij bij de verlening van deze vergunning geen voorafgaand onderzoek heeft gedaan naar de implementatie van de beheersmaatregelen door de aanvrager.

6 Conclusie

Het Protocol Incidentenwaarschuwingssysteem Veilig Vrachtvervoer van 17 maart 2026, versie 1.25 welke als bijlage 3 was bijgevoegd bij de aanvraag geeft een adequate uitwerking van de inhoudelijke waarborgen die een behoorlijke en zorgvuldige gegevensverwerking borgt. Daarnaast voorziet het Protocol in organisatorische waarborgen die een juiste en zorgvuldige gegevensverwerking borgt. Ook zijn er voldoende maatregelen genomen die waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad. Het Protocol kent verder een uitwerking van de rechten van betrokkenen die voor de noodzakelijke balans- en correctiemogelijkheden zorgen.

Op grond van het voorgaande concludeert de AP dat de voorgenomen verwerking van persoonsgegevens in het Protocol voldoende waarborgen bevat, zodat de AP besluit op grond van artikel 33, vierde lid onder c, UAVG de aangevraagde vergunning te verlenen. De AP verbindt daaraan de hieronder genoemde voorschriften.

7 Voorschriften

De vergunning wordt verleend met inachtneming van de volgende voorwaarden:

1. De verwerking van persoonsgegevens van strafrechtelijke aard ten behoeve derden moet plaatsvinden conform het Protocol Incidentenwaarschuwingssysteem Veilig Vrachtvervoer van 17 maart 2026, versie 1.25 welke als bijlage 3 was bijgevoegd bij de aanvraag, dat door de Autoriteit Persoonsgegevens op 31 maart 2026 is beoordeeld. Het Protocol maakt deel uit van deze vergunning.

2. De looptijd voor het Protocol is vastgesteld op acht jaar vanaf 31 maart 2026. Deze vergunning wordt toegekend voor de periode van de resterende looptijd van het Protocol.

3. Als een wijziging van de verwerking van persoonsgegevens leidt tot een andere verwerking dan hoe deze in het Protocol is omschreven, dan moet voor de gewijzigde werkwijze een nieuwe vergunning bij de AP aan worden gevraagd. De AP zal dan opnieuw besluiten of voor deze werkwijze een vergunning kan worden verleend.

4. De goedkeuring voor het Protocol kent een verplichting om jaarlijks aan de AP een auditrapportage op te leveren. Aanvrager is verplicht hieraan mee te werken.

5. Dit besluit laat onverlet dat de AP ambtshalve of op basis van klachten of andere informatie over de verwerking nadere inlichtingen inwint of een onderzoek start om te controleren of de verwerking van persoonsgegevens in overeenstemming is met de AVG.

8 Afsluiting en rechtsmiddel

Indien u het niet eens bent met dit besluit kunt u binnen zes weken na de datum van verzending van het besluit ingevolge de Awb een bezwaarschrift indienen bij de Autoriteit Persoonsgegevens. U kunt een bezwaarschrift indienen per post door deze te zenden naar Postbus 93374, 2509 AJ Den Haag, onder vermelding van “Awb-bezwaar” op de envelop. U kunt ook een digitaal bezwaarschrift indienen, zie www.autoriteitpersoonsgegevens.nl. onder het kopje “Bezwaar maken tegen een besluit”. Het indienen van een bezwaarschrift schort de werking van dit besluit niet op.

Den Haag, 31 augustus 2026,

Autoriteit Persoonsgegevens,
Overeenkomstig het door de Autoriteit Persoonsgegevens genomen besluit,

J.J.F. Versluijs
Directeur Systeemtoezicht, Beveiliging en Technologie

Bijlage 1: Wettelijke kader

1. Verwerking van strafrechtelijke gegevens ten behoeve van derden

Artikel 10 AVG bepaalt:
"Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen mogen op grond van artikel 6, lid 1, alleen worden verwerkt onder toezicht van de overheid of indien de verwerking is toegestaan bij Unierechtelijke of lidstaatrechtelijke bepalingen die passende waarborgen voor de rechten en vrijheden van de betrokkenen bieden. Omvattende registers van strafrechtelijke veroordelingen mogen alleen worden bijgehouden onder toezicht van de overheid."

Artikel 1 UAVG bepaalt:
"In deze wet en de daarop berustende bepalingen wordt verstaan onder:
[...]
Persoonsgegevens van strafrechtelijke aard: persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen als bedoeld in artikel 10 van de verordening, alsmede persoonsgegevens betreffende een door de rechter opgelegd verbod naar aanleiding van onrechtmatig of hinderlijk gedrag; [...]"

Artikel 31 UAVG bepaalt:
Onverminderd artikel 10 van de verordening mogen persoonsgegevens van strafrechtelijke aard alleen worden verwerkt voor zover dit krachtens de artikelen 32 en 33 is toegestaan.
Artikel 33, vierde lid, aanhef en onder c, UAVG bepaalt:
"Persoonsgegevens van strafrechtelijke aard mogen ten behoeve van derden worden verwerkt:
[...]
c. indien de Autoriteit persoonsgegevens met inachtneming van het vijfde lid een vergunning voor de verwerking heeft verleend."

Artikel 33, vijfde lid, UAVG bepaalt:
"Een vergunning als bedoeld in het vierde lid, onderdeel c, kan slechts worden verleend, indien de verwerking noodzakelijk is met het oog op een zwaarwegend belang van derden en bij de uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad. Aan de vergunning kunnen voorschriften worden verbonden."

Artikel 6, eerste lid, aanhef en onder f, AVG bepaalt:
"De verwerking is alleen rechtmatig indien en voor zover aan ten minste een van de onderstaande voorwaarden is voldaan:
[...]
f) de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is."

Overweging 47 van de AVG stelt:
"De gerechtvaardigde belangen van een verwerkingsverantwoordelijke, waaronder die van een verwerkingsverantwoordelijke aan wie de persoonsgegevens kunnen worden verstrekt, of van een derde,

kan een rechtsgrond bieden voor verwerking, mits de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene niet zwaarder wegen, rekening houdend met de redelijke verwachtingen van de betrokkene op basis van zijn verhouding met de verwerkingsverantwoordelijke. […] In elk geval is een zorgvuldige beoordeling geboden om te bepalen of sprake is van een gerechtvaardigd belang, alsook om te bepalen of een betrokkene op het tijdstip en in het kader van de verzameling van de persoonsgegevens redelijkerwijs mag verwachten dat verwerking met dat doel kan plaatsvinden. De belangen en de grondrechten van de betrokkene kunnen met name zwaarder wegen dan het belang van de verwerkingsverantwoordelijke wanneer persoonsgegevens worden verwerkt in omstandigheden waarin de betrokkenen redelijkerwijs geen verdere verwerking verwachten. […]"

Artikel 5 AVG bepaalt:
"1. Persoonsgegevens moeten:

a) worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is („rechtmatigheid, behoorlijkheid en transparantie");
b) voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt; de verdere verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden wordt overeenkomstig artikel 89, lid 1, niet als onverenigbaar met de oorspronkelijke doeleinden beschouwd („doelbinding");
c) toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt („minimale gegevensverwerking");
d) juist zijn en zo nodig worden geactualiseerd; alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren („juistheid");
e) worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is; persoonsgegevens mogen voor langere perioden worden opgeslagen voor zover de persoonsgegevens louter met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden worden verwerkt overeenkomstig artikel 89, lid 1, mits de bij deze verordening vereiste passende technische en organisatorische maatregelen worden getroffen om de rechten en vrijheden van de betrokkene te beschermen („opslagbeperking");
f) door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging („integriteit en vertrouwelijkheid").

2. De verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van lid 1 en kan deze aantonen („verantwoordingsplicht")."

2. Zorgvuldig ontwerp voorgenomen verwerking

Artikel 35, tweede lid, aanhef en onder b, AVG bepaalt:
"Een gegevensbeschermingseffectbeoordeling als bedoeld in lid 1 is met name vereist in de volgende gevallen:
[…]

b) grootschalige verwerking van bijzondere categorieën van persoonsgegevens als bedoeld in artikel 9, lid 1, of van gegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten als bedoeld in artikel 10; of […]"

Artikel 36, eerste lid, AVG bepaalt:
"Wanneer uit een gegevensbeschermingseffectbeoordeling krachtens artikel 35 blijkt dat de verwerking een hoog risico zou opleveren indien de verwerkingsverantwoordelijke geen maatregelen neemt om het risico te beperken, raadpleegt de verwerkingsverantwoordelijke voorafgaand aan de verwerking de toezichthoudende autoriteit."

Het Besluit inzake lijst van verwerkingen van persoonsgegevens waarvoor een gegevensbeschermingseffectbeoordeling (DPIA) verplicht is[8] stelt:
"[De Autoriteit Persoonsgegevens] stelt vast dat voor de volgende verwerkingen van persoonsgegevens een gegevensbeschermingseffectbeoordeling verplicht is:

[…] 2. Zwarte lijsten
Verwerkingen waarbij persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten, gegevens over onrechtmatig of hinderlijk gedrag of gegevens over slecht betalingsgedrag door bedrijven of particulieren worden verwerkt en gedeeld met derden (artikel 33, vierde lid, aanhef en onder c, van de Uitvoeringswet Algemene verordening gegevensbescherming) (zwarte lijsten of waarschuwingslijsten, zoals deze bijvoorbeeld gebruikt worden door verzekeraars, horecabedrijven, winkelbedrijven, telecomproviders alsook zwarte lijsten die betrekking hebben op onrechtmatig gedrag van werknemers, bijvoorbeeld in de zorg of door uitzendbureaus). […]

11. Controle werknemers
Grootschalige verwerking van persoonsgegevens en-of stelselmatig monitoring van activiteiten van werknemers (bijvoorbeeld controle van e-mail en internetgebruik, GPS-systemen in (vracht)auto's van werknemers of cameratoezicht ten behoeve van diefstal- en fraudebestrijding). […]"

[8] Autoriteit Persoonsgegevens 27 november 2019, "Besluit inzake lijst van verwerkingen van persoonsgegevens waarvoor een gegevensbeschermingseffectbeoordeling (DPIA) verplicht is", Stcrt 2019 nr. 64418. Het besluit is gegrond op artikel 35, vijfde lid, en artikel 57, eerste lid onder k, AVG.

Bijlage 2: Relevante Kamerstukken

- *de mate waarin opname van een individu in het systeem waarop de gegevensuitwisseling betrekking heeft, kan betekenen dat betrokkene wordt uitgesloten van bijvoorbeeld eerste levensbehoeften of van goederen of diensten die betrekking hebben op een (klassiek of sociaal) grondrecht;*
- *de kwetsbaarheid van bepaalde groepen betrokkenen, zoals minderjarige klanten en werknemers, oudere werknemers en werknemers die geen mogelijkheid hebben om een eventueel ontslag aan te vechten;*
- *de reikwijdte van het systeem, in termen van zowel degenen die het systeem kunnen vullen, degenen die gegevens in het systeem kunnen raadplegen en degenen van wie persoonsgegevens in het systeem worden verwerkt. Hoe groter de reikwijdte, hoe ingrijpender de gevolgen van opname voor de betrokkene in het systeem kunnen zijn. Naarmate de reikwijdte van een systeem groter is, zullen derhalve de waarborgen voor betrokkenen zwaarder moeten zijn of zal het systeem in het geheel niet door de toetsing komen. Het beperken van de reikwijdte van het systeem (geografisch, sectoraal of anderszins) kan bijdragen aan een positieve uitkomst van de proportionaliteitsafweging.*[9]

[9] Kamerstukken II 2017-18, 34 851, nr. 7, Nota naar aanleiding van het verslag, p. 55.