AUTORITEIT
PERSOONSGEGEVENS

Handreiking cross-sectorale gegevensdeling tussen private partijen

Samenvatting

Niet toegestaan
Het uitgangspunt is dat het cross-sectoraal delen tussen private partijen van gegevens op een zwarte lijst niet is toegestaan. Tenzij wordt voldaan aan de zeer hoge eisen uit de Algemene verordening gegevensbescherming (AVG) en de Uitvoeringswet AVG (UAVG). Daarmee is het dus alleen in zeer uitzonderlijke gevallen toegestaan.

Protocol nodig
Private organisaties mogen niet zomaar gegevens van eenieder op een zwarte lijst zetten en deze met elkaar delen. Hier moet een uiterst zorgvuldig en zeer goed doordacht protocol aan ten grondslag liggen.

Mogelijk vergunning nodig
Staan op een cross-sectorale zwarte lijst strafrechtelijke gegevens? En wordt deze zwarte lijst gedeeld met derden? Dan zal hiervoor een vergunning aangevraagd moeten worden bij de Autoriteit Persoonsgegevens (AP). De kans is overigens zeer klein dat de AP een vergunning verleent om strafrechtelijke gegevens (zoals over fraude of diefstal) cross-sectoraal te delen met volstrekt andere branches of sectoren.

Inleiding
Veel ondernemers krijgen te maken met criminaliteit, zoals diefstal van producten en eigendommen, schade aan hun pand en/of agressie tegen hun personeel en klanten. Het gevolg: omzetverlies en veel (immaterieel) leed. Vaak ook blijken dezelfde criminelen actief te zijn in meerdere sectoren. Het is begrijpelijk dat ondernemers dit zo snel mogelijk willen stoppen. En daarom mogelijk overwegen criminelen op een zwarte lijst te plaatsen en die zwarte lijst te delen met andere ondernemers.

Toch is het dan goed om even een pas op de plaats te maken en de AVG/UAVG erbij te pakken. De (U)AVG beschermt burgers, bijvoorbeeld tegen onterecht op een zwarte lijst komen te staan. Het bijhouden van een zwarte lijst met (mogelijke) dieven, fraudeurs of overlastgevers is daarom aan regels gebonden. En het delen van die gegevens met derden mag zeker niet zonder meer. Al helemaal niet als het strafrechtelijke gegevens betreft, zoals over een winkeldiefstal. Feitelijk creëer je dan een politiedatabase, die vrij toegankelijk is voor ondernemers. Dit soort zwarte lijsten is alleen toegestaan als de (U)AVG goed in acht is genomen.

Omdat de AP heeft gesignaleerd dat de private sector behoefte heeft aan handvatten, heeft de AP in dit document een beknopt overzicht opgesteld van de belangrijkste AVG-normen waaraan deze *zeer uitzonderlijke gevallen* minimaal moeten voldoen.

Wat is een zwarte lijst?

Het doel van een zwarte lijst is om te waarschuwen voor bepaalde personen. Zo kunnen organisaties beoordelen of zij met die personen zaken willen doen. Bijvoorbeeld of zij die personen in hun winkel willen binnenlaten of in hun hotel willen laten overnachten. Op een zwarte lijst staan vaak strafrechtelijke gegevens of gegevens over ongewenst gedrag. Bijvoorbeeld dat iemand is veroordeeld voor winkeldiefstal of ernstige overlast heeft veroorzaakt. Private organisaties mogen niet zomaar een zwarte lijst opstellen en gebruiken, hieraan zijn voorwaarden verbonden.

Er zijn diverse zwarte lijsten:

1. Interne zwarte lijst
   De bestrijding van fraude binnen een eigen organisatie door het bijhouden van een interne zwarte lijst is onder strikte AVG-voorwaarden toegestaan. Als de onderneming deel uitmaakt van een concern, levert het binnen dit concern delen van een zwarte lijst in principe geen problemen op.
2. Sectorale zwarte lijst
   De AVG biedt enige ruimte voor het delen van een zwarte lijst met andere private organisaties binnen één sector. Of binnen een beperkt geografisch gebied. Maar hiervoor gelden wel strengere restricties dan voor een interne zwarte lijst. Om gegevens te mogen verwerken (en delen) heb je een grondslag nodig. Bij een zwarte lijst is de grondslag 'gerechtvaardigd belang' in de praktijk meestal de enige mogelijke grondslag. Fraudebestrijding kan voor een organisatie een gerechtvaardigd belang zijn. Dit kan ook als de fraudeurs opgenomen worden in een fraudepreventiesysteem dat gedeeld wordt met derden. Vanwege de grotere impact op de betrokkenen, stelt de AVG/UAVG zwaardere eisen aan zulke fraudepreventiesystemen.
3. Cross-sectorale zwarte lijst
   Er is sprake van een cross-sectorale zwarte lijst als private partijen een zwarte lijst willen gaan delen met andere private partijen buiten hun eigen sector. Voorbeelden van sectoren zijn: detailhandel, toerisme, horeca, logistieke sector, financiële sector, telecomsector, etc. Bij een cross-sectorale zwarte lijst vindt het delen niet enkel plaats in een sector, maar worden de gegevens in diverse sectoren gedeeld.
4. Vergunningplichtige zwarte lijst
   Voor (cross-)sectorale zwarte lijsten kan daarnaast een vergunning vereist zijn. Dit is het geval als er op de zwarte lijst strafrechtelijke gegevens staan en/of gegevens over een door de rechter opgelegd verbod vanwege onrechtmatig of hinderlijk gedrag. En een organisatie deze zwarte lijst wil delen met andere organisaties. De organisatie moet dan eerst een vergunning aanvragen bij de AP. Zonder vergunning mag de organisatie de zwarte lijst niet delen.

Best practices - sectorale zwarte lijsten

De AP heeft de volgende drie modelprotocollen beoordeeld, die de basis vormen voor vergelijkbare vergunningaanvragen:

Collectief winkelverbod

In veel steden en dorpen werken winkeliers, gemeente, politie en Openbaar Ministerie samen om veelplegende winkeldieven en structurele overlastveroorzakers (agressie, geweld) aan te pakken. Een van de instrumenten hiervoor is het opleggen van een collectief winkelverbod. Hiermee kunnen winkeliers ongewenste klanten toegang weigeren tot meerdere winkels binnen een specifiek winkelgebied.

Collectieve horecaontzegging
Het doel van een collectieve horecaontzegging is criminaliteit en overlast in het uitgaansleven terug te dringen. En zo de veiligheid van horecaondernemers, horecamedewerkers en bezoekers te waarborgen en te verbeteren.

Protocol incidentenwaarschuwingssysteem financiële instellingen
Financiële instellingen (verzekeraars, hypothecaire instellingen, financieringsondernemingen en banken) worden regelmatig geconfronteerd met fraude en criminaliteit. Een van de maatregelen om dit tegen te gaan is een incidentenwaarschuwingssysteem (zwarte lijst). Deze zwarte lijst biedt aangesloten financiële instellingen de mogelijkheid om gegevens over frauderende (rechts)personen te registreren en uit te wisselen.

Waarom is het delen van een zwarte lijst buiten een sector problematisch?

Het wordt in AVG-termen uiterst problematisch als private partijen een zwarte lijst willen gaan delen met andere private partijen *buiten hun eigen sector*. In deze gevallen spreken we over 'cross-sectorale gegevensdeling' (ofwel: een cross-sectorale zwarte lijst). De (U)AVG biedt binnen het Nederlandse rechtsbestel weinig tot geen juridische mogelijkheden voor cross-sectorale gegevensdeling tussen private partijen voor (horizontale) fraudebestrijding. Uit de wetsgeschiedenis blijkt namelijk dat de wetgever bij het vergunningstelsel uit de UAVG gegevensuitwisselingen binnen een bepaalde branche of in een afgebakend geografisch gebied voor ogen heeft.

Waarom is proportionaliteit extra belangrijk bij cross-sectorale zwarte lijsten?

Een goede proportionaliteitsafweging is essentieel bij alle gedeelde zwarte lijsten, om de noodzaak van de gegevensdeling aan te tonen. De organisatie die een zwarte lijst deelt met andere organisaties, moet kunnen aantonen dat 'het doel de middelen heiligt'. Dus: of het belang van de opsteller van de zwarte lijst (bijvoorbeeld fraude, winkeldiefstal of agressie tegengaan) opweegt tegen de gevolgen voor degene op de lijst (bijvoorbeeld geen bankrekening meer kunnen openen of bepaalde winkels of horeca niet meer binnen mogen).

Voor een cross-sectorale gegevensdeling is dit vereiste nog relevanter, omdat de gegevens in meerdere sectoren terecht kunnen komen. En daarmee automatisch grotere gevolgen kunnen hebben voor een persoon op de lijst (een betrokkene). De onderstaande criteria – die overigens ook gelden voor sectorale zwarte lijsten – zullen extra goed moeten worden afgewogen:

- Wordt een betrokkene uitgesloten van bijvoorbeeld eerste levensbehoeften of van goederen of diensten die een (klassiek of sociaal) grondrecht vertegenwoordigen?
- Is de betrokkene extra kwetsbaar? Denk daarbij aan: minderjarige klanten, daklozen en (oudere) werknemers die geen mogelijkheid hebben om een eventueel ontslag aan te vechten.
- Is de reikwijdte van het systeem goed omschreven? Denk daarbij aan: wie vult het systeem? Wie kunnen de gegevens in het systeem raadplegen? En van wie worden persoonsgegevens in het systeem verwerkt?

Aandachtspunt

Bij een cross-sectorale gegevensdeling is het van belang om te realiseren dat hoe groter de reikwijdte, hoe ingrijpender de gevolgen voor de betrokkene kunnen zijn. Wanbetaling bij de fietsenmaker kan dan onbedoeld leiden tot uitsluiting, zoals geen woning kunnen huren of geen hypotheek of baan kunnen krijgen. Naarmate de reikwijdte van een systeem groter is, zullen daarom de waarborgen voor betrokkenen zwaarder moeten zijn. Anders 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.

Voorbeeld

Eerder heeft de AP een vergunningaanvraag van een organisatie afgewezen. De gegevensdeling was cross-sectoraal opgezet om fraude te voorkomen. Dat betekende dat de gegevens van betrokkenen waarover meldingen van fraude in een bepaalde sector waren binnengekomen, niet gekoppeld aan die specifieke sector werden opgeslagen. Dit maakte de reikwijdte van de verwerking in sectorale zin zeer breed.

Deze organisatie was van plan om met het fraudepreventiesysteem meldingen van diverse (meer dan tien) soorten frauduleuze activiteiten vast te leggen. De reikwijdte van deze types fraude was groot en zag op een groot deel van het economisch verkeer. Hierdoor was de impact voor een betrokkene potentieel groot.

Daarbij was niet voorzien in waarborgen die deze reikwijdte beperkten voor de toegang van betrokkenen tot primaire levensbehoeften of tot goederen of diensten die een (klassiek of sociaal) grondrecht vertegenwoordigen. Ook werd er geen onderscheid gemaakt in partijen die zich als deelnemer konden aansluiten bij dit fraudepreventiesysteem.

Wat staat er minimaal in het protocol van een cross-sectorale zwarte lijst?

Wilt u als ondernemer een cross-sectorale zwarte lijst aanleggen? Dan moet u een protocol opstellen. In het protocol omschrijft u hoe u de persoonsgegevens gaat verwerken en hoe deze voorgenomen gegevensverwerking voldoet aan de eisen uit de AVG. Voor een vergunningaanvraag is het vereist om een protocol (plus een DPIA en het ingevulde aanvraagformulier) mee te sturen.

Om tot een rechtmatige cross-sectorale zwarte lijst te komen, moet u de volgende punten extra goed uitwerken in uw protocol:

1. Zorg voor een duidelijke cross-sectorale afbakening

   Bij een cross-sectorale gegevensdeling geldt dat registratie in een cross-sectorale zwarte lijst niet alleen nadelige gevolgen heeft in een afgebakende sector. Alle meldingen kunnen in elke deelnemende sector opgeslagen worden, waardoor de gevolgen automatisch groter zijn voor de (ten onrechte én terecht) geregistreerde crimineel. Als iemand ten onrechte als crimineel geregistreerd staat, kan diegene nadelige gevolgen ondervinden, zoals stigmatisering, uitsluiting van gebruik van een dienst of ontzegging van toegang in een compleet andere sector. Dit geldt overigens ook voor een terechte registratie: iemand die zich heeft misdragen bij de bakker, kan mogelijk door deze registratie opeens geen bankrekening meer openen of geen hypotheek meer afsluiten. Dit is een extra drijfveer om goed over de gegevensverwerking na te denken en deze goed uit te werken in het protocol.

Geef, om de sectoren duidelijk af te bakenen, in het protocol antwoord op de volgende vragen:

- Is er sprake van een sterke samenhang, verwevenheid of verwantschap tussen de sectoren waarin deze cross-sectorale zwarte lijst gedeeld gaat worden?
- Ligt het voor de hand dat deze sectoren met dezelfde soort 'boeven' te maken gaan krijgen?
- Komt bepaalde criminaliteit min of meer logisch/automatisch voor in een keten van sectoren als gevolg van de aard van de criminaliteit?
- Is het gekunsteld om elkaar **niet** te waarschuwen voor bepaalde vormen van criminaliteit?

Is het antwoord op een van bovenstaande vragen nee? Dan is dat een indicatie dat cross-sectoraal delen niet nodig is.

Verder moet u onderstaande vragen onderzoeken en toelichten in het protocol:

- Hoe toon je aan dat de criminaliteit/fraude zowel in sector X als sector Y zal plaatsvinden (dubbele aantoonplicht op ketenaspecten)? Bijvoorbeeld: mensen komen altijd bij dienstverlener A én bij dienstverlener B als het om deze vorm van criminaliteit gaat.
- Hoe toon je aan dat iemand in al deze sectoren toe zal slaan?
- In hoeverre is de dreiging van specifieke vormen van criminaliteit/fraude concreet en evident aanwezig in de deelnemende sectoren?

Lukt het u niet om een sluitende redenering vast te leggen in het protocol als antwoord op deze vragen? Dan is dat een indicatie dat uw cross-sectorale zwarte lijst niet is toegestaan.

Voorbeeld
Als je weet dat witwassers eerst altijd bij de notaris langsgaan, daarna naar de bank en vervolgens hetzelfde trucje proberen bij de makelaar, dan is dat een *indicatie* dat het cross-sectoraal delen van de gegevens van deze witwasfraudeurs tussen deze drie sectoren is toegestaan.

2. Zorg voor een duidelijke geografische afbakening

Hoe groter het geografisch gebied dat een cross-sectorale zwarte lijst beslaat, hoe meer waarborgen noodzakelijk zijn. U moet daarom een goede toelichting/motivering (sluitende redenering) opnemen in het protocol waarom is gekozen voor dit gebied. Geef daartoe antwoord op de volgende vragen:

- Waarom heeft u gekozen voor dit gebied?
- In hoeverre kunt u het gebied verkleinen?
- In hoeverre kunt u aantonen dat deze criminelen in dit specifieke geografische gebied opereren?

Een (te) groot geografische gebied is een indicatie dat uw cross-sectorale zwarte lijst niet is toegestaan.

Voorbeeld
Een huurder heeft van zijn woningcorporatie een collectief woonverbod opgelegd gekregen. Alle woningcorporaties in Zuid-Holland zijn aangesloten bij deze zwarte lijst. Hierdoor kan deze huurder voor een periode van vijf jaar niet in aanmerking komen voor een sociale huurwoning in geheel Zuid-Holland. *Toelichting:* een huurder die woont in een sociale huurwoning, kan in een te omvangrijk gebied helemaal niet meer in aanmerking komen voor een huurwoning. Een sociale huurder kan ook niet uitwijken naar de duurdere huurwoningen. Dit is daarom een disproportionele gegevensverwerking.

3. Zorg voor afgebakende fraudevormen (doelbinding)

Geef in het protocol duidelijk aan:

- welke vormen van criminaliteit/fraude worden opgenomen op de cross-sectorale zwarte lijst in relatie tot het vooraf omschreven doeleinde;
- welke (categorieën van) gegevens op deze cross-sectorale zwarte lijst worden geregistreerd;
- de wijze waarop deze gegevens worden verkregen;
- of het nodig is dat alle gegevens met alle deelnemers in alle sectoren gedeeld worden;
- op welke manier de verwerkingsverantwoordelijke verifieert of de gegevens juist en nauwkeurig zijn;
- hoe de geregistreerde persoonsgegevens tussen de verschillende deelnemers worden uitgewisseld: wanneer heeft een deelnemer recht om de cross-sectorale zwarte lijst te raadplegen en wanneer niet?

Bij een cross-sectorale gegevensdeling kan een beperking op bovenstaande punten een belangrijke waarborg zijn.

Voorbeeld
Autoverhuurbedrijven hebben veel last van personen die een auto huren met valse identiteitsbewijzen. Om deze fraudevorm (identiteitsfraude) tegen te gaan, is het van belang om de gegevens van deze fraudeurs te delen met andere autoverhuurbedrijven. Als een autoverhuurbedrijf bedenkt dat het handig is om ook andere, niet aan identiteitsfraude gelieerde fraudevormen hierbij op te nemen, dan is dat niet toegestaan (doelbinding).

4. Zorg voor de tijdelijkheid van de zwarte lijst of zeer korte bewaartermijnen

Bepaal of kan worden volstaan met een tijdelijke cross-sectorale zwarte lijst.

- Gaat het om een probleem dat tijdelijk van aard is?
- Is het noodzakelijk dat deze cross-sectorale zwarte lijst permanent van aard is?
- Is het mogelijk om korte bewaartermijnen door te voeren?

Is het antwoord op bovenstaande vragen nee? Dan is dat een indicatie dat cross-sectoraal delen disproportioneel is.

Voorbeeld
Als het bekend is dat WhatsAppfraude alleen in de zomermaanden plaatsvindt, dan is het niet toegestaan om deze zwarte lijst het gehele jaar aan te houden.

5. Realiseer een streng opnamebeleid

Bepaal op basis van welke concrete gedragingen betrokkenen op de cross-sectorale zwarte lijst geplaatst worden. Deze criteria moeten eenduidig en concreet zijn.

- Welke vorm(en) van criminaliteit/fraude wilt u aanpakken? Maak dit zo specifiek mogelijk én transparant voor de betrokkenen. Dit betekent dat vooraf voor betrokkenen duidelijk moet zijn op grond van welke gedragingen zij op de zwarte lijst terecht kunnen komen.
- Is achteraf goed te toetsen of de plaatsing op de zwarte lijst rechtmatig is?
- Is er logischerwijs samenhang tussen de vorm van criminaliteit of fraude, de diverse sectoren en de dader (betrokkene)? Maak dit inzichtelijk in het protocol.

Een zeer streng opnamebeleid kan bijdragen aan een positieve uitkomst van de proportionaliteit van de cross-sectorale zwarte lijst.

Voorbeeld
Het modelprotocol collectief winkelverbod (2020) bevat een uitgebreide procedure over in welke concrete gevallen bepaalde maatregelen in zullen gaan. Ook staat daarbij expliciet aangegeven welke persoonsgegevens verwerkt zullen worden.

6. Beperk het aantal deelnemers

Maak inzichtelijk welke soort private partijen (kunnen) deelnemen aan de zwarte lijst. Daarbij kunt u aan de volgende aspecten denken:

- Wanneer mag een bepaalde partij deelnemer worden? Het is wenselijk om vooraf toetredingscriteria hiervoor op te stellen, zoals: kan een deelnemer (evident) aantonen dat hij ook met diezelfde vorm van criminaliteit/fraude te maken heeft (gehad)?
- Is het mogelijk om een limitatieve lijst aan deelnemers vast te stellen?
- Maak de deelnemerslijst kenbaar, zodat betrokkenen hiervan kennis van kunnen nemen. Het moet voorzienbaar zijn voor betrokkenen dat hun gegevens ook terecht kunnen komen bij die deelnemers in een andere sector.
- Moeten alle deelnemers altijd toegang hebben tot alle gegevens of kan hier ook een beperking doorgevoerd worden?

Als er te veel deelnemers zijn opgenomen, is dat een indicatie dat de cross-sectorale zwarte lijst niet is toegestaan.

Voorbeeld
Bij een zwarte lijst van collectieve winkelverboden is in het protocol vooraf bepaald dat alleen de winkeliers in winkelcentrum X mogen deelnemen. Hierdoor is het is inzichtelijk voor het winkelend publiek welke winkeliers kunnen deelnemen aan deze gedeelde zwarte lijst.

Disclaimer

Dit document is expliciet bedoeld als een overzicht van waar een cross-sectorale gegevensdeling tussen private partijen minimaal aan moet voldoen. Andere, niet benoemde AVG-vereisten moeten uiteraard ook worden uitgewerkt in het protocol.