CBP Agenda 2015

Het verzamelen en gebruiken van persoonsgegevens – online en offline – neemt explosief toe. Overheden gebruiken deze gegevens bijvoorbeeld om belastingfraude tegen te gaan en om voorspellingen te doen over de zorgbehoefte van burgers. Bedrijven verzamelen en gebruiken persoonsgegevens onder meer om de dienstverlening te verbeteren en om mensen gerichter aanbiedingen te doen. Via digitale apparatuur worden voortdurend grote hoeveelheden gegevens vastgelegd over het gedrag van mensen. Het aanleggen, koppelen en analyseren van enorme gegevensbestanden wordt ook wel big data genoemd.

Big data

De toepassing van big data biedt kansen om innovatieve diensten te ontwikkelen en om problemen in de samenleving aan te pakken. Deze toepassing brengt echter ook grote risico's met zich mee. Bij onvoldoende beveiliging is het risico dat die bergen gegevens op straat komen te liggen. Bovendien is het voor mensen vaak totaal onduidelijk wie welke gegevens over hen voor welk doel verzamelt. En welke profielen organisaties op grond hiervan van hen opstellen, op basis waarvan zij anders kunnen worden behandeld dan anderen. Dat kan prettig zijn, maar dan moeten zij hierover wel goed zijn geïnformeerd en zelf een keuze kunnen maken. De kern van de bescherming van persoonsgegevens is immers dat mensen zeggenschap hebben en houden over hun persoonsgegevens, zodat ze zich vrij kunnen ontwikkelen.

Maatschappelijk debat

In de Europese en de daaruit afgeleide Nederlandse privacywetgeving zijn principes vastgelegd voor de verwerking van persoonsgegevens. Bijvoorbeeld dat je niet meer gegevens mag verzamelen dan noodzakelijk is voor het doel dat je nastreeft, dat je verzamelde gegevens niet voor een ander doel mag gebruiken en dat je transparant moet zijn over de gegevens die je van mensen verwerkt. Die principes hebben hun waarde bewezen en de tand des tijds doorstaan. Maar tegen de achtergrond van het fenomeen big data is naast het toezicht op de naleving van die principes een breed maatschappelijk en politiek debat nodig. Een debat waarin niet alleen de praktische voordelen van big data voor bijvoorbeeld bestuur en beleid aan de orde komen, maar waarin ook de risico's indringend tegen het licht worden gehouden. Zodat we als samenleving de grenzen bepalen waarbinnen we big data verantwoord kunnen toepassen.

Keuzes

Net als andere toezichthouders moet het College bescherming persoonsgegevens (CBP) vanwege zijn omvang keuzes maken en kan het niet overal optreden waar aanwijzingen van overtredingen zijn. Wij doen onderzoek bij het vermoeden van ernstige overtredingen van de wet die structureel van aard zijn, die veel mensen treffen en waarbij wij met onze bevoegdheden verschil kunnen maken.

In 2015 richt het CBP zich in het bijzonder op de onderstaande vijf thema's. Daarnaast komen wij in actie naar aanleiding van actuele gebeurtenissen en aanhoudende tips over (mogelijke) overtredingen die bij ons binnenkomen.

Onze missie

Het CBP staat voor het grondrecht op bescherming van persoonsgegevens. Iedereen heeft recht op een zorgvuldige omgang met zijn persoonsgegevens. Het CBP houdt toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens en adviseert over nieuwe regelgeving.

→ THEMA 1

Profiling

Profiling is een breed begrip. Op basis van patronen en (toevallige) correlaties binnen gegevensbestanden kunnen organisaties mensen indelen in profielen. Op grond van die profielen kunnen die organisaties deze personen vervolgens anders behandelen of gerichter benaderen, vaak zonder dat zij dat weten. Overheden kunnen profiling toepassen als een vorm van risicomanagement, bijvoorbeeld bij grenscontroles. Bedrijven kunnen met profiling iemand indelen in de categorie 'commercieel interessant' of 'niet-interessant', op basis van gedrag en voorspelde interesses gerichte aanbiedingen doen of anderszins beslissingen over deze persoon nemen. De twee belangrijkste risico's van profiling zijn het gebrek aan transparantie en het gevaar dat beslissingen over mensen worden genomen op basis van een (soms zelfs foutief) profiel. Het bestrijden van die twee risico's is dan ook in 2015 een speerpunt van het CBP op het gebied van profiling.

Tracking & tracing

Via digitale apparatuur zoals smartphones, smart watches, smart tv's en smart meters worden voortdurend grote hoeveelheden gegevens vastgelegd over het gedrag van mensen, zoals over hun locatie en hun surf- en kijkgedrag. De betrokkenen weten vaak niet welke gegevens organisaties precies verzamelen en voor welke doelen zij de gegevens gebruiken. Op basis van deze gegevens kunnen organisaties mensen in profielen indelen en anders behandelen dan anderen.

Het is van groot belang dat mensen zeggenschap houden over wat er met hun gegevens gebeurt. In veel gevallen is tracking & tracing alleen toegestaan met toestemming van degene die het betreft. Is de gegevensverwerking noodzakelijk voor het bedrijfsbelang en de inbreuk op de privacy gering? Dan hoeft een organisatie niet eerst toestemming te vragen, maar moet deze bijvoorbeeld wel een opt-out bieden.

In 2015 richt het CBP zich op het gebied van tracking & tracing vooral op de naleving van de eis dat mensen goed worden geïnformeerd. Ook kijkt het CBP of op de juiste wijze om toestemming is gevraagd dan wel dat een adequate opt-outmogelijkheid is geboden.

Onze visie

Het grondrecht op bescherming van persoonsgegevens is fundamenteel voor de werking van de rechtsstaat.

Het CBP beschermt dit grondrecht door:

- overtredingen van de wet aan te pakken;
- over nieuwe regelgeving te adviseren;
- op de hoogte te zijn van de dilemma's die in de samenleving spelen op het gebied van privacy;
- overheid, bedrijfsleven en andere maatschappelijke organisaties alert te maken op hun verantwoordelijkheid bij de bescherming van persoonsgegevens;
- informatie te verstrekken waarmee mensen hun recht kunnen uitoefenen;
- resultaten van toezicht en handhaving openbaar te maken;
- nationaal en internationaal samenwerking te zoeken ten behoeve van de bescherming van persoonsgegevens.

Onze kernwaarden

Het CBP is **onafhankelijk**. Dat betekent dat wij binnen de kaders van de wet onze eigen koers bepalen. Wij kiezen prioriteiten op basis van de ernst en de omvang van overtredingen. Intern bevorderen wij de onafhankelijke denkkracht van onze medewerkers.

Deskundigheid staat bij het CBP hoog in het vaandel. Wij zetten ons dan ook volledig in om hoogwaardig werk af te leveren. Daartoe werken wij samen in multidisciplinaire teams. Het CBP investeert in kennis, vaardigheden en de ontwikkeling van zijn medewerkers.

Het CBP is **transparant** over zijn resultaten en keuzes, creëert draagvlak voor zijn werk en nodigt uit tot dialoog. Wij zijn open, eerlijk en zichtbaar. Intern bevorderen wij een positieve en open werksfeer.

Het CBP werkt aan de bescherming van een grondrecht. Daar zijn wij trots op. Wij zijn **betrokken** bij ons werk en bij elkaar en staan met beide benen in de samenleving.

→ THEMA 2

Bijzondere persoonsgegevens

Bijzondere persoonsgegevens zijn gegevens over godsdienst, ras, politieke gezindheid, gezondheid en strafrechtelijk verleden. Omdat deze gegevens extra gevoelig zijn, heeft de wetgever bepaald dat zij alleen onder strikte voorwaarden mogen worden verzameld, bewaard en gebruikt. Gezondheidsgegevens en strafrechtelijke gegevens hebben in 2015 de speciale aandacht van het CBP.

Gezondheid

Op het gebied van gezondheid zijn drie grote bewegingen te zien. Ten eerste een verschuiving van zorgtaken vanuit het Rijk naar de gemeenten (zie hieronder bij 'decentralisatie'). Ten tweede is een tendens zichtbaar dat grote technologiebedrijven zich richten op de productie en promotie van apparatuur waarmee mensen zelf hun gezondheid en levensstijl kunnen monitoren. Dit heeft tot gevolg dat allerlei gezondheidsgegevens op die apparatuur staan opgeslagen, zich bij de aanbieders van de functionaliteiten bevinden en door derden opgevangen kunnen worden, doordat gebruik wordt gemaakt van zogeheten sensor data. De traditionele bescherming die mensen hebben door het medisch beroepsgeheim, is daarbij niet meer aanwezig. Ten derde zien zorginstellingen en individuele hulpverleners naar het oordeel van het CBP onvoldoende de noodzaak om bij de toepassing van nieuwe ICT de privacyrisico's goed in te schatten en te ondervangen. Het CBP richt zich in 2015 op alle drie de ontwikkelingen.

Strafrechtelijke gegevens

Politie en justitie wisselen steeds meer strafrechtelijke gegevens uit binnen samenwerkingsverbanden. Dat kan zijn met andere overheidsinstellingen, maar ook met private partijen, zoals particuliere beveiligingsbureaus. Ook maakt de politie steeds meer gebruik van het cameranetwerk van particulieren.

In 2015 richt het CBP zich op de vraag of het verzamelen, uitwisselen en bewaren van deze gegevens gebeurt binnen de wettelijke regels. Daarbij kijkt het CBP in het bijzonder of niet bovenmatig veel gegevens worden verzameld en of mensen goed worden geïnformeerd over de gegevensverwerking.

→ THEMA 3

Persoonsgegevens bij lokale overheden

Decentralisatie

Op 1 januari 2015 zijn de Jeugdwet, de Participatiewet en de Wet maatschappelijke ondersteuning 2015 (Wmo 2015) in werking getreden. De gemeenten zijn nu, in plaats van de rijksoverheid, verantwoordelijk voor de uitvoering van taken op het gebied van jeugdzorg, werk & inkomen en zorg aan langdurig zieken en ouderen (ook wel: het sociale domein). Dit wordt de decentralisatie van overheidstaken genoemd. Als gevolg hiervan vinden er verschillende gegevensverwerkingen plaats door verschillende partijen. Hier zitten ook gevoelige gegevens bij, zoals gezondheidsgegevens.

Een overkoepelende regeling voor gegevensuitwisseling in het sociale domein ontbreekt. Hierdoor is het voor gemeenten ingewikkeld om te beoordelen of zij in de praktijk aan de privacywetgeving voldoen. Daarnaast is het voor burgers lastig of zelfs ondoenlijk om hun privacyrechten uit te oefenen, zoals het recht op inzage in de eigen gegevens. Ook zijn er verschillende andere risico's: het bovenmatig verwerken van gegevens, het gebruik van gegevens voor andere doelen en onvoldoende beveiliging van de gegevens.

Het CBP heeft in 2013 en 2014 meerdere malen aandacht gevraagd voor deze risico's, zowel bij regering en parlement als bij de Vereniging van Nederlandse Gemeenten (VNG) en de gemeenten zelf. In 2015 controleert het CBP of de verwerking van persoonsgegevens in het sociale domein in overeenstemming met de privacywetgeving plaatsvindt. →

Medische gegevens zijn gevoelig en mogen alleen onder strikte voorwaarden worden verzameld en gebruikt.

Cameratoezicht in het lokale domein

Lokale overheden maken veel gebruik van cameratoezicht en passen hierbij nieuwe technieken toe. Zo zetten zij steeds vaker 'slimme' camera's en drones in om de openbare orde te bewaken. Bovendien is door een nieuw wetsvoorstel ook flexibel (mobiel) cameratoezicht in de openbare ruimte mogelijk. Deze nieuwe toepassingen van cameratoezicht zijn niet altijd even zichtbaar. Hierdoor is het des te belangrijker dat mensen goed worden geïnformeerd op welke plaatsen er cameratoezicht is.

Het CBP publiceert in 2015 richtsnoeren over cameratoezicht. Hierbij richt het CBP zich vooral op cameratoezicht door gemeenten en op cameratoezicht waarbij gemeenten met private partijen samenwerken. Met deze richtsnoeren geeft het CBP een toelichting op de geldende wettelijke regels voor cameratoezicht in het lokale domein.

Nationale samenwerking

Het CBP werkt op nationaal niveau samen en deelt kennis met verschillende nationale toezichthouders. Bijvoorbeeld als er raakvlakken zijn in het werkterrein. Ook neemt het CBP deel aan het Markttoezichthoudersberaad (MTB). De andere deelnemers zijn: Autoriteit Consument en Markt (ACM), Autoriteit Financiële Markten (AFM), De Nederlandsche Bank (DNB), Kansspelautoriteit en Nederlandse Zorgautoriteit (NZa).

Internationale samenwerking

Zowel in het Europese samenwerkingsverband van de zogeheten Artikel 29-werkgroep als in de internationale conferentie van privacytoezichthouders heeft het CBP een voortrekkersrol. In 2015 vindt die conferentie in Amsterdam plaats en treedt het CBP als gastheer op. Het thema van deze conferentie is 'privacy bridges'. Hiermee wordt voortgeborduurd op het initiatief van de CBP-voorzitter om een expertgroep te laten onderzoeken hoe bruggen kunnen worden geslagen tussen de Europese en het Amerikaanse rechtsstelsels op het gebied van de bescherming van persoonsgegevens. Het doel van het project is om praktische handvatten te ontwikkelen om de huidige privacykloof tussen die rechtsstelsels te overbruggen.

De relatie tussen werkgever en werknemer is kwetsbaar. Werknemers zijn immers in financieel en maatschappelijk opzicht afhankelijk van hun werkgever.

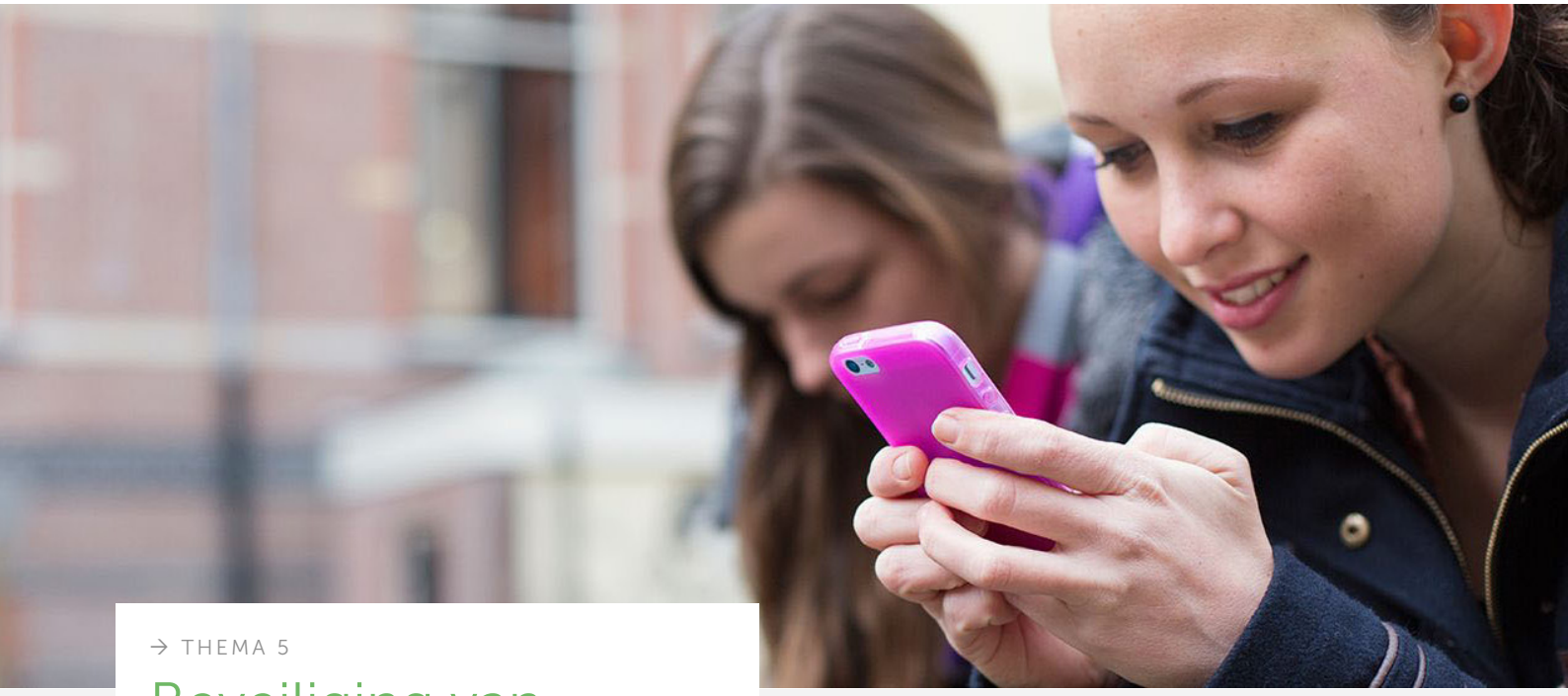
→ THEMA 4

Persoonsgegevens in de arbeidsrelatie

De relatie tussen werkgever en werknemer is kwetsbaar. Werknemers zijn immers in financieel en maatschappelijk opzicht afhankelijk van hun werkgever. Dit kan hen in een lastig parket brengen als de werkgever een verzoek doet dat raakt aan hun persoonlijke levenssfeer. Ook zal een werknemer een werkgever niet gemakkelijk aanspreken als binnen het bedrijf in strijd met de wet wordt gehandeld. De druk om persoonsgegevens prijs te geven kan voor werknemers sterker zijn in tijden van hoge werkloosheid.

Mede uit signalen van burgers en vakbonden blijkt dat werkgevers op verschillende manieren inbreuk maken op de persoonlijke levenssfeer van werknemers. Zo gebruiken bedrijven de camera's die zij ophangen voor beveiligingsdoeleinden geregeld om werknemers te controleren op hun functioneren. Ook vragen werkgevers allerlei medische gegevens van werknemers als zij zich ziek melden, terwijl dit niet mag.

In 2015 doet het CBP onderzoek naar overtredingen, maar is het ook in gesprek met brancheverenigingen en vakbonden. Ook langs die weg bevorderen wij de naleving van de bescherming van persoonsgegevens op de werkplek.



→ THEMA 5

Beveiliging van persoonsgegevens

ICT is doorgedrongen tot in de haarvaten van onze samenleving, zowel in de publieke als de private sector. Aan de ene kant biedt ICT talloze gebruiksmogelijkheden. Aan de andere kant zorgen de wijdverbreide toepassing van ICT en de omvang van de gegevensbestanden ervoor dat de impact bij onvoldoende beveiliging van de gegevens sterk is toegenomen.

Organisaties moeten tot op het hoogste niveau zijn doordrongen van het belang van adequate beveiliging van persoonsgegevens.

Bedrijven en overheden moeten op grond van de Wet bescherming persoonsgegevens zowel technische als organisatorische maatregelen nemen om de persoonsgegevens die zij onder hun hoede hebben voldoende te beveiligen. Deze organisaties moeten tot op het hoogste niveau zijn doordrongen van het belang van adequate beveiliging van persoonsgegevens. En al in het eerste stadium van de ontwikkeling van nieuwe producten en diensten moet dit onderwerp op de agenda staan.

Naar verwachting treedt in 2015 de meldplicht datalekken in werking. Het doel van deze meldplicht is zowel het beveiligingsniveau van gegevens als de zelfredzaamheid van burgers te vergroten. Publieke en private organisaties zullen datalekken moeten melden aan het CBP en in ernstige gevallen ook aan de mensen van wie de gegevens zijn. In de telecomsector bestaat deze verplichting al, maar moeten organisaties de melding doen bij de Autoriteit Consument en Markt (ACM). In de toekomst moeten zij zowel datalekken in de telecomsector als in andere sectoren melden aan het CBP, voor zover hierbij persoonsgegevens in het geding zijn. Het CBP treft voorbereidingen om de meldingen op een efficiënte en effectieve manier te verwerken. Daarnaast doet het CBP in 2015, net als in voorgaande jaren, onderzoeken naar vermeende overtredingen van de wettelijke eis persoonsgegevens adequaat te beveiligen.

Werkwijze CBP

Het CBP is de autoriteit die toezicht houdt op de naleving van de privacywetgeving. Om naleving te bevorderen, zet het CBP een mix van instrumenten in op het gebied van toezicht, handhaving en communicatie.

Toezicht

Tips die het CBP ontvangt via zijn website en telefonisch spreekuur geven belangrijke aanwijzingen over mogelijke privacyovertredingen. Op basis van deze tips en kennis van het toezichtdomein bepaalt het CBP waarnaar het onderzoek doet. We passen hierbij een 'trechter' toe, omdat we niet bij alle overtredingen in actie kunnen komen. Wij doen onderzoek bij het vermoeden van ernstige overtredingen van de wet die structureel van aard zijn, die veel mensen treffen en waarbij wij met onze bevoegdheden verschil kunnen maken.

In bepaalde gevallen starten we geen onderzoek, maar sturen we een brief aan bedrijven overheden of voeren we een gesprek. Dit kan al voldoende zijn om de overtreding te laten beëindigen. Wij geven handreikingen aan organisaties door richtsnoeren uit te brengen waarin we voor een specifieke sector of soort gegevensverwerking een toelichting geven op de geldende regels.

Handhaving

Het CBP heeft de bevoegdheid om bedrijven en overheden die de wet overtreden een last onder dwangsom op te leggen. Zij krijgen een bepaalde periode om de overtredingen te beëindigen. Als dit niet gebeurt, moeten zij de dwangsom betalen. Op dit moment is een wetswijziging in voorbereiding die het CBP ook de bevoegdheid geeft direct een boete op te leggen. Het opleggen van een boete is geen doel op zich. Het gaat ons vooral om de preventieve werking die uitgaat van een boetebevoegdheid, waardoor de wet naar verwachting beter zal worden nageleefd. Wij zullen dan ook in beginsel bij geconstateerde overtredingen een last onder dwangsom opleggen en alleen in het uiterste geval een boete uitdelen.

Wij doen onderzoek bij het vermoeden van ernstige overtredingen van de wet die structureel van aard zijn, die veel mensen treffen en waarbij wij met onze bevoegdheden verschil kunnen maken.

Communicatie

Externe communicatie is een belangrijk middel om onze doelen te bereiken. Wij communiceren op open wijze met burgers, pers, bedrijven, overheden en andere stakeholders. Dit doen wij niet alleen om mensen te informeren, te waarschuwen en hun handvatten te geven om zelf hun rechten uit te oefenen. We willen ook verantwoording afleggen over onze keuzes. Daarnaast is externe communicatie een belangrijk instrument om naleving van de privacywetgeving te bevorderen. Wij doen dit onder meer door onze prioriteiten te publiceren, onderzoeksbevindingen en sancties openbaar te maken en te reageren op ontwikkelingen in de actualiteit.

Het CBP verzorgt regelmatig externe optredens en voert gesprekken met brancheorganisaties. Daarnaast gaan we in rondetafelgesprekken de dialoog aan met groepen stakeholders. Dit doen wij om het contact met hen te onderhouden en om te horen hoe zij tegen het CBP aankijken, maar ook om te vernemen tegen welke problemen zij aanlopen in de praktijk.

Zo kan de inzet van communicatie er op verschillende manieren toe leiden dat niet alleen onderzochte bedrijven en overheden tot naleving van de wet worden aangezet, maar dat sprake is van een uitstralende werking binnen een hele sector.