COLLEGE BESCHERMING
PERSOONSGEGEVENS
Prins Clauslaan 20
Postbus 93374
2509 AJ Den Haag
TELEFOON 070 381 13 00
FAX 070 381 13 01
E-MAIL info@cbpweb.nl
INTERNET www.cbpweb.nl

De Wet Bescherming Persoonsgegevens

INHOUD

Over de bescherming van uw persoonlijke gegevens

COLOFON
Augustus 2001
Uitgave: College bescherming persoonsgegevens
Grafisch ontwerp: Miriam Monster
Druk: Sdu Grafische Bedrijven

COLLEGE BESCHERMING PERSOONSGEGEVENS

PERSOONSGEGEVENS ZIJN ALLE GEGEVENS

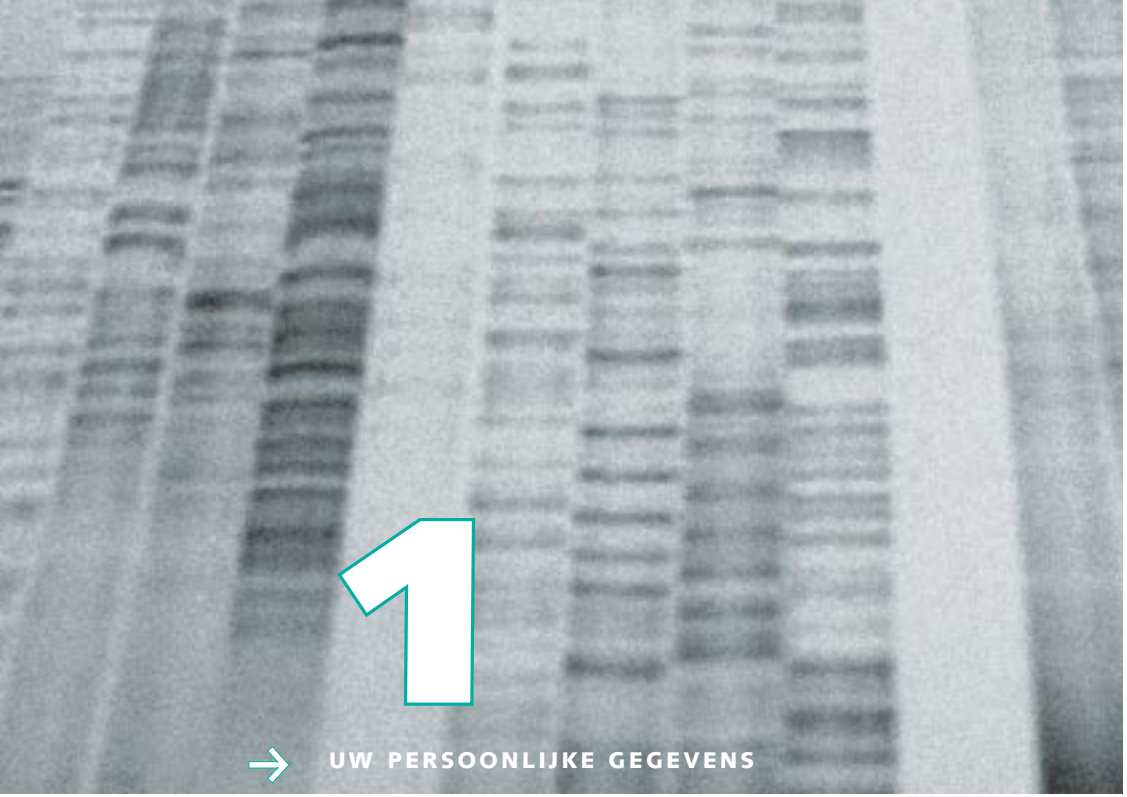
DIE IETS OVER U ZEGGEN EN

DIE VAN INVLOED KUNNEN ZIJN OP DE MANIER

WAAROP U WORDT BEOORDEELD OF BEHANDELD

INHOUDSOPGAVE

< VORIGE | INHOUD | VOLGENDE >



1

UW PERSOONLIJKE GEGEVENS

Om uiteenlopende redenen worden regelmatig, gevraagd en ongevraagd, allerlei gegevens over u vastgelegd.
Het energiebedrijf houdt bij hoeveel gas en elektriciteit u verbruikt en wanneer u betaalt. De bibliotheek houdt bij welke boeken u leent. Als u een ziektekosten- of levensverzekering wilt afsluiten moet u een lijst van vragen beantwoorden over uw gezondheid. In het aangiftebiljet inkomstenbelasting vraagt de fiscus u gedetailleerde gegevens over uw inkomsten, uw bezittingen, uw schulden, etc. Om voor een uitkering in aanmerking te komen moet u gegevens verstrekken over uw arbeidsverleden, over het laatst genoten salaris, etc.

De gegevens die u aan verschillende instanties of organisaties verstrekt, worden meestal opgeslagen in computers. Daarmee zijn ze gemakkelijk te verwerken en voor verschillende instanties of personen beschikbaar. Dankzij computers kan de overheid tal van ingewikkelde wetten doelmatig uitvoeren en de burger optimaal van dienst zijn. Ook particuliere organisaties en bedrijven kunnen door geautomatiseerde gegevensverwerking efficiënter werken. Maar tegelijkertijd is het voor u minder makkelijk geworden om te achterhalen welke gegevens van u door (overheids)organisaties en bedrijven zijn vastgelegd, waar die gegevens voor worden gebruikt en aan wie ze worden doorgegeven.

De gegevens die van u worden gebruikt, moeten juist en volledig zijn. Ze moeten in principe ook alleen worden gebruikt voor het doel waar u ze voor verstrekt heeft. Van sommige gegevens wilt u graag dat ze vertrouwelijk worden behandeld, dat ze uitsluitend worden vastgelegd door de persoon of instantie die ze nodig heeft en dat ze niet verder worden verspreid dan noodzakelijk is. Het zijn immers uw persoonlijke gegevens.

Om te bevorderen dat uw persoonlijke gegevens zorgvuldig worden behandeld en om u in staat te stellen dat zelf te controleren is er een speciale wet opgesteld, de Wet bescherming persoonsgegevens.

< VORIGE | INHOUD | VOLGENDE >

2

WET BESCHERMING PERSOONSGEGEVENS

Sinds 1 september 2001 is de Wet bescherming persoonsgegevens (WBP) van kracht. De wet geeft aan wat de rechten zijn van iemand van wie gegevens worden gebruikt en wat de plichten zijn van de instanties of bedrijven die gegevens gebruiken. Een aantal bepalingen in de WBP is nader uitgewerkt in besluiten.

De WBP introduceert een aantal definities. Deze definities worden hieronder uitgelegd. De WBP gaat over het verwerken van persoonsgegevens. Dat kunnen zijn uw naam, uw geboortedatum en uw adres, maar ook uw banksaldo, uw beroep, uw nationaliteit, uw politieke overtuiging en gegevens over uw gezondheid. Persoonsgegevens zijn alle gegevens die iets over u zeggen en die van invloed kunnen zijn op de manier waarop u wordt beoordeeld of behandeld. Met verwerken wordt bedoeld alle handelingen met die gegevens vanaf het verzamelen tot aan het vernietigen. Bijvoorbeeld het vastleggen van gegevens die nodig zijn voor het voeren van een cliëntenadministratie van een bedrijf, of medische dossiers van een ziekenhuis en het bestand van woningzoekenden in een gemeente. In de meeste gevallen zal het gaan om geautomatiseerde verwerkingen. Het kan echter ook gaan om niet-geautomatiseerde verwerkingen van persoonsgegevens die in een bestand zijn opgenomen, zoals een kaartenbak. Deze persoonsgegevens moeten dan wel een gestructureerd geheel vormen. De verantwoordelijke voor een verwerking is de (overheids)organisatie, het bedrijf of de persoon die uw gegevens gebruikt voor eigen doeleinden. De betrokkenen zijn de personen van wie gegevens worden verwerkt.

De Wet bescherming persoonsgegevens is niet van toepassing op onder meer:
- het gebruik van persoonsgegevens uitsluitend voor persoonlijke of huishoudelijke doeleinden;
- verwerkingen van persoonsgegevens door inlichtingen- en veiligheidsdiensten;
- het uitvoeren van de politietaak.

Op de gegevens die verwerkt worden in de bevolkingsadministratie van uw gemeente, is de Wet gemeentelijke basisadministratie van toepassing. Op de gegevens die verwerkt worden in de politieregisters, is de Wet politieregisters van toepassing.

< VORIGE | INHOUD | VOLGENDE >

3

VERPLICHTINGEN VAN DE VERANTWOORDELIJKE

Gegevens moeten op een behoorlijke en zorgvuldige manier en in overeenstemming met de WBP en toepasselijke andere wetten verwerkt worden. Voordat een verantwoordelijke uw gegevens mag verzamelen, moet hij eerst bepalen voor welk doel of doelen hij dat doet. Daarnaast mag een verantwoordelijke alleen op basis van één of meer in de WBP genoemde grondslagen uw persoonsgegevens verwerken.

Voorbeelden van zulke grondslagen zijn:

- uw vrije en gerichte toestemming;
- het uitvoeren van een overeenkomst. Een verantwoordelijke mag dus uw gegevens gebruiken die noodzakelijk zijn voor het opstellen van een rekening;
- het nakomen van een wettelijke verplichting. Uw werkgever is verplicht om bepaalde gegevens over u aan de Belastingdienst te verstrekken;
- een gerechtvaardigd (bedrijfs)belang. Een verantwoordelijke kan een legitiem belang hebben bij het gebruik van uw gegevens. Uw gegevens mogen gebruikt worden als dat noodzakelijk is voor de behartiging van een dergelijk belang, maar dan moet wel met uw belang rekening gehouden worden.

Voor bepaalde categorieën van bijzondere persoonsgegevens, zoals godsdienst, ras, gezondheid en strafrechtelijk verleden, gelden nog andere beperkingen. Een verantwoordelijke mag zulke gegevens alleen verwerken als daarvoor een grondslag is te vinden in een wet.

Alleen onder strikte voorwaarden mag een verantwoordelijke de verzamelde gegevens ook voor andere doeleinden gebruiken dan waarvoor hij ze oorspronkelijk verzameld heeft. Dat kan alleen als het gebruik niet op gespannen voet staat met het oorspronkelijke doel. Zo heeft een verzekeringsmaatschappij in het kader van een ziektekostenverzekering bepaalde medische gegevens van u nodig, maar die mag zij niet gebruiken om te beslissen of ze u vervolgens al dan niet een levensverzekering aanbiedt.

De verantwoordelijke heeft de verplichting om maatregelen te treffen om onnodige verzameling of verder gebruik van uw persoonsgegevens tegen te gaan. Dat is te bereiken door bijvoorbeeld waar mogelijk de gegevens te ontdoen van de naam van de betrokkene en andere identificerende kenmerken. De getroffen maatregelen moeten ook gericht zijn tegen onjuist gebruik binnen de organisatie van de verantwoordelijke.

Een verantwoordelijke moet het verwerken van gegevens melden bij het College bescherming persoonsgegevens (CBP, voorheen Registratiekamer), tenzij de betreffende verwerking hiervan uitgezonderd is in het Vrijstellingsbesluit. Voorbeelden van vrijgestelde verwerkingen zijn abonnementadministraties en salarisadministraties. De vrijstelling geldt overigens alleen als de verwerking aan bepaalde eisen voldoet en alleen maar bepaalde gegevens bevat. Indien een verantwoordelijke of een brancheorganisatie een functionaris voor de gegevensbescherming heeft benoemd, kan de melding ook bij die functionaris gedaan worden. U kunt informatie opvragen over een melding bij het CBP. U kunt ook aan de verantwoordelijke informatie vragen over vrijgestelde verwerkingen. Vrijstelling van melding betekent overigens niet dat een verantwoordelijke vrijgesteld is van de overige bepalingen van de WBP.

< VORIGE | INHOUD | VOLGENDE >

4

RECHTEN VAN DE BETROKKENE

De Wet bescherming persoonsgegevens geeft u een aantal rechten waardoor u controle kunt uitoefenen op het gebruik van uw persoonsgegevens door een verantwoordelijke.

Recht op informatie
U moet kunnen nagaan wat er met uw gegevens gebeurt. Daarom moet een verantwoordelijke u informeren over het doel (of de doeleinden) van het verzamelen en zijn naam en adres. Vaak moeten daarbij ook andere bijzonderheden vermeld worden, die u een inzicht kunnen geven in het gebruik van uw gegevens. Als de verantwoordelijke direct bij u uw gegevens verzamelt, moet u vooraf worden geïnformeerd. Deze informatie kan slechts achterwege gelaten worden als u al van het verzamelen daadwerkelijk op de hoogte bent, bijvoorbeeld omdat u die informatie in de vorm van een brochure hebt gekregen.

Recht op inzage
U hebt het recht om inzage te verzoeken in uw persoonsgegevens en het gebruik daarvan door een verantwoordelijke. Modelbrief A achterin deze brochure kunt u gebruiken om een verantwoordelijke te vragen of deze uw persoonsgegevens verwerkt. Als dat het geval blijkt te zijn, moet de verantwoordelijke u binnen vier weken een overzicht van de gegevens geven. Hij moet ook informatie verstrekken over het doel van de verwerking(en), de ontvangers van de gegevens en over de herkomst van de gegevens. Voor het geven van deze informatie kan de verantwoordelijke doorgaans een vergoeding van ten hoogste 4,50 euro vragen.

Als een overzicht ook gegevens bevat van een derde, die naar verwachting bezwaar zal hebben tegen het verstrekken van die gegevens aan u, dan moet de verantwoordelijke die derde in de gelegenheid stellen om zijn zienswijze naar voren te brengen. De verantwoordelijke kan weigeren aan een verzoek om inzage te voldoen als dat bijvoorbeeld noodzakelijk is in het belang van voorkoming, opsporing en vervolging van strafbare feiten of ter bescherming van de rechten en vrijheden van anderen.

Recht op verbetering, aanvulling, verwijdering of afscherming
Nadat u inzage hebt gekregen, kunt u de verantwoordelijke verzoeken uw persoonsgegevens te verbeteren, aan te vullen, te verwijderen of af te schermen (correctierecht). Dat kan als de gegevens die gebruikt worden door de verantwoordelijke feitelijk onjuist, onvolledig of niet ter zake dienend zijn voor het doel of de doeleinden van de verwerking. De verantwoordelijke moet binnen vier weken reageren op uw verzoek. Een weigering moet hij motiveren. Achterin deze brochure vindt u modelbrief B voor het doen van een verzoek.

In geval van inwilliging van het verzoek, moeten andere organisaties aan wie de (onjuiste of niet ter zaken doende) gegevens zijn verstrekt, van de wijzigingen op de hoogte gesteld worden, tenzij dat onmogelijk is of een onredelijke inspanning oplevert voor de verantwoordelijke. De verantwoordelijke moet de wijzigingen zo snel mogelijk doorgeven.

Recht van verzet
Het recht van verzet houdt in dat u het recht hebt om bezwaar te maken (verzet aan te tekenen) tegen het gebruik van uw gegevens door een verantwoordelijke. Er zijn twee vormen van verzet:
– U kunt in enkele gevallen verzet aantekenen in verband

< VORIGE | INHOUD | VOLGENDE >

met uw bijzondere persoonlijke omstandigheden. Een verantwoordelijke moet dan beslissen of hij stopt met de verwerking of hiermee doorgaat omdat hij meent een goede reden hiervoor te hebben. De verantwoordelijke mag u een vergoeding van ten hoogste 4,50 euro vragen om uw verzoek in behandeling te nemen. Dit geld moet hij weer teruggeven als hij het verzoek inwilligt. Voor het aantekenen van deze vorm van verzet kunt u modelbrief C achterin deze brochure gebruiken.
– Zodra u verzet aantekent tegen het gebruik van uw gegevens voor commerciële en charitatieve doelen, moet de verantwoordelijke dat gebruik altijd direct beëindigen. Dit is het absolute recht van verzet. U hoeft niet te zeggen waarom en de verantwoordelijke mag geen vergoeding vragen om een verzoek in behandeling te nemen. Een verantwoordelijke moet u informeren over het recht van verzet. Voor het aantekenen van deze vorm van verzet kunt u modelbrief D achterin deze brochure gebruiken.

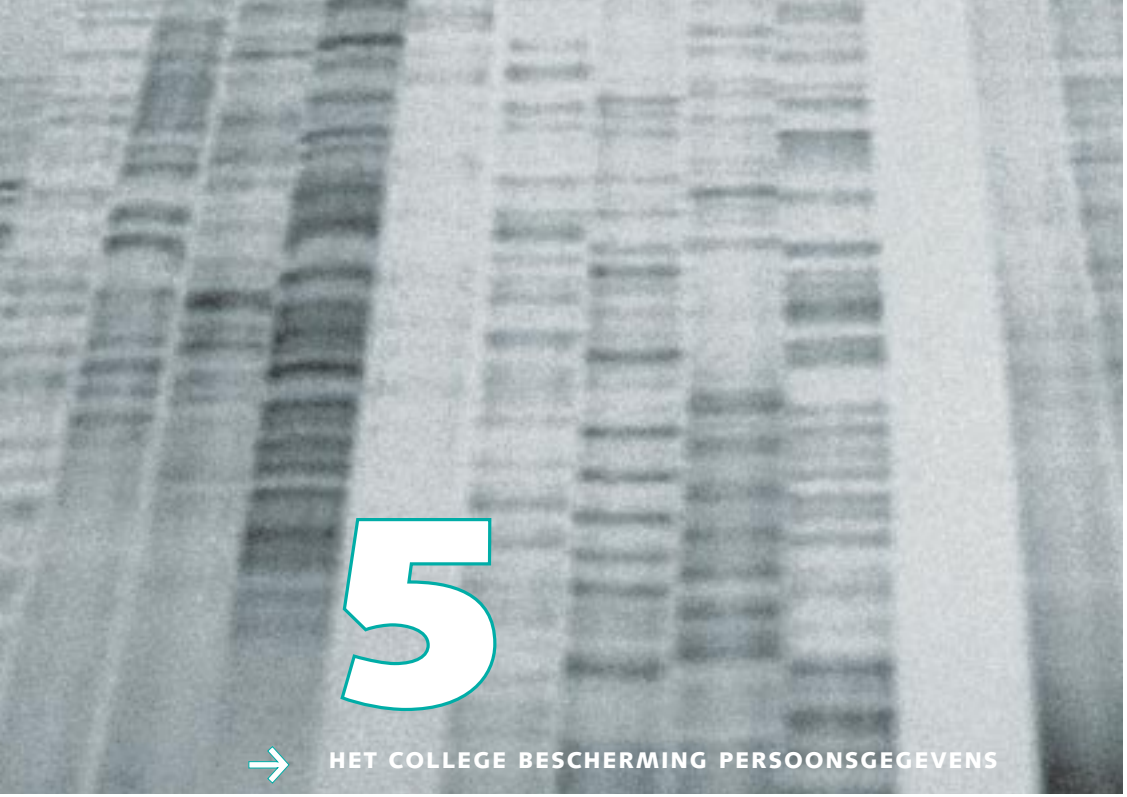
Hoe kunt u uw rechten uitoefenen?
Voor het uitoefenen van de genoemde rechten moet u zich schriftelijk wenden tot de verantwoordelijke. Dat kunnen zijn: burgemeester en wethouders van uw gemeente, de directeur van uw bank, de directie van de verzekeringsmaatschappij, etc. Het is raadzaam eerst (telefonisch) contact op te nemen met de betreffende organisatie of instelling over de wijze waarop u uw verzoek kunt indienen. Sommige instellingen hebben daar speciale formulieren voor. U kunt ook gebruik maken van de modelbrieven achter in deze brochure.

Als u een verzoek doet om inzage in of correctie van uw persoonsgegevens, moet u aantonen dat u inderdaad de persoon bent van wie u de gegevens wilt inzien of corrigeren. Het is immers niet de bedoeling dat anderen uw gegevens inzien of dat u de gegevens van anderen kunt corrigeren. Zorg er dus voor dat u in uw brief uw volledige naam en voorletters vermeldt, uw geboortedatum en uw volledige adres. De verantwoordelijke kan u ook vragen een kopie bij te voegen van uw rijbewijs, paspoort of ander identiteitsbewijs.

U kunt de volgende acties ondernemen bij geschillen over het uitoefenen van uw rechten:
– Als een verantwoordelijke of een brancheorganisatie een functionaris voor de gegevensbescherming heeft aangesteld, kunt u bij deze functionaris terecht met vragen en klachten.
– Als een branche een gedragscode heeft vastgesteld en daarin is een regeling voor het oplossen van geschillen opgenomen, kunt u op grond daarvan actie ondernemen.
– Als het gaat om besluiten van overheidsorganen op verzoeken om inzage, verbetering, aanvulling, verwijdering of afscherming dan wel op verzet, kunt u bezwaar en beroep aantekenen tegen deze besluiten.
  Voor informatie over bezwaar en beroep kunt u terecht op de website van het ministerie van Justitie: www.minjust.nl.
  Wanneer het overheidsorgaan een beslissing heeft genomen over uw ingediende bezwaarschrift en u bent het niet eens met deze beslissing, kunt u ook een verzoek tot bemiddeling indienen bij het CBP.
– Is de verantwoordelijke geen overheidsorgaan, dan kunt u binnen zes weken een verzoek tot bemiddeling indienen bij het CBP. U kunt ook een verzoekschrift indienen bij de rechtbank met het verzoek de verantwoordelijke een bevel te geven. De rechter kan bijvoorbeeld de verantwoordelijke gebieden bepaalde gegevens uit zijn computersystemen te verwijderen (www.cbpweb.nl).

Informatie over bemiddeling kunt u vinden in het informatieblad ‘Bemiddeling door het College bescherming persoonsgegevens’.

< VORIGE INHOUD VOLGENDE >



5

HET COLLEGE BESCHERMING PERSOONSGEGEVENS

Om te bevorderen dat de privacy van de burger voldoende gewaarborgd blijft en dat de wetten die daartoe zijn vastgelegd worden nageleefd, is in 2001 het College bescherming persoonsgegevens (CBP) ingesteld. Bij de opslag en het gebruik van persoonsgegevens moet de privacy van iedereen voldoende worden gewaarborgd. De belangrijkste regels voor het verwerken van persoonsgegevens zijn vastgelegd in de Wet bescherming persoonsgegevens (WBP). Deze wet regelt ook het functioneren van het CBP.

Het College heeft ervoor gekozen de bescherming van persoonsgegevens langs vier sporen te bevorderen: bewustwording, normontwikkeling, technologie en handhaving. Door voorlichting en communicatie met uiteenlopende doelgroepen probeert het CBP het privacybewustzijn te versterken en de normen onder de aandacht te brengen. In studies, maar ook in de adviezen die het College uitbrengt, wordt bijgedragen aan de normontwikkeling op bestaande en nieuwe terreinen. In dit kader stimuleert het College ook zelfregulering door branches of sectoren. Door onderzoek te doen naar ontwikkelingen en toepassingen van informatie- en communicatietechnologie probeert het CBP de kritieke momenten in beeld te brengen en aan te geven hoe de normen voor gegevensbescherming in de techniek een vertaling kunnen vinden. Het sluitstuk vormt de doorwerking van de privacybescherming in de praktijk. Door privacyaudits en andere vormen van handhaving wordt deze doorwerking bevorderd.

5.1 Bewustwording

In de voorlichting van het CBP staat de internetsite centraal. Op deze manier is informatie voor een breed publiek toegankelijk. Op de internetsite zijn per thema onder andere wetteksten, publicaties, uitspraken en veel voorkomende vragen te vinden. Het publiek kan verder gebruik maken van de expertise van de medewerkers van het CBP door telefonisch of schriftelijk vragen voor te leggen. Daarnaast worden bijeenkomsten georganiseerd en verzorgen medewerkers lezingen en artikelen in vakbladen. Ook journalisten benaderen het CBP: ze zijn op zoek naar meer achtergrondinformatie of vragen naar een standpunt. Het CBP doet tenslotte onderzoek naar nieuwe vraagstukken op het gebied van privacybescherming. De uitkomsten van dergelijke onderzoeken worden vaak in studies van het CBP gepubliceerd.

5.2 Normontwikkeling

Het CBP heeft mede de taak bij te dragen aan de ontwikkeling en concretisering van bestaande en nieuwe normen die de persoonlijke levenssfeer beschermen tegen inbreuken bij de verwerking van persoonsgegevens.

Advisering aan de regering

Het CBP adviseert de regering gevraagd en ongevraagd over de uitvoering van de WBP en over andere onderwerpen waarbij de privacy van de burger in het geding is.

Zo is aan de regering advies uitgebracht over de nieuwe uitvoeringsstructuur van de sociale zekerheid (Structuur Uitvoering Werk en Inkomen, SUWI II). Hierin is onder andere aangedrongen op het formuleren van heldere bepalingen aangaande de informatie-uitwisseling. Het advies over de invoering van het persoonsgebonden nummer in het onderwijs heeft er toe geleid dat er wordt voorzien in adequate waarborgen die misbruik en oneigenlijk gebruik van de betrokken

< VORIGE | INHOUD | VOLGENDE >

persoonsgegevens voorkomen en die verdere uitwaaiering van het sofi-nummer kunnen tegengaan.

Toetsing gedragscodes
Het CBP kan gedragscodes beoordelen waarin de algemene regels van de WBP nader worden uitgewerkt voor het gebruik van persoonsgegevens binnen een bepaalde sector, beroepsgroep of branche, zoals het verzekeringsbedrijf of de banken. Een gedragscode kan ook aanvullende regels bevatten over bijvoorbeeld de behandeling van klachten over inzage- en correctieverzoeken. De branche of sector kan het College verzoeken te verklaren dat de regels in de gedragscode een juiste uitwerking zijn van de wettelijke bepalingen betreffende de verwerking van persoonsgegevens.

Normatieve kaders
Bij het uitoefenen van zijn taak signaleert het CBP regelmatig dat er in de maatschappij behoefte bestaat aan meer duidelijkheid over de omgang met persoonsgegevens in concrete situaties. In publicaties geeft het CBP invulling aan de voor een specifiek onderwerp relevante privacyregels.

Zo zijn er in de studie *Goed werken in netwerken* vuistregels vastgelegd voor het gebruik van e-mail en internet op de werkplek. Verder zijn er onderzoeksrapporten over screening door de politie, de zorg voor gegevens bij medische indicatiestelling en het verzamelen en verstrekken van gegevens door een handelsinformatiebureau.

5.3 Technologie

Door de technologische ontwikkeling kunnen organisaties omvangrijke hoeveelheden persoonsgegevens verwerken (zoals verzamelen, registreren, analyseren en gebruiken voor verschillende doeleinden). Het wordt steeds eenvoudiger gegevensbestanden te koppelen. Op deze wijze kunnen op het eerste gezicht relatief onschuldige persoonsgegevens een andere betekenis krijgen.

Beveiliging van persoonsgegevens
De WBP verplicht de verantwoordelijke om gegevensverwerkingen te beveiligen. Deze moet passende technische en organisatorische maatregelen nemen om het verlies van gegevens of onrechtmatige verwerkingen tegen te gaan. Dit kan bijvoorbeeld door middel van wachtwoordbeveiliging op de computer, toegangsbeveiliging of het gebruik van firewalls bij koppeling van het systeem met het internet.

Maar de technologische ontwikkelingen vormen zeker niet alleen bedreigingen maar bieden ook kansen voor de privacybescherming. Inzicht in de risico's bij verwerking van persoonsgegevens door middel van informatietechnologie en de mogelijkheden van de technologie dragen bij tot een goed niveau van bescherming van persoonsgegevens binnen organisaties.

Privacy-Enhancing Technologies
Privacy-Enhancing Technologies (PET) kunnen een belangrijk hulpmiddel zijn om een behoorlijke en zorgvuldige omgang met persoonsgegevens te waarborgen en de werking van de privacybeginselen te realiseren. PET is gedefinieerd als een samenhangend geheel van maatregelen dat de persoonlijke levenssfeer beschermt door het elimineren of verminderen van persoonsgegevens of door het voorkomen van onnodige dan wel ongewenste verwerking van persoonsgegevens, een en ander zonder verlies van de functionaliteit van het informatiesysteem. De toepassing van deze technologie is in artikel 13 WBP verankerd en heeft inmiddels een belangrijke plaats verworven in het praktisch en theoretisch repertoire van privacybeschermende middelen.

5.4 Handhaving

Het College bescherming persoonsgegevens is primair ingesteld om toezicht te houden op de naleving van de privacywetgeving en de bescherming van persoonsgegevens in het algemeen. Het College ziet in dat kader ook toe op de doorwerking van de gestelde normen in de praktijk. Daarnaast kan er binnen een organisatie of branche ook toezicht worden gehouden door een functionaris voor de gegevensbescherming.

Functionaris voor de gegevensbescherming
De WBP biedt organisaties – in zowel de publieke als de private sector - de mogelijkheid om een functionaris voor de gegevensbescherming aan te stellen. Deze houdt binnen de organisatie toezicht op de verwerking van persoonsgegevens en daarmee op de toepassing en naleving van de WBP. Meldingen van verwerkingen van persoonsgegevens kunnen

< VORIGE | INHOUD | VOLGENDE >

bij deze functionaris worden gedaan. Tevens is hij een deskundig aanspreekpunt voor de verantwoordelijke. Ook kan hij als contactpersoon optreden voor de personen over wie persoonsgegevens worden verwerkt: klanten, personeelsleden en burgers.

Benoeming van zo'n functionaris zal ertoe leiden dat het CBP zich als nationale toezichthouder terughoudend opstelt ten aanzien van organisaties waarin een functionaris voor de gegevensbescherming naar behoren werkzaam is.

Als nationale toezichthouder staan het College bescherming persoonsgegevens verschillende handhavingsmiddelen ten dienste.

Melding

Personen of instanties die persoonsgegevens verwerken zijn in principe verplicht dat te melden bij het CBP. De gegevensverwerking wordt gemeld via het WBP-Meldingsformulier of door middel van het WBP-Meldingsprogramma. In beide gevallen moeten daarbij bepaalde gegevens worden verstrekt over de verwerking, zoals het doel, de categorieën van betrokkenen en de categorieën van gegevens. De meldingsprocedure is kosteloos. De meldingsplicht geldt niet voor alle verwerkingen. In het Vrijstellingsbesluit is vastgelegd voor welke typen verwerkingen een vrijstelling geldt en onder welke voorwaarden. De WBP blijft overigens wel van toepassing op verwerkingen die zijn vrijgesteld van melding.

Audits

Het CBP stimuleert zelfregulering door organisaties die persoonsgegevens verwerken. De bescherming van persoonsgegevens is een verantwoordelijkheid voor alle organisaties die met persoonsgegevens omgaan. In dit kader heeft het CBP in een samenwerkingsverband met audit- en adviesorganisaties, koepelorganisaties van auditors, werknemers-, werkgevers- en consumentenorganisaties en de ministeries van Justitie en Binnenlandse Zaken en Koninkrijksrelaties een aantal auditproducten ontwikkeld:

- De Quickscan: een beknopte vragenlijst waarmee men binnen een organisatie snel inzicht krijgt in de mate waarin men zich bewust is van de stand van zaken rond de bescherming van persoonsgegevens.
- De WBP Zelfevaluatie: waarmee een organisatie zelfstandig en in betrekkelijk korte tijd de kwaliteit van de maatregelen voor de bescherming en beveiliging van persoonsgegevens kan beoordelen.
- Het Raamwerk Privacy Audit: een kader voor het opstellen van een werkplan voor het uitvoeren van een Privacy Audit door een (privacy)deskundige auditor.

Via deze producten kunnen organisaties zelf nagaan hoe het met de bescherming van persoonsgegevens in hun organisatie is gesteld. De Quickscan treft u als bijlage bij deze folder aan.

Geschillenoplossing

Het CBP bemiddelt bij geschillen over het uitoefenen van rechten. Reageert de verantwoordelijke niet op bijvoorbeeld een inzageverzoek of is de betrokkene niet tevreden met de reactie, dan kan de betrokkene een verzoek om bemiddeling indienen bij het CBP. Bij behandeling van het verzoek past het CBP het beginsel van hoor en wederhoor toe: beide partijen krijgen de gelegenheid om hun standpunt nader toe te lichten. Aan de behandeling van een verzoek door het CBP zijn geen kosten verbonden. Het CBP beëindigt doorgaans de bemiddeling als u tevreden bent met de uitkomst bijvoorbeeld doordat u inzage in uw gegevens heeft gekregen of als uw gegevens zijn verbeterd of verwijderd. Informatie over uw rechten met betrekking tot uw persoonsgegevens bij de politie staat in de brochure *Wet politieregisters, uw gegevens bij de politie.*

Geschillen kunnen ook worden voorgelegd aan de rechter. De rechter kan in dergelijke gevallen advies vragen aan het CBP.

Indien men meent schade te hebben geleden doordat de verantwoordelijke bepaalde verplichtingen niet nakomt, dan moet men naar de rechter stappen: het College is niet bevoegd om schadevergoeding vast te stellen.

Onderzoeken

Op eigen initiatief of op verzoek van een belanghebbende kan het CBP een onderzoek instellen om te bepalen of de verwerking van persoonsgegevens in overeenstemming is met de wet. Het CBP heeft voor het doen van zo'n onderzoek bijzondere bevoegdheden: de verantwoordelijke moet inlichtingen geven en alle overige medewerking verlenen. Een onderzoek van het CBP kan leiden tot een openbaar rapport. Een dergelijk onderzoek heeft bijvoorbeeld geleid tot het rapport *Klant in het web: privacywaarborgen voor internettoegang*, een onderzoek naar de

< VORIGE | INHOUD | VOLGENDE >

wijze waarop internetproviders persoonsgegevens verzamelen en verder gebruiken.

Voorafgaand onderzoek

Als een verantwoordelijke een gegevensverwerking meldt bij het CBP waarop een voorafgaand onderzoek van toepassing kan zijn, verricht het College een voorbereidend onderzoek dat maximaal vier weken kan duren. Na deze periode ontvangt de verantwoordelijke het besluit van het CBP al dan niet tot nader onderzoek over te gaan. Een voorafgaand onderzoek kan ingesteld worden indien:

- de verantwoordelijke een nummer ter identificatie van personen voor andere doeleinden wil gebruiken dan waarvoor het nummer specifiek bestemd is. Met dit nummer kunnen gegevens in verband worden gebracht met gegevens die door een andere verantwoordelijke worden gebruikt. Denk hierbij aan het sofi-nummer;
- de verantwoordelijke gegevens wil vastleggen op grond van eigen waarneming zonder de betrokkene hiervan op de hoogte te brengen;
- de verantwoordelijke, zonder een specifieke vergunning daartoe, strafrechtelijke gegevens of gegevens over onrechtmatig of hinderlijk gedrag wil verwerken ten behoeve van derden.

Boete en bestuursdwang

In een aantal gevallen kan het CBP een boete opleggen van ten hoogste 4.540 euro, namelijk als:

- de verantwoordelijke de gegevensverwerking niet heeft gemeld;
- de gegevensverwerking onjuist of onvolledig is gemeld;
- wijzigingen in de melding niet (tijdig) zijn doorgegeven;
- van de melding afwijkende verwerkingen niet bewaard zijn.

Als een verantwoordelijke één of meer bepalingen van de WBP of de daarop gebaseerde regelingen overtreedt, kan het College bescherming persoonsgegevens na onderzoek bestuursdwang toepassen. Bestuursdwang houdt in dat de verantwoordelijke een termijn krijgt om zijn verplichtingen na te komen. Laat hij dat na, dan kan het CBP zelf op kosten van de verantwoordelijke het gewenste resultaat tot stand doen brengen.

Het CBP kan ook kiezen om een dwangsom op te leggen. Het College kan de verantwoordelijke dan gelasten bepaalde gegevensverwerkingen te beëindigen of herhaling daarvan te voorkomen, op straffe van een dwangsom voor iedere dag dat de verantwoordelijke hieraan niet voldoet.

Bij de uitvoering van deze bevoegdheden is het College gehouden aan de normen die worden gesteld in de Algemene Wet Bestuursrecht. Als de verantwoordelijke bijvoorbeeld wordt geconfronteerd met een boete, dan kan hij bezwaar en beroep aantekenen.

Nationale Ombudsman

Iedereen heeft verder het recht een schriftelijk verzoek bij de Nationale ombudsman in te dienen om een onderzoek in te stellen naar het handelen van het College bescherming persoonsgegevens. Dit moet gebeuren binnen een jaar nadat een bepaalde aangelegenheid zich heeft voorgedaan. Voordat de verzoeker een klacht indient bij de Nationale ombudsman moet hij eerst de klacht voorleggen aan het CBP.

< VORIGE | INHOUD | VOLGENDE >

6 INTERNATIONALE TAKEN

Het College bescherming persoonsgegevens neemt deel aan diverse vormen van internationale samenwerking. Alle landen van de Europese Unie en een aantal daarbuiten kennen een instelling vergelijkbaar met het CBP. Het College onderhoudt contacten en werkt waar nodig samen met deze zusterorganisaties.

Een andere taak voor het CBP ligt in het zogenaamde Verdrag van Straatsburg (28 januari 1981) inzake gegevensbescherming. Het doel van dit verdrag is de bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens. Het College vertegenwoordigt Nederland bij de uitvoering van het verdrag en verleent rechtshulp aan personen en instanties uit het buitenland.

Ook neemt het CBP deel aan het gemeenschappelijk toezicht op de verwerking van persoonsgegevens door de politie in het kader van het Verdrag van Schengen en de organisatie Europol.

BIJLAGE: MODELBRIEVEN

< VORIGE | INHOUD | VOLGENDE >

Modelbrief A

Een schriftelijk verzoek om inzage kan er als volgt uit zien:

Datum

Geachte,

Met verwijzing naar artikel 35 van de Wet bescherming persoonsgegevens wil ik graag binnen vier weken van u weten of u mijn gegevens verwerkt. Als dat het geval is, verzoek ik u mij binnen vier weken een overzicht van de gegevens te geven. Ik verzoek u ook inlichtingen te verstrekken over het doel van de verwerking(en), de ontvangers van de gegevens en over de herkomst van de gegevens.

Als u met het oog op de vaststelling van mijn identiteit behoefte heeft aan een kopie van een rijbewijs, paspoort of ander identiteitsbewijs, ben ik bereid u deze te verstrekken.

Hoogachtend,

Naam
Geboortedatum
Adres
Postcode en woonplaats

Modelbrief B

Een schriftelijk verzoek om verbetering, aanvulling, verwijdering of afscherming van gegevens kan er als volgt uit zien:

Datum

Geachte,

Met verwijzing naar artikel 36 van de Wet bescherming persoonsgegevens, wil ik graag verbetering/aanvulling/verwijdering/afscherming van mijn gegevens[1].

Ik wens de volgende aanpassingen in mijn gegevens:
–
–

Ik verzoek u mij binnen vier weken schriftelijk te berichten of dan wel in hoeverre u aan mijn verzoek voldoet. Als u aan mijn verzoek hebt voldaan, dient u zo spoedig mogelijk de aanpassingen door te geven aan derden aan wie u mijn gegevens hebt verstrekt.

Als u met het oog op de vaststelling van mijn identiteit behoefte heeft aan een kopie van een rijbewijs, paspoort of ander identiteitsbewijs, ben ik bereid u deze te verstrekken.

Hoogachtend,

Naam
Geboortedatum
Adres
Postcode en woonplaats

[1] U kunt om verbetering, aanvulling, verwijdering en/of afscherming vragen. Geef duidelijk aan wat u wenst.

< VORIGE INHOUD VOLGENDE >

Modelbrief C

Het schriftelijk aantekenen van verzet kan als volgt:

Datum

Geachte,

Met verwijzing naar artikel 40 van de Wet bescherming persoonsgegevens, maak ik bezwaar tegen de verwerking van mijn gegevens in [beschrijf hier om welke verwerking het gaat]. Aan dit bezwaar liggen de volgende bijzondere persoonlijke omstandigheden ten grondslag:
-
-

Ik verzoek u de verwerking te beëindigen.

Hoogachtend,

Naam
Geboortedatum
Adres
Postcode en woonplaats

Modelbrief D

Het schriftelijk aantekenen van absoluut verzet kan als volgt:

Datum

Geachte,

Met verwijzing naar artikel 41 van de Wet bescherming persoonsgegevens, teken ik verzet aan tegen de verwerking van mijn gegevens voor commerciële of charitatieve doeleinden. Ik verzoek u de verwerking direct te beëindigen.

Hoogachtend,

Naam
Geboortedatum
Adres
Postcode en woonplaats

BIJLAGE: QUICKSCAN BESCHERMING PERSOONSGEGEVENS

BIJLAGE: QUICKSCAN BESCHERMING PERSOONSGEGEVENS

Wet bescherming persoonsgegevens

De privacybescherming in Nederland wordt sinds 2001 geregeld in de Wet bescherming persoonsgegevens (WBP). Deze wet, als opvolger van de Wet Persoonsregistraties (WPR), stelt eisen aan de wijze waarop organisaties persoonsgegevens verwerken. Vrijwel elke organisatie in Nederland doet dat en heeft dus te maken met de WBP. De eisen in de WBP zijn veranderd en uitgebreid ten opzichte van de WPR. Dit betekent dat als uw organisatie voldoet aan de wettelijke bepalingen van de WPR dit niet zonder meer betekent dat zij voldoet aan alle WBP-bepalingen. Het College bescherming persoonsgegevens (CBP) is als opvolger van de Registratiekamer belast met het toezicht op de naleving van de WBP.

Doel van de Quickscan

Als u vindt dat personeelsleden, klanten, debiteuren, bezoekers en andere relaties vertrouwen moeten hebben in uw organisatie dan moet uw organisatie dat vertrouwen verdienen en vervolgens waarmaken. Een zorgvuldige verwerking van persoonsgegevens draagt bij aan dit vertrouwen. Het is daarom belangrijk vast te stellen hoe uw organisatie persoonsgegevens verwerkt. Een eerste stap hierbij is het creëren van voldoende bewustzijn over het belang van de zorgvuldige omgang met persoonsgegevens binnen uw organisatie. Om het proces van bewustwording te stimuleren, is een korte privacyvragenlijst opgesteld. De uitkomsten van deze vragenlijst geven een globale indruk hoe het met de privacybescherming binnen uw organisatie is gesteld. De uitkomsten van de vragenlijst zijn nuttig voor de leiding van de organisatie die verantwoordelijk is voor de naleving van de privacywetgeving, maar ook voor de ondernemingsraad en, indien benoemd, de functionaris voor de gegevensbescherming. Ook in werkoverleg kan aandacht besteed worden aan de uitkomsten van deze vragenlijst.
Let op: De vragenlijst is beknopt en gaat niet in op alle aspecten van de bescherming van persoonsgegevens, zoals die in de WBP zijn geregeld.

Hoe werkt de vragenlijst?

Elke medewerker in een organisatie kan de vragenlijst zelfstandig invullen. De vragenlijst bestaat uit dertien vragen. U kunt de vragen beantwoorden met ‘ja’ of ‘nee’. Door een vraag met ‘ja’ te beantwoorden, geeft u aan dat uw organisatie aandacht heeft voor het onderwerp van die vraag. Of er in voldoende mate en op de juiste wijze aandacht wordt besteed, kan pas worden gezegd na gericht onderzoek. Indien u ‘nee’ heeft geantwoord dan vraagt het betreffende onderwerp om nadere aandacht binnen uw organisatie. Mogelijk schiet uw organisatie tekort in het naleven van de wettelijke bepalingen. Op welke wijze de organisatie hier vervolg aan kan geven, vraagt eveneens om meer gericht onderzoek.

Op de website van het CBP (www.cbpweb.nl) vindt u per vraag een toelichting op de antwoordmogelijkheden van deze vragenlijst. Via deze toelichting kunt u zelf de voor uw organisatie beste vervolgstap bepalen.

Vervolgstap

Na het bekend worden van de uitkomsten van de vragenlijst kan de organisatie een gericht onderzoek uitvoeren naar de concrete invulling van de privacyeisen binnen de organisatie. Daarvoor is in eerste instantie een uitgebreide WBP Zelfevaluatie te verkrijgen. Via deze zelfevaluatie kunnen medewerkers van uw organisatie zelfstandig de kwaliteit van de maatregelen ter bescherming van persoonsgegevens beoordelen en nagaan op welke gebieden noodzakelijke maatregelen ontbreken of ontoereikend zijn. Daarmee vergroot u het vertrouwen van relaties in de zorgvuldige omgang met persoonsgegevens binnen uw organisatie.

Meer informatie?

Mocht u meer informatie willen over deze Quickscan of over het omgaan met persoonsgegevens in het algemeen dan kunt u de internetsite van het College bescherming persoonsgegevens (www.cbpweb.nl) raadplegen. Via deze website kunt u ook de WBP Zelfevaluatie downloaden. Op de website treft u ook het Raamwerk Privacy Audit aan. Op basis van dit raamwerk kan een interne of externe auditor een gedetailleerd onderzoek uitvoeren naar de wijze waarop en de mate waarin uw organisatie omgaat met de bescherming van persoonsgegevens. Ook kunt u tussen 09.00 en 12.30 uur bellen met een adviseur van het CBP via tel. (070) 381 13 00. U kunt ook faxen (070) 381 13 01 of e-mailen: info@cbpweb.nl.

Van wie is de vragenlijst afkomstig?

De vragenlijst is ontwikkeld in een samenwerkingsverband bestaande uit het CBP, diverse koepelorganisaties en verschillende marktpartijen van audit- en adviesorganisaties.

< VORIGE | INHOUD | VOLGENDE >

QUICKSCAN VRAGENLIJST

Het is mogelijk dat u geen zicht heeft op de totale organisatie waarin u werkzaam bent. In dat geval kunt u voor onderstaande vragen voor het woord organisatie ook de afdeling lezen waarin u werkzaam bent.

Privacybewustzijn in de organisatie
Voor het realiseren van een goede bescherming van de persoonsgegevens in een organisatie is privacybewustzijn en het proces van privacybewustwording van belang.

1 Is in uw bedrijf voorlichting gegeven over de nieuwe privacywet (WBP)? ☐ Ja ☐ Nee
2 Heeft de directie of leiding uitgesproken dat de organisatie de privacy van personen moet respecteren? ☐ Ja ☐ Nee

De directie of leiding van een organisatie kan op verschillende manieren de privacy bij haar medewerkers onder de aandacht brengen. Daarbij kan gedacht worden aan: informatiesessies over privacy, een privacyrichtlijn voor medewerkers, specifieke acties en maatregelen ter bescherming van de privacy.

3 Wordt er op uitvoerend niveau binnen uw organisatie aandacht besteed aan privacybescherming? ☐ Ja ☐ Nee

Uitvoering wettelijke bepalingen
Onder het verwerken van persoonsgegevens wordt onder meer verstaan het, zowel geautomatiseerd als handmatig, verzamelen, vastleggen, bewerken, bewaren, verstrekken, verwijderen en vernietigen van persoonsgegevens door organisaties.
De wet beperkt het verwerken van persoonsgegevens tot de doelstelling(en) waarvoor ze verzameld zijn, zoals door de organisatie vooraf geformuleerd, en doelstellingen die daarmee verenigbaar zijn.

4 Beperkt uw organisatie het verwerken van persoonsgegevens tot de doelstelling(en) waarvoor ze verzameld zijn en doelstellingen die daarmee verenigbaar zijn? ☐ Ja ☐ Nee

Het verwerken van persoonsgegevens kan uitsluitend plaatsvinden als daarvoor een rechtmatige grondslag aanwezig is. De WBP geeft aan op welke gronden verwerking toegestaan is.

5 Vindt het verwerken van persoonsgegevens binnen uw organisatie plaats in overeenstemming met de grondslagen van de WBP? ☐ Ja ☐ Nee

Persoonsgegevens moeten in overeenstemming met de wet en op een behoorlijke en zorgvuldige wijze worden verwerkt.

6 Zijn er regels vastgesteld voor het verwerken van persoonsgegevens binnen uw organisatie? ☐ Ja ☐ Nee

De wet stelt strengere eisen aan de verwerking van bijzondere persoonsgegevens. Dit betreft gegevens over: godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en strafrechtelijke gegevens.

7 Zijn er specifieke regels vastgesteld voor het verwerken van bijzondere persoonsgegevens binnen uw organisatie? ☐ Ja ☐ Nee

Voor een zorgvuldige verwerking moeten de persoonsgegevens die in uw organisatie worden verwerkt, correct zijn.

8 Controleert uw organisatie persoonsgegevens op juistheid en volledigheid? ☐ Ja ☐ Nee

De WBP legt organisaties die persoonsgegevens verwerken een informatieplicht op. Daardoor weten de personen (betrokkenen) van wie persoonsgegevens worden verwerkt hoe de organisatie met hun persoonsgegevens omgaat.

9 Leeft uw organisatie de informatieplicht naar betrokkenen na? ☐ Ja ☐ Nee

De WBP kent aan personen (betrokkenen) van wie persoonsgegevens worden verwerkt bepaalde rechten toe. Dit betreft het recht tot inzage, wijziging en verwijdering van persoonsgegevens en het recht op verzet tegen het verwerken van persoonsgegevens.

10 Komt uw organisatie de rechten van betrokkenen na? ☐ Ja ☐ Nee

Beveiliging
Persoonsgegevens moeten in overeenstemming met de wet en op een behoorlijke en zorgvuldige wijze worden verwerkt. Dit betekent dat niet iedereen in een organisatie toegang mag hebben tot persoonsgegevens of deze mag bewerken, verstrekken of verwijderen.

11 Heeft uw organisatie bevoegdheden aan medewerkers toegekend zodat uitsluitend geautoriseerde medewerkers ☐ Ja ☐ Nee

< VORIGE INHOUD VOLGENDE >

toegang hebben tot persoonsgegevens?
De WBP stelt dat een organisatie passende technische en organisatorische maatregelen moet treffen om persoonsgegevens te beveiligen tegen verlies of onrechtmatige verwerking, met inbegrip van onnodige verwerking.

12 Heeft uw organisatie maatregelen getroffen die verlies en onrechtmatige verwerking van persoonsgegevens tegengaan? ☐ Ja ☐ Nee

Controle
Controle op de naleving van de maatregelen die de organisatie getroffen heeft, bij de onderwerpen van de vragen 4 tot en met 12, is belangrijk voor een goede bescherming van de persoonsgegevens.

13 Wordt de naleving van de maatregelen voor privacybescherming binnen uw organisatie van tijd tot tijd gecontroleerd? ☐ Ja ☐ Nee

COLLEGE BESCHERMING PERSOONSGEGEVENS

Het College bescherming persoonsgegevens (CBP) – onder de Wet bescherming persoonsgegevens (WBP) de opvolger van de Registratiekamer – houdt toezicht op de naleving van wetten die het gebruik van persoonsgegevens regelen. Bij het CBP moet het gebruik van persoonsgegevens worden gemeld, tenzij hiervoor een vrijstelling geldt.

Advies, bemiddeling, onderzoek en interventie
Het CBP adviseert de regering en organisaties over de bescherming van persoonsgegevens en onderwerpen die daarmee samenhangen. Het CBP toetst gedragscodes en bemiddelt in geschillen tussen burgers en gebruikers van persoonsgegevens. Op eigen initiatief of op verzoek van een belanghebbende kan het CBP onderzoeken of de manier waarop persoonsgegevens in een bepaalde situatie zijn gebruikt, in overeenstemming is met de wet en daaraan zonodig gevolgen verbinden. Voor in gebreke blijven bij de melding kan een boete worden opgelegd. Bij overtreding van de wet of daarop gebaseerde regelingen kan het CBP overgaan tot bestuursdwang of een dwangsom opleggen.

Over zijn werkzaamheden en bevindingen brengt het CBP jaarlijks een openbaar verslag uit. Het CBP is bij de uitvoering van zijn bevoegdheden gehouden aan de normen die worden gesteld in de Algemene wet bestuursrecht. Beslissingen van het CBP zijn vatbaar voor bezwaar en beroep. Het gedrag van het CBP kan onderzocht worden door de Nationale Ombudsman.

Informatie
Voor meer informatie kunt u kijken op de website: www.cbpweb.nl.
Alle publicaties kunt u via de website bestellen of elektronisch binnenhalen; telefonisch bestellen is ook mogelijk. Voor eerste advies kunt u gebruik maken van het telefonisch spreekuur, op werkdagen van 9.00 – 12.30 uur, telefoon 070 381 13 00.

< VORIGE INHOUD VOLGENDE >