



Algemene privacyregeling Veiligheidsregio Utrecht

Algemene privacyregeling Veiligheidsregio Utrecht, zoals vastgesteld door het algemeen bestuur van de Veiligheidsregio Utrecht op 13 december 2013

Het algemeen bestuur van de Veiligheidsregio Utrecht;

gelet op,

het bepaalde in artikel 160 Gemeentewet, artikel 8.1 Gemeenschappelijke Regeling Veiligheidsregio Utrecht 2010, alsmede artikel 28 lid 3 Organisatieregeling Veiligheidsregio Utrecht 2010 en op grond van de Wet bescherming persoonsgegevens (Stbl. 2000, 302) en de daarmee samenhangende wet- en regelgeving;

overwegende dat;

de Veiligheidsregio Utrecht persoonsgegevens van medewerkers alsmede persoonsgegevens van burgers en bedrijven verwerkt in de voorbereiding op rampen en crises en bestrijding van brand;

de Veiligheidsregio Utrecht ten tijde van een ramp of crises of in de uitvoering van haar reguliere hulpverleningstaken persoonsgegevens en slachtoffergegevens verwerkt;

het van belang is dat persoonsgegevens door de Veiligheidsregio Utrecht op transparante wijze worden verwerkt;

de verwerking voldoet aan de wettelijke kaders, alsmede de eisen die de Veiligheidsregio Utrecht daar zelf aan stelt;

het daarom van belang is om een privacyregeling vast te stellen dat duidelijkheid en kaders schept voor de verwerking van persoonsgegevens binnen de Veiligheidsregio Utrecht;

besluit:

Vast te stellen het volgende:

Algemene regeling voor de omgang met persoonsgegevens binnen de Veiligheidsregio Utrecht;

§ 1 ALGEMENE BEPALINGEN

Artikel 1 Begripsbepalingen

In deze regeling wordt in aansluiting bij en in aanvulling op de Wet bescherming persoonsgegevens verstaan onder:

- a. wet: Wet bescherming persoonsgegevens;
- b. VRU: Veiligheidsregio Utrecht;
- c. bestand: elk gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen;
- d. betrokkene: degene op wie een persoonsgegeven betrekking heeft of zijn vertegenwoordiger;

- e. Cbp: College bescherming persoonsgegevens, het College als bedoeld in artikel 51 van de wet;
- f. beheerder: degene onder verantwoordelijkheid van de verantwoordelijke die is belast met de dagelijkse zorg voor de verwerking van persoonsgegevens, voor de juistheid van de ingevoerde gegevens, alsmede voor het bewaren, verwijderen, dan wel van enigerlei uitvoer van de verwerking kennis te nemen;
- g. bewerker: degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen;
- h. derde: ieder, niet zijnde de betrokkene, de verantwoordelijke, de bewerker, of enig persoon die onder rechtstreeks gezag van de verantwoordelijke of de bewerker gemachtigd is om persoonsgegevens te verwerken;
- i. persoonsgegeven: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon in de zin van de wet;
- j. regeling: Algemene privacyregeling Veiligheidsregio Utrecht;
- k. verantwoordelijke: het bestuursorgaan dat of namens wie de doelen van en de middelen voor de verwerking van persoonsgegevens worden vastgesteld, zijnde het algemeen bestuur van de VRU;
- l. verwerking van persoonsgegevens: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.

Artikel 2 Doel

Deze regeling heeft tot doel een kader te scheppen waarbinnen de verschillende verwerkingen van persoonsgegevens binnen de gehele VRU op eenduidige en rechtmatige wijze plaatsvinden.

Artikel 3 Reikwijdte

1. Deze regeling is van toepassing binnen de VRU en heeft betrekking op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede de niet geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.
2. De doeleinden en overige kenmerken van de verwerkingen van persoonsgegevens in de VRU, worden per verwerking vastgesteld en vastgelegd, voor zover dat voor die kenmerken is bepaald in deze regeling. Het vastleggen vindt door of namens het dagelijks bestuur van de VRU plaats.
3. Het dagelijks bestuur van de VRU stelt een Uitvoeringsregister vast. Het Uitvoeringsregister vat ten aanzien van de vastgelegde gegevensverwerkingen binnen de VRU, zoals bedoeld onder het voorgaande lid, samen wat de doeleinden zijn, wat de verwerkte gegevens zijn en de overige kenmerken van de verwerking, voor zover dat in deze regeling wordt bepaald.

§ 2 VERWERKING VAN PERSOONSGEGEVENS

Artikel 4 De verwerking van persoonsgegevens in het algemeen

1. Persoonsgegevens worden in overeenstemming met deze regeling op behoorlijke en zorgvuldige wijze verwerkt en alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. De doeleinden worden verzameld in het Uitvoeringsregister dat op grond van deze regeling is vastgesteld.
2. Persoonsgegevens worden niet verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen.
3. Persoonsgegevens worden slechts verwerkt voor zover zij, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, toereikend, ter zake dienend en niet bovenmatig zijn.

Artikel 5 Voorwaarden verwerking van persoonsgegevens in het algemeen

Persoonsgegevens mogen slechts worden verwerkt indien:

- a. de betrokkene voor de verwerking zijn ondubbelzinnige toestemming heeft verleend;
- b. dit noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of voor handelingen die op verzoek van de betrokkene worden verricht en die noodzakelijk zijn voor het sluiten van een overeenkomst;
- c. dit noodzakelijk is om een wettelijke verplichting na te komen waaraan de verantwoordelijke onderworpen is;
- d. de gegevensverwerking noodzakelijk is ter vrijwaring van een vitaal belang van de betrokkene;
- e. de gegevensverwerking noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door de VRU, of;
- f. de gegevensverwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert.

Artikel 6 De verwerking van bijzondere persoonsgegevens

1. Het verbod om persoonsgegevens te verwerken als bedoeld in artikel 16 van de wet, is niet van toepassing indien de verwerking geschiedt door de VRU voor zover dat met het oog op het beheer van de organisatie noodzakelijk is.
2. In de gevallen als bedoeld in het eerste lid worden de gegevens alleen verwerkt door personen die uit hoofde van ambt, beroep of wettelijk voorschrift, dan wel krachtens een overeenkomst tot geheimhouding zijn verplicht.
3. Indien de verantwoordelijke gegevens persoonlijk verwerkt en op hem niet reeds uit hoofde van ambt, beroep of wettelijk voorschrift een geheimhoudingsplicht rust, is hij verplicht tot geheimhouding van de gegevens, behoudens voor zover de wet hem tot mededeling verplicht of uit zijn taak de noodzaak voortvloeit dat de gegevens worden meegedeeld aan anderen die krachtens het eerste lid bevoegd zijn tot verwerking daarvan.

Artikel 7 Voorwaarden verwerking van bijzondere persoonsgegevens

Onverminderd artikel 6 van deze regeling is het verbod om persoonsgegevens als bedoeld in artikel 16 van de wet, te verwerken niet van toepassing voor zover:

- a. dit geschiedt met expliciete en uitdrukkelijke toestemming van de betrokkene;
- b. de gegevens door de betrokkene duidelijk openbaar zijn gemaakt;
- c. dit noodzakelijk is voor de vaststelling, de uitoefening of de verdediging van een recht in rechte;
- d. dit noodzakelijk is ter verdediging van de vitale belangen van de betrokkene of van een derde en het vragen van diens uitdrukkelijke toestemming onmogelijk blijkt;
- e. dit noodzakelijk is ter voldoening aan een volkenrechtelijke verplichting; of
- f. dit noodzakelijk is met het oog op een zwaarwegend algemeen belang, passende waarborgen worden geboden ter bescherming van de persoonlijke levenssfeer en dit bij wet wordt bepaald dan wel het Cbp ontheffing heeft verleend. Het Cbp kan bij de verlening van ontheffing beperkingen en voorschriften opleggen;
- g. de gegevens worden verwerkt door het Cbp of een Ombudsman als bedoeld in artikel 9:17 van de Algemene wet bestuursrecht en dit noodzakelijk is met het oog op een zwaarwegend algemeen belang, voor de uitvoering van de hun wettelijk opgedragen taken en bij die uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad.

Artikel 8 Verstrekking van persoonsgegevens

Op grond van de doelstelling en de rechtmatige grondslag kunnen door of namens de verantwoordelijke persoonsgegevens worden verstrekt aan derden.

Artikel 9 Verdere verwerking persoonsgegevens

1. De te verwerken persoonsgegevens zullen slechts verder worden verwerkt op een wijze die niet onverenigbaar is met de doeleinden waarvoor ze zijn verkregen. Daarbij zal rekening worden gehouden met de verwantschap van de doeleinden, de aard van de gegevens en de waarborgen ter bescherming van de persoonlijke sfeer.
2. Gegevens mogen verder worden verwerkt indien dat noodzakelijk is om een wettelijke verplichting na te komen waaraan verantwoordelijke onderworpen is of geschiedt met de expliciete en uitdrukkelijke toestemming van de betrokkene.

§ 3 BEVOEGDHEDEN EN Plichten VAN VERANTWOORDELIJKE EN BEHEERDER

Artikel 10 Geheimhoudingsplicht

1. De persoonsgegevens worden alleen verwerkt door personen die uit hoofde van ambt, beroep of wettelijk voorschrift, dan wel krachtens een overeenkomst tot geheimhouding zijn verplicht.
2. Ambtenaren in dienst van de VRU, zijn op grond van artikel 125a, derde lid, Ambtenarenwet, verplicht tot geheimhouding van de persoonsgegevens waarvan zij kennis nemen.

Artikel 11 Melding verwerking persoonsgegevens bij het Cbp

1. Een geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens die voor de verwezenlijking van een doeleinde of samenhangende doeleinden bestemd is, wordt alvorens met de verwerking wordt aangevangen gemeld bij het Cbp.
2. De niet geautomatiseerde verwerking van persoonsgegevens die voor de verwezenlijking van een doeleinde of samenhangende doeleinden bestemd is, wordt gemeld indien deze is onderworpen aan voorafgaand onderzoek.
3. Het eerste lid van dit artikel is niet van toepassing indien er sprake is van een vrijgestelde verwerking van persoonsgegevens als bedoeld in het Vrijstellingsbesluit Wet bescherming persoonsgegevens.
4. In hoeverre binnen de VRU sprake is van een vrijgestelde gegevensverwerking blijkt uit het op grond van deze regeling vastgestelde Uitvoeringsregister.

Artikel 12 Bewaren

1. Persoonsgegevens worden niet langer bewaard dan noodzakelijk is voor de verwezenlijking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt.
2. Persoonsgegevens mogen langer worden bewaard dan noodzakelijk voor de verwezenlijking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, wanneer zij geanonimiseerd worden of voor zover ze uitsluitend voor historische, statistische of wetenschappelijke doeleinden worden bewaard.
3. De verantwoordelijke stelt vast hoelang de in bepaalde bestanden opgenomen persoonsgegevens bewaard blijven. Deze gegevens worden samengevat in het Uitvoeringsregister.

Artikel 13 Verwijdering van verwerkte persoonsgegevens

1. De beheerder verwijdert de persoonsgegevens bij opheffing van de VRU.
2. Een besluit als bedoeld in artikel 10, lid 2, van de wet wordt, al dan niet op verzoek van de beheerder, genomen door de verantwoordelijke.
3. Verwijdering impliceert vernietiging of een zodanige bewerking dat het niet meer mogelijk is de persoon te identificeren.
4. Vernietiging van het bestand of van de daarin opgenomen persoonsgegevens geschiedt met inachtneming van de Archiefwet.

Artikel 14 Rechtstreeks toegang tot de persoonsgegevens

Uitsluitend de beheerder en de door de beheerder aangewezen gebruikers hebben, met het oog op de dagelijkse zorg voor en het goed functioneren van de verwerking, rechtstreeks toegang tot de persoonsgegevens. In welke mate toegang wordt verleend, wordt vastgelegd. Deze informatie wordt samengevat in het Uitvoeringsregister.

Artikel 15 Beveiliging

De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de afstand van de techniek en de kosten van de ten uitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen.

Artikel 16 Bewerker

Indien gebruik wordt gemaakt van de diensten van een bewerker, legt de verantwoordelijke de wederzijdse verplichtingen met betrekking tot de omgang met persoonsgegevens schriftelijk in een overeenkomst met die bewerker vast. De bewerker verwerkt de persoonsgegevens overeenkomstig diens overeengekomen verplichtingen.

§ 4 RECHTEN VAN DE BETROKKENE

Artikel 17 Informatieverstrekking aan de betrokkene

1. Indien bij de betrokkene de persoonsgegevens worden verkregen, deelt de verantwoordelijke voor het moment van verkrijging de betrokkene mede:
 - a. zijn identiteit;
 - b. de doeleinden van de verwerking waarvoor de gegevens zijn bestemd, tenzij de betrokkene daarvan reeds op de hoogte is.
2. De verantwoordelijke verstrekt nadere informatie voor zover dat gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt, nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen.
3. De verantwoordelijke informeert over de rechten van de betrokkene en op welke wijze de betrokkene deze rechten kan inroepen.

Artikel 18 Recht op inzage en afschrift van persoonsgegevens

1. De betrokkene heeft het recht kennis te nemen van de op zijn persoon betrekking hebbende verwerkte gegevens.
2. De gevraagde inzage en/of het gevraagde afschrift zal zo spoedig mogelijk, doch uiterlijk binnen vier weken, plaatsvinden respectievelijk worden verstrekt.
3. Voor de verstrekking van een afschrift mag een redelijke vergoeding in rekening worden gebracht.
4. Recht op inzage of afschrift kan worden geweigerd voor zover dit noodzakelijk is in het belang van de bescherming van de persoonlijke levenssfeer van een ander.

Artikel 19 Recht op aanvulling en correctie van persoonsgegevens

1. Desgevraagd worden de opgenomen persoonsgegevens aangevuld met een door de betrokkene afgegeven verklaring met betrekking tot de opgenomen gegevens.
2. De betrokkene kan verzoeken om correctie van op hem betrekking hebbende gegevens. Dat indien deze feitelijk onjuist, voor het doel van de verwerking onvolledig of niet ter zake dienend zijn, dan wel in strijd met een wettelijk voorschrift, in de verwerking voorkomen.
3. De verantwoordelijke bericht de verzoeker binnen vier weken na ontvangst van het schriftelijk verzoek tot correctie of aanvulling schriftelijk of dan wel in hoeverre hij daaraan voldoet. Een weigering is met redenen omkleed.
4. De verantwoordelijke draagt zorg dat een beslissing tot correctie zo spoedig mogelijk wordt uitgevoerd.

Artikel 20 Recht op verwijdering of vernietiging van persoonsgegevens

1. De betrokkene kan verzoeken om vernietiging van op hem betrekking hebbende gegevens.
2. De verantwoordelijke bericht de verzoeker binnen vier weken na ontvangst van het schriftelijk verzoek tot vernietiging schriftelijk of dan wel in hoeverre hij daaraan voldoet. Een weigering is met redenen omkleed.
3. De verantwoordelijke vernietigt de gegevens binnen drie maanden na een daartoe strekkend verzoek van de betrokkene, tenzij redelijkerwijs aannemelijk is dat de bewaring van aanmerkelijk belang is voor een ander dan de betrokkene, alsmede voor zover bewaring op grond van een wettelijk voorschrift vereist is.

Artikel 21 Klachtenbehandeling

Indien de betrokkene van mening is dat de bepalingen van deze regeling niet worden nageleefd of andere reden tot klagen heeft over de verwerking van zijn persoonsgegevens, kan hij/zij zich wenden tot:

- a. de verantwoordelijke, conform de Klachtenregeling VRU; of
- b. het Cbp.

§ 5 SLOTBEPALINGEN

Artikel 22 Wijziging van deze regeling

1. Wijzigingen van deze regeling worden vastgesteld door het algemeen bestuur.
2. De wijzigingen in de regeling zijn van kracht vier weken nadat ze bekend zijn gemaakt aan betrokkenen.

Artikel 23 Inwerkingtreding en citeertitel

1. Deze regeling treedt in werking, vier weken na haar bekendmaking op de website van de VRU.
2. Deze regeling wordt aangehaald als "*Algemene privacyregeling VRU*".

Vastgesteld in de vergadering van het algemeen bestuur VRU op 13 december 2013

A. Wolfsen
Voorzitter

P.J.L. Bos
Secretaris

TOELICHTING

Toelichting bij paragraaf 1: Algemene bepalingen

De Wet bescherming persoonsgegevens (Wbp) beschermt de privacy van burgers in Nederland. De Wbp regelt in grote mate hoe wordt omgegaan met persoonsgegevens van burgers en welke rechten zij daarbij hebben. Ook binnen een organisatie als de Veiligheidsregio Utrecht (VRU) worden persoonsgegevens verwerkt, want zonder die verwerking kan de VRU geen goede invulling geven aan haar bedrijfsvoering en aan de taken die zij dient uit te voeren op grond van de wet, primair de Wet veiligheidsregio's. Bij het verwerken van persoonsgegevens dient de VRU uiteraard rekening te houden met de Wbp.

Om op een juiste wijze rekening te houden met de Wbp moet een organisatie daar wel het een en ander voor regelen. De vereisten uit de wet vergen wat uitleg en acties binnen een organisatie, dus ook voor de VRU.

Door een algemene privacyregeling vast te stellen, draagt de organisatie uit dat zij de verwerking van persoonsgegevens serieus neemt. Daarnaast wordt het voor verwerkers en betrokkenen binnen de VRU duidelijker wat de toepasselijke regels zijn ten aanzien van het verwerken van persoonsgegevens. Dat bevordert een duidelijke werkwijze op dit vlak.

Zodra duidelijke en algemeen geldende regels voor de organisatie zijn vastgelegd, wordt het mogelijk om in de lijn van de organisatie specifieke of gedetailleerde regels of beschrijvingen vast te stellen. Dat is nodig, omdat persoonsgegevens op verschillende manieren worden verwerkt. Dat komt doordat ze in verschillende systemen zitten en daar zitten die gegevens in met een bepaald doel.

Aan de hand van de Algemene privacyregeling worden vervolgens in meerdere, lager vastgestelde regelingen de doelen van de verschillende verwerkingen vastgelegd. Daar worden ook enkele andere zaken in vastgelegd, bijvoorbeeld de bewaartermijn. Op die manier is voor alle betrokkenen per gegevensverwerking inzichtelijk wat is afgesproken over de die verwerkingen.

Een samenvatting van de belangrijkste punten uit alle lagere regelingen wordt vastgesteld in een apart besluit, een register, zoals bepaald in artikel 3 van deze regeling. Dat besluit heet het Uitvoeringsregister.

Persoonsgegevens

Om een beeld te krijgen waar we in deze regeling over spreken, is het van belang om te weten wat eigenlijk wordt verstaan onder persoonsgegevens. Zoals ook uit de Wbp valt op te maken, omschrijven we persoonsgegevens als volgt:

Persoonsgegevens geven directe of indirecte informatie over een persoon. Deze persoon moet daarbij wel te identificeren zijn.

Wat houdt dit in? Het gaat om elk gegeven, dus niet alleen tekst, maar ook foto's of geluid van een persoon. Ook hier kunnen namelijk persoonsgegevens in staan. Denk aan een foto, die geeft in één oogopslag informatie over ras en geslacht.

De gegevens moeten een persoon betreffen. Dat kan direct of indirect zijn. Bij direct moet men denken aan met naam en toenaam:

- Naam
- Adres
- E-mail
- Dossier met naam erin
- Vingerafdrukken

Vingerafdrukken bevatten weliswaar geen naam, maar het gaat hier toch om gegevens die heel duidelijk horen bij één persoon.

Bij indirecte gegevens gaat het om gegevens die vooral gaan over een zaak, dossier of feiten. Maar die gegevens kunnen wel via een omweg informatie bevatten over een persoon. Denk aan:

- Inkomen
- Beoordeling
- Algemeen verslag

Als die gegevens in verband kunnen worden gebracht met persoon en bepalend zijn voor de manier waarop die persoon vervolgens wordt behandeld of beoordeeld, dan spreken we alsnog van persoonsgegevens.

Identificeren van persoon

Als je niet weet om welke persoon het gaat, kun je lastig spreken van persoonsgegevens. Bij directe persoonsgegevens is een persoon al geïdentificeerd of in ieder geval met naam en toenaam bekend waardoor identificeren eenvoudig is.

Als je alleen een simpel gegeven hebt, zoals een woonplaats of een leeftijd, dan gaat het er om of je de identiteit van de betrokken persoon zonder al te veel inspanning kunt vast stellen. Daarbij is het van belang in welke mate degene die de gegevens bezit heeft, over mogelijkheden beschikt om die identiteit vast te stellen. Met andere woorden: Hoe meer mensen, middelen, geld en toegang tot andere systemen een organisatie heeft, hoe makkelijker het wordt om iemand te identificeren aan de hand van verschillende losse gegevens.

Bijzondere persoonsgegevens (artikel 16 Wbp)

Naast gewone persoonsgegevens kent de Wbp ook bijzondere persoonsgegevens. Daar gelden strengere regels voor. In principe is de verwerking van dat soort gegevens verboden. De Wbp omschrijft zelf de uitzonderingen op grond waarvan de verwerking van bijzondere persoonsgegevens wel is toegestaan. Onder bijzondere persoonsgegevens verstaat de wet:

- ras (daar valt dus ook een foto onder).
- godsdienst of levensovertuiging;
- politieke gezindheid;
- gezondheid;
- strafrechtelijk verleden;
- seksuele geaardheid;
- lidmaatschap van een vakvereniging.

Toelichting bij paragraaf 2: Verwerking van persoonsgegevens

Heb je in je werk te maken met het verwerken van persoonsgegevens? Dan is het belangrijk om rekening te houden met enkele kaders en regels.

Denk aan rechtmatigheid van het verwerken, doelmatigheid, proportionaliteit, zorgvuldigheid, beveiliging, bewaartermijnen en dergelijke. Die begrippen worden onderstaand toegelicht.

Doeleinden (artikelen 4 en 9)

Als binnen een organisatie uiteindelijk is bepaald dat de verwerking noodzakelijk is, mag volgens de wet de verwerking ook niet verder gaan dan nodig. Het doel van de verwerking moet worden vastgelegd.

Bij het verwerken van persoonsgegevens komt het namelijk nog wel eens voor dat men in verloop van tijd opeens hele andere dingen gaat doen met de persoonsgegevens. Dat was in het begin vaak niet zo bedacht. Door het vastleggen van de doeleinden, kunnen de organisatie en de betrokken persoon zelf controleren of de verwerking nog wel netjes gebeurt in lijn met de oorspronkelijke gedachte.

De wetgever heeft het bovenstaande over de doeleinden vastgelegd in artikel 9 van de Wbp. Dat wordt het doelbindingsprincipe genoemd en daardoor kan en moet een verwerking van persoonsgegevens dus worden beperkt tot een specifiek doel of specifieke doeleinden.

Grondslagen (artikel 5)

Als men persoonsgegevens gaat verwerken, moeten de doeleinden dus duidelijk worden omschreven. Maar dat is niet alles, dat doel moet wel vallen binnen de wettelijke grondslagen voor rechtmatige verwerking. De grondslagen voor een rechtmatige verwerking zijn opgenomen in artikel 8 van de Wbp en artikel 5 van deze regeling. Als de gegevensverwerking niet valt te rijmen met één van die grondslagen, dan is het niet toegestaan.

- De meest voor de hand liggende grondslag is de ondubbelzinnige toestemming van de betrokkene. Dat betekent: als je zelf heel duidelijk akkoord bent gegaan met verwerking, dan is het toegestaan. Daarnaast gelden de volgende grondslagen:
- wanneer de gegevensverwerking (dan wel gegevensverstrekking aan een derde partij) noodzakelijk is voor de uitvoering van een overeenkomst waarbij betrokkene partij is
 - o Dat betekent: Je gaat ergens werken, je koopt iets, je ondertekent een contract. Dan is het belangrijk om bepaalde persoonsgegevens te verstrekken.
- voor nakoming van een wettelijke verplichting;
 - o Dat betekent: Als de wet vereist dat in bepaalde gevallen persoonsgegevens moeten worden verstrekt, dan zul je daar aan mee moeten werken.
- ter vrijwaring van een vitaal belang van de betrokkene;
 - o Dat betekent: Denk aan je gezondheid, je veiligheid. Als je leven in het geding is, dan kan het noodzakelijk zijn dat je persoonsgegevens worden verwerkt.
- voor de goede invulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan;
 - o Dat betekent: Het gaat hier om net iets anders dan de grondslag van de wettelijke verplichting. Een publieke taak is bijvoorbeeld wat de VRU doet, voorbereiden op rampenbestrijding en crisisbeheersing. Daarbij bestaat geen wettelijke plicht om persoonsgegevens te verwerken, maar toch kan het noodzakelijk zijn om de opleidingsgegevens van hulpverleners te

verwerken in overzichten, omdat anders niet kan worden beoordeeld of de hulpverlening de juiste kwaliteit in huis heeft. Dat verstoort de voorbereiding.

- of voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt.
 - o Het gerechtvaardigde belang moet je zien als een voorwaardelijke eis. Dat betekent dat een verantwoordelijke niet op een normale manier kan doen wat hij of zij als organisatie moet doen, zonder de gegevens te verwerken.
 - o Voorbeeld: Je geeft je persoonsgegevens aan een verzekeraar bij het afsluiten van een verzekering. Om schade voor jou af te handelen, zal de verzekeraar jouw gegevens moeten verwerken. Bijvoorbeeld door ze te verstrekken aan een andere verzekeraar. Dat is dus een voorwaarde: Zonder het verstrekken van jouw gegevens kan je verzekeraar niet voor jou optreden als verzekeraar.

Bijzondere persoonsgegevens (artikelen 6 en 7)

Voor de verwerking van bijzondere persoonsgegevens is het van belang om extra waarborgen in te bouwen. Door in de regeling, in lijn met de Wbp, de uitzonderingen op het verbod van verwerken van dit soort gegevens op te nemen, is duidelijk in welke specifieke gevallen bijzondere persoonsgegevens verwerkt mogen worden.

Toelichting bij paragraaf 3: De bevoegdheden en plichten van de verantwoordelijke en de beheerder.

Voor de verwerking van persoonsgegevens in een organisatie ligt de verantwoordelijkheid bij de verantwoordelijke en de beheerder. De Wbp definieert de verantwoordelijke als diegene die het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Dat is in het geval van de algemene privacyregeling VRU het algemeen bestuur.

De beheerder is degene die verantwoordelijk is voor een bepaalde verwerking in de organisatie. Dat is de lagere verantwoordelijke, denk aan een afdelingshoofd, die het algehele beheer over het systeem voert. Die beheerder is ook verantwoordelijk voor het vastleggen van de specifieke doeleinden en andere vereisten voor verwerking in dat systeem.

Onder de beheerder valt nog de gebruiker. Dat zijn medewerkers in de organisatie die gegevens in het systeem zetten of bewerken uit hoofde van hun functie. Denk daarbij onder meer aan het beheren van personeelsdossiers, opleidingsdossiers of roosterprogramma's.

Geheimhouding (artikelen 10 en 16)

Alle ambtenaren binnen de VRU zijn op grond van de Ambtenarenwet verplicht tot geheimhouding. Overtreding van een geheimhoudingsplicht is strafbaar.

De geheimhoudingsplicht geldt ook voor personen, niet werkzaam bij de VRU, die voor de VRU werkzaamheden uitvoeren waarbij ze persoonsgegevens verwerken. In de Wbp worden die personen bewerkers genoemd. Een bewerkker moet een zogenaamde bewerkersovereenkomst tekenen, waarvan de geheimhoudingsplicht onderdeel uit maakt.

Meldingsplicht (artikel 11)

Als een organisatie op geautomatiseerde wijze gegevens gaat verwerken, dan moet zij daar melding van doen bij het College Bescherming Persoonsgegevens, het Cbp. Dat is de toezichthouder op het gebied van privacywetgeving.

Maar niet alles hoeft gemeld te worden. Voor veel verwerkingen bestaat een vrijstelling op basis van het Vrijstellingsbesluit Wbp. Daarin worden verwerkingen vrijgesteld, zoals: personeels –en salarisadministratie, opleidingsgegevens, vergunningen en meldingen, netwerk –en computersystemen, toegangssystemen en communicatiebestanden.

Als blijkt dat bepaalde verwerkingen binnen de VRU onder die vrijstelling vallen, dan komt dat in het overzicht in het Uitvoeringsregister bij de regeling terug.

Bewaren en verwijderen (artikelen 12 en 13)

Persoonsgegevens worden niet langer bewaard dan noodzakelijk is voor de verwerkelijking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt. Dat betekent dat de beheerder van een verwerking in een protocol of een regeling bij die verwerking moet vaststellen hoe lang de gegevens bewaard worden. In het Uitvoeringsregister worden die bewaartermijnen van de verschillende verwerkingen vervolgens overzichtelijk samengevat.

Als op een bepaald moment blijkt dat een verwerking van gegevens in haar geheel verwijderd moeten worden, dan stelt een beheerder van een systeem dat vast. Dat besluit wordt vervolgens echter door of namens de verantwoordelijke genomen. Gegevens worden niet verwijderd als ze op grond van de Archiefwet nog bewaard moeten worden.

Toegang en beveiliging (artikelen 14 en 15)

Uitsluitend de beheerder en de door de beheerder aangewezen gebruikers kunnen persoonsgegevens inzien. Het is de bedoeling dat een organisatie werkt met autorisatieniveaus. Alleen personen die uit hoofde van hun functie met bepaalde persoonsgegevens werken, krijgen toegang. Die toegang wordt beperkt tot het strikt noodzakelijke, dus niet meer inzien dan noodzakelijk. Dat betekent dat de beheerders op een verantwoordelijke manier om moeten gaan met het uitdelen van autorisaties aan hun personeel. De manier waarop dat gebeurt dient te worden beschreven voor een bepaalde gegevensverwerking.

Daarnaast moeten de systemen waarin persoonsgegevens worden verwerkt, op een passende manier beveiligd zijn. Daarmee wordt bedoeld dat de beveiliging een niveau moet hebben dat voldoet aan de eisen die in de dagelijkse praktijk voor soortgelijke systemen en organisaties noodzakelijk en gangbaar is. De beheerder en de verantwoordelijke voor het technisch beheer van dergelijke systemen, dat kan ook een externe leverancier zijn, zorgen er voor dat die beveiliging op orde is.

Toelichting bij paragraaf 4: De rechten van de betrokkene (artikelen 17, 18, 19, 20)

De wet kent aan een betrokkene een aantal rechten toe. De verantwoordelijke informeert de betrokkene over die rechten. Daarbij is de verantwoordelijke ook verplicht om een betrokkene te informeren over het hoe en waarom van een verwerking als hij om de gegevens vraagt aan de betrokkene.

Een betrokkene heeft het recht om zijn gegevens in te zien. In beginsel mag een organisatie daar een vergoeding voor vragen. Maar ook geldt een reactietermijn. Binnen vier weken moeten de inzage in de gegevens worden gegeven.

Als een betrokkene tot de conclusie komt dat zijn gegevens onjuist zijn, kan hij de verantwoordelijke verzoeken om zijn gegevens te verbeteren. De verantwoordelijke moet daar in principe aan meewerken. Hij kan weigeren, maar moet dat dan wel goed uitleggen aan de betrokkene. Hetzelfde geldt voor een verzoek van een betrokkene om zijn gegevens te laten vernietigen.

Klachten (artikel 20)

De organisatie moet vragen over de verwerking van persoonsgegevens kunnen beantwoorden. De beheerder is daarvoor in eerste instantie de aangewezen persoon. Hij is verantwoordelijk voor het systeem en kan de meeste vragen inhoudelijk het best behandelen. Daarnaast kan bij een afdeling Personeel en Organisatie of Juridische Zaken aanvullende informatie over de toepassing van wet /en regelgeving worden gevraagd.

Indien de betrokkene toch van mening is dat de bepalingen van de regeling niet worden nageleefd of andere reden tot klagen heeft over de verwerking van zijn persoonsgegevens, kan hij zich aan de hand van de klachtenregeling VRU wenden tot de verantwoordelijke of tot de toezichthouder, het Cbp.