HANDREIKING GEGEVENS-BESCHERMING

vereniging van
woningcorporaties

aedes

VOORWOORD

Steeds meer gegevens zijn digitaal beschikbaar. Informatie over vastgoed, maar ook over mensen en hun gedrag. Ook woningcorporaties digitaliseren en koppelen informatie over huurders. Het zal u niet verbazen dat dit aan strikte wettelijke regels is gebonden. Een belangrijke regel die recent in werking is getreden is de meldplicht datalekken: organisaties die een datalek constateren moeten dat melden aan de Autoriteit Persoonsgegevens en soms ook bij de personen op wie de gegevens zien. Datalekken kunnen grote gevolgen hebben. Met een kopie van een paspoort bijvoorbeeld kunnen criminelen leningen afsluiten of een ruimte voor een wietplantage huren. Per dag zijn er in Nederland zo'n 500 gevallen van identiteitsfraude bekend.

De bescherming van persoonsgegevens omvat echter ook vele andere aspecten waar woningcorporaties rekening mee moeten houden. Te denken valt aan het verstrekken van gegevens aan andere partijen, zwarte lijsten, het aanstellen van een Functionaris voor de Gegevensbescherming en nog een hele hoop andere aspecten. Handelt u in strijd met de wet, dan kunnen de boetes oplopen tot 820.000 euro of 10 procent van de jaaromzet.

Met deze *Handreiking gegevensbescherming* helpen we u om gegevens zo te verwerken dat u handelt in overeenstemming met de wet omtrent de bescherming van persoonsgegevens, de Wet bescherming persoonsgegevens (Wbp). De handreiking richt zich in eerste instantie op de privacy van huurders. Daarnaast wordt ook kort ingegaan op de privacybescherming van medewerkers van woningcorporaties. De handreiking biedt u op een begrijpelijke en praktische manier inzicht in de Wbp. Daarbij sluiten we aan bij de Europese Algemene Verordening Gegevensbescherming (AVG) die vanaf 2018 van kracht zal zijn.

We benadrukken dat deze handreiking een hulpmiddel is en geen algehele blauwdruk voor iedere corporatie. Het beheersen en beheren van privacy is namelijk maatwerk, en dus afhankelijk van de wijze waarop uw organisatie technisch en organisatorisch is ingericht.

Marc Calon
Voorzitter Aedes vereniging van woningcorporaties

INHOUD

INHOUD (VERVOLG)

INHOUD (VERVOLG)

WETTEN EN UITGANGSPUNTEN

Het recht op gegevensbescherming is een onderdeel van het recht op bescherming van de persoonlijke levenssfeer, beter bekend als het recht op privacy. Er zijn drie vormen van dit recht te onderscheiden: ruimtelijke privacy (zoals het huisrecht), relationele privacy (zoals de vrijheid van vereniging en vergadering) en informationele privacy (gegevensbescherming). Al deze varianten vallen samen onder de overkoepelende term privacy. Het handboek richt zich alleen op de laatstgenoemde variant, de gegevensbescherming.[1]

De bescherming van persoonsgegevens is uitgewerkt in verschillende wetten. In onder meer de Grondwet (sinds 1983) en het Europees Verdrag voor de Rechten van de Mens (EVRM) (sinds 1950) is het recht op bescherming van persoonsgegevens vastgelegd. Een belangrijk fundament voor het recht op gegevensbescherming is in 1980 gelegd door de Organisatie voor Economische Samenwerking en Ontwikkeling (OESO). De OESO heeft uitgangspunten geformuleerd voor de verwerking van gegevens., die nog altijd een belangrijke rol spelen:

- beperk het verzamelen van persoonsgegevens;
- gebruik alleen de gegevens die relevant zijn voor het doel en voldoende up-to-date zijn;
- verzamel de gegevens alleen voor een specifiek doel;
- gebruik de gegevens niet voor een ander doel dan omschreven;
- zorg voor voldoende beveiligingsmaatregelen;
- geef openheid over het gebruik van persoonsgegevens;
- het individu heeft het recht om te achterhalen of er gegevens over hem worden verzameld en het recht deze te corrigeren, aan te vullen of te laten verwijderen;
- de beheerder is verantwoordelijk voor de naleving van de beginselen.

De OESO-uitgangspunten zijn voor het eerst in de Nederlandse wet verankerd in de Wet persoonsregistraties (1988). Ook in de Europese Privacyrichtlijn 95/46/EG kwamen deze uitgangspunten – al dan niet in andere bewoordingen – terug.[2] Met de opvolger van de Wet persoonsregistraties in 2001 werd deze richtlijn uitgewerkt in de Wet bescherming persoonsgegevens (Wbp). Deze wet vormt nog altijd het algemene Nederlandse kader voor de bescherming van persoonsgegevens en is ook van toepassing op woningcorporaties. Naast bovengenoemde uitgangspunten bevat de Wbp verplichtingen over onder meer bewaartermijnen, het melden van datalekken en het verbod op het verwerken van bijzondere persoonsgegevens. Al deze aspecten zullen in dit handboek apart worden behandeld. Daarnaast zijn er nog diverse specifieke regels omtrent gegevensbescherming opgenomen in andere sectorspecifieke wetten, zoals de Telecommunicatiewet. Deze wetten blijven in dit handboek achterwege, maar verdienen mogelijk wel uw aandacht.

Op 25 mei 2018 zal de Europese Algemene Verordening Gegevensbescherming (hierna: AVG of verordening) de Wbp vervangen.[3] De AVG bevat in essentie dezelfde uitgangspunten als de Wbp, maar brengt een aantal aanscherpingen en nieuwe (administratieve) plichten met zich mee voor alle organisaties die persoonsgegevens verwerken. Daar waar de AVG belangrijke vernieuwingen met zich meebrengt ten opzichte van de besproken normen uit de Wbp wordt in dit handboek een nadere toelichting gegeven. Het karakteristieke van een Europese verordening – en dus ook de AVG – is dat deze zogenaamde rechtstreekse werking heeft in alle lidstaten en dat omzetting in een nationale wet als gevolg daarvan niet vereist is. De regels zijn daardoor in heel Europa hetzelfde, hoewel in de AVG op een aantal punten ruimte wordt gelaten voor nationale regelgeving.

1 Voor de leesbaarheid zullen de termen gegevensbescherming en privacy in dit handboek door elkaar heen worden gebruikt.
2 Uiteraard is de geschiedenis van het privacyrecht veel omvangrijker, maar voor het doel van deze handreiking niet noodzakelijk om uitgebreid te bespreken.
3 De Nederlandse versie van de AVG is online te raadplegen op de volgende website: http://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=OJ:JOL_2016_119_R_0001&from=EN

TERMEN EN DEFINITIES

De Wbp hanteert een aantal standaarddefinities. Deze definities komen in verschillende wetsartikelen voor en worden ook gebruikt in dit handboek. Omdat de termen soms verwarrend of onduidelijk kunnen zijn, vindt u hier een uitleg over de belangrijkste termen van de Wbp. In de Wbp zijn de definities uitgewerkt in artikel 1. Let op: in de AVG zullen een aantal definities veranderen! Deze zijn als zodanig aangegeven in onderstaande tabel.

Autoriteit Persoonsgegevens (AP)	De toezichthoudende autoriteit die toeziet op de naleving van de Wbp. De Autoriteit Persoonsgegevens beschikt ook over adviserende taken en geeft voorlichting over bepaalde onderwerpen. Tot 31-12-2015 heette de AP het College Bescherming Persoonsgegevens.
Betrokkene	De betrokkene is degene op wie de persoonsgegevens betrekking hebben. Bij bijvoorbeeld een huurdersbestand zijn alle huurders wiens gegevens zijn opgeslagen aan te merken als betrokkenen. Ook woningzoekenden, kopers van woningen en andere personen van wie de woningcorporatie persoonsgegevens verwerkt zijn betrokkenen in de zin van de Wbp.
Bewerker (AVG: verwerker)	De bewerker is degene die persoonsgegevens verwerkt in opdracht van de verantwoordelijke, zonder onder dezelfde organisatie te vallen als de verantwoordelijke en zonder aan zijn rechtstreekse gezag te zijn onderworpen. Een voorbeeld is een externe accountant die beschikt over de personeelsadministratie van de verantwoordelijke om de lonen uit te keren aan de werknemers van de verantwoordelijke. De accountant, of het bedrijf waar deze accountant in dienst is, is dan een bewerker.
Datalek	Een inbreuk op de beveiliging, bedoeld in artikel 13 Wbp, die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens. Zie voor nadere toelichting paragraaf 14.
Derde(n)	Ieder andere (rechts)persoon dan de betrokkene, de verantwoordelijke of de bewerker in de zin van de Wbp.
Persoonsgegevens	Persoonsgegevens zijn alle gegevens die zo kenmerkend zijn voor een bepaalde persoon dat hij/zij aan de hand van die gegevens kan worden geïdentificeerd. Hoofdregel is dat een persoon identificeerbaar is als zijn identiteit zonder onevenredige inspanning vastgesteld kan worden. Hieronder vallen zowel gegevens die direct identificerend zijn (zoals namen) als indirect identificeerbare gegevens die alleen in combinatie met andere gegevens tot een bepaalde persoon herleidbaar zijn (unieke gegevens, zoals een burgerservicenummer en unieke combinaties, zoals geboortedatum en adres). Persoonsgegevens zien alleen op in leven zijnde, natuurlijke personen. Bedrijfsgegevens, met uitzondering van bepaalde namen van eenmanszaken, vallen hier dus niet onder. In plaats van de term persoonsgegevens wordt voor de leesbaarheid ook wel het woord 'gegevens' gebruikt.

Privacy Impact Assessment (PIA) (AVG: gegevensbeschermings-effectbeoordeling)	Met een Privacy Impact Assessment (PIA) wordt onderzocht welk effect een of meerdere gegevensverwerkingen hebben op de persoonlijke levenssfeer. Het is daarmee een middel om te kijken of voldoende rekening wordt gehouden met de privacybelangen van betrokkenen en of verwerking(en) rechtmatig zijn. Zie voor meer informatie paragraaf 2 in het hoofdstuk over implementatie.
Toestemming	Elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem betreffende persoonsgegevens worden verwerkt. Zie voor een nadere uitwerking paragraaf 2.
Verantwoordelijke (AVG: verwerkings-verantwoordelijke)	De verantwoordelijke is degene die het doel en de middelen van de verwerking van persoonsgegevens bepaalt. Een verantwoordelijke kan zowel een (natuurlijke) persoon als rechtspersoon zijn.
Verwerking van persoonsgegevens	Elke handeling met betrekking tot persoonsgegevens is aan te merken als een verwerking van persoonsgegevens. Een actieve wijziging (bewerking) is dus niet vereist om onder de term 'verwerking' te vallen! Ook bijvoorbeeld het verzamelen, inzien, wijzigen, opvragen, gebruiken, verspreiden, afschermen, koppelen, uitwissen of vernietigen van gegevens is een verwerking. Volledig geautomatiseerde handelingen kunnen ook worden aangemerkt als een verwerking.

WET BESCHERMING PERSOONSGEGEVENS

De Wet bescherming persoonsgegevens (Wbp) bevat regels over het vastleggen en verstrekken van persoonsgegevens ter bescherming van de persoonlijke levenssfeer van de betrokkene. Woningcorporaties die als verantwoordelijke persoonsgegevens (laten) verwerken hebben te maken met de volgende regels:

- Persoonsgegevens moeten op een zorgvuldige en behoorlijke wijze worden verwerkt, in overeenstemming met de wet (artikel 6 Wbp).
- De verwerking moet plaatsvinden met een rechtmatige grondslag (artikel 8 Wbp).
- Verdere verwerking van persoonsgegevens kan slechts plaatsvinden op grond van welbepaalde, uitdrukkelijk omschreven, gerechtvaardigde doelen (artikel 7, 9 en 43 Wbp).
- De kwaliteit van persoonsgegevens moet op orde zijn, ter zake dienend en niet bovenmatig (artikel 11 Wbp).
- Verwerkingen van persoonsgegevens moeten worden gemeld bij de AP (artikel 27 Wbp).
- Er moeten passende technische en organisatorische beveiligingsmaatregelen worden genomen om de persoonsgegevens te beschermen (artikel 13 Wbp).
- Waar nodig moeten afspraken met derden worden gemaakt over de verwerking van persoonsgegevens (artikel 14 Wbp).
- Persoonsgegevens mogen niet nodeloos (lang) worden bewaard (artikel 10 Wbp).
- Het instellen van een functionaris voor de gegevensbescherming (FG) (artikel 62-64 Wbp).
- De betrokkene heeft recht op informatie over de verwerking van zijn gegevens (artikel 33 en 34 Wbp).
- De betrokkene heeft recht op inzage, wijziging, verwijdering van de eigen persoonsgegevens (artikel 35, 36, 40-41 Wbp) en het recht om niet te worden onderworpen aan geautomatiseerde individuele besluitvorming (artikel 42 Wbp).
- Aparte, strengere regimes voor de verwerking van bijzondere persoonsgegevens (artikel 16-23 Wbp) en gevoelige persoonsgegevens, waaronder wettelijke persoonsnummers (artikel 24 Wbp).
- Per 1 januari 2016 moeten datalekken bij de AP en aan betrokkene worden gemeld (nieuw artikel 34a Wbp).
- Sancties voor het verwerken van persoonsgegevens in strijd met de Wbp (artikel 66 Wbp).

Deze regels worden in dit handboek meer in detail afzonderlijk besproken.

1. ZORGVULDIGE EN BEHOORLIJKE VERWERKING

Zorgvuldige en behoorlijke verwerking van persoonsgegevens (artikel 6 Wbp) is een essentiële norm die doorklinkt in de hele Wbp. Het is een basisvoorwaarde voor iedere verwerking van persoonsgegevens. De norm houdt in dat elke vorm van gegevensverwerking 'eerlijk' ('fair') is en in overeenstemming is met alle wettelijke regels die op de verwerking van persoonsgegevens zien.[4] Bij de beoordeling of een verwerking zorgvuldig en behoorlijk is wordt aangesloten bij de open behoorlijkheidsnorm van de Ombudsman, de redelijkheid en billijkheidsbepaling uit het Burgerlijk Wetboek (artikel 6:162 BW) en de algemene beginselen van behoorlijk bestuur. Per geval moet worden afgewogen of dit het geval is.

Een voorwaarde voor eerlijke c.q. zorgvuldige en behoorlijke gegevensverwerking is in ieder geval dat betrokkenen weten *dat* hun gegevens worden verwerkt. Huurders en woningzoekenden moeten worden geïnformeerd over de manier waarop hun persoonsgegevens worden verwerkt (zie verder paragraaf 10 over de informatieplicht). Het ongemerkt verzamelen en verwerken van gegevens door bijvoorbeeld heimelijk cameratoezicht, is dus vaak niet toegestaan en daarmee ook in strijd met deze norm.

Daarnaast geven de artikelen 7 tot en met 15 van de Wbp een nadere invulling aan het beginsel van zorgvuldige en behoorlijke verwerking van persoonsgegevens. Zo moeten gegevens juist, accuraat en up-to-date zijn, en mogen er niet meer persoonsgegevens worden verwerkt dan noodzakelijk voor het doel waarvoor deze worden verzameld en verwerkt (artikel 11 Wbp, zie nader paragraaf 4).

In bepaalde gevallen zijn (individuele) uitzonderingen mogelijk op deze regel (artikelen 43 en 44 Wbp), zie hiervoor paragraaf 3.1.

2. DOEL EN GRONDSLAG

Om überhaupt persoonsgegevens te mogen verwerken moet er een welbepaald, uitdrukkelijk omschreven, vooraf bepaald en gerechtvaardigd doel zijn vastgesteld voor de verwerking (artikel 7 Wbp). Het doel mag dus niet vaag zijn of heel ruim omschreven. De betrokkene moet immers kunnen begrijpen waarom gegevens worden verwerkt. Voorbeelden van doelen zijn woonruimtebemiddeling, de woningverhuur, het voeren van een personeelsadministratie of tevredenheidsonderzoek. Het is dus van belang om te documenteren waarom gegevens voor relevante werkprocessen worden verwerkt.

Daarnaast mogen persoonsgegevens alleen worden verwerkt voor een bepaald doel als de verwerking een *grondslag* heeft en de *noodzaak* van de gegevensverwerking is aangetoond, zo blijkt uit artikel 8 Wbp (zie telkens het woord 'noodzakelijk' bij de grondslagen[5]). Bij de verwerking van persoonsgegevens gaat het dus niet per se om de vraag of de verwerking *mag*, maar om de vraag of de verwerking *nodig is*.

Bij het beoordelen van de noodzaak moet steeds de vraag worden gesteld of het verwerken van het betreffende gegeven echt noodzakelijk is om – bijvoorbeeld – de huurovereenkomst te kunnen uitvoeren of om andere doelen te realiseren. Om de noodzaak te kunnen bepalen moet steeds worden beoordeeld of: 1) de privacy van de betrokkene in redelijke verhouding staat tot het doel van de verwerking (*proportionaliteit*), en 2) het doel waarvoor de persoonsgegevens worden verwerkt niet redelijkerwijs op een andere, voor de betrokkene minder nadelige wijze kan worden bereikt *(subsidiariteit)*.

Er zijn zes limitatieve grondslagen genoemd in artikel 8 Wbp:

1. de betrokkene heeft voor de verwerking zijn *ondubbelzinnige toestemming* verleend;
2. de gegevensverwerking is noodzakelijk voor de *uitvoering van een overeenkomst* waarbij de betrokkene partij is, of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene en die gegevensverwerking is noodzakelijk voor het sluiten van een overeenkomst;
3. de gegevensverwerking is noodzakelijk om een *wettelijke verplichting* na te komen waaraan de verantwoordelijke onderworpen is;
4. de gegevensverwerking is noodzakelijk ter vrijwaring van een *vitaal belang* van de betrokkene;

4 Zo bevatten naast de Wbp ook de Telecommunicatiewet en de Wet Politiegegevens regels over het verwerken van persoonsgegevens.
5 Bij de grondslag over toestemming is het woord 'noodzakelijk' niet opgenomen. Toch eist de rechter dat ook in geval van toestemming moet worden voldaan aan de beginselen van proportionaliteit en subsidiariteit. Zie HR 9 september 2011, ECLI:NL:HR:2011:BQ8097.

5. de gegevensverwerking is noodzakelijk voor de goede *vervulling van een publiekrechtelijke* taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt, of
6. de gegevensverwerking is noodzakelijk 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.

Elke gegevensverwerking moet onder een van deze zes grondslagen vallen. Kunnen de gegevens met andere woorden niet worden verwerkt op basis van een van deze grondslagen, dan mogen die persoonsgegevens niet worden verwerkt. Sommige verwerkingen kunnen worden gebaseerd op meerdere grondslagen.

Voorbeeld: grondslagen bij woningcorporaties
Een woningcorporatie verhuurt woningen in de omgeving Groningen. Om te onderzoeken hoe tevreden huurders zijn met de dienstverlening, wil de woningcorporatie een niet-geanonimiseerd onderzoek doen onder haar huurders met behulp van vragenlijsten.

De gegevens die worden verwerkt in het kader van de woningverhuur vallen onder artikel 8 sub b: de *uitvoering van een overeenkomst*. Daarbij mogen *alleen* de gegevens worden verwerkt die daadwerkelijk noodzakelijk zijn om de huurovereenkomst uit te kunnen voeren. Het doen van onderzoek is bijvoorbeeld niet vereist voor de uitvoering van een huurovereenkomst. De enige mogelijke grondslag om dit onderzoek uit te voeren is de *ondubbelzinnige toestemming* van de huurder, omdat met het onderzoek persoonsgegevens eveneens worden verwerkt. De woningcorporatie mag de gegevens voor dit onderzoek pas verwerken als woningzoekenden daadwerkelijk toestemming hebben gegeven dat de woningcorporatie zijn persoonsgegevens mag verwerken voor dit doel.

De toestemming kan vooraf gevraagd worden, bijvoorbeeld bij inschrijving als woningzoekende. Deze toestemming is niet nodig, wanneer gegevens anoniem worden verwerkt voor het maken van bijvoorbeeld statistiek. Hiervoor kent de Wbp de nodige uitzonderingen.

De meest voorkomende wettelijke grondslagen voor woningcorporaties zijn: toestemming, uitvoering van een (huur)overeenkomst, nakoming van een wettelijke verplichting en het gerechtvaardigde belang van de verantwoordelijke (de woningcorporatie).

2.1 TOESTEMMING

De eerste bij wet genoemde grondslag voor het verwerken van persoonsgegevens is toestemming van de betrokkene. Wat toestemming precies inhoudt is nader bepaald in artikel 1 onder i Wbp. De definitie vereist dat toestemming:

- in vrijheid, dat wil zeggen niet onder druk, is gegeven. In financiële, emotionele of praktische afhankelijke relaties, zoals een werkgeversrelatie, kan toestemming in een aantal gevallen niet in vrijheid zijn gegeven. Er is dan immers sprake van een afhankelijkheid tussen verantwoordelijke en betrokkene, wat de vrijheid vanwege het bestaan van een zekere mate van hiërarchie per definitie belemmert.
- specifiek is gegeven met betrekking tot een bepaald aantal gegevensverwerkingen. Zeer algemene toestemming vragen met betrekking tot alle vormen van gegevensverwerking ('de algemene bedrijfsvoering') is niet mogelijk. Toestemming moet zien op een concreet doel.
- op informatie berust. Dit betekent dat de toestemming alleen rechtsgeldig kan worden gegeven indien aan de betrokkene duidelijk is gemaakt hoe en waarom zijn gegevens worden verwerkt, bijvoorbeeld met een privacystatement (zie ook paragraaf 10 over de informatieplicht).
- ondubbelzinnig, zonder twijfel, is gegeven. Impliciete toestemming, bijvoorbeeld het vooraf invullen van een akkoord door middel van een 'vinkje', voldoet hierbij niet. De verantwoordelijke zal moeten aantonen dat de betrokkene daadwerkelijk toestemming heeft gegeven.
- een wilsuiting is. Toestemming moet een actieve handeling zijn, zoals het zetten van een handtekening of het aanvinken van een hokje. Ook om deze reden volstaat impliciete toestemming niet.

Toestemming kan op grond van artikel 5 lid 2 Wbp altijd worden ingetrokken door de betrokkene. Intrekking van toestemming heeft geen gevolgen voor gegevensverwerkingen vóór het moment van intrekking. Wel heeft dit gevolgen voor gegevensverwerkingen ná intrekking. Er is dan niet langer meer een grondslag voor de verwerking van persoonsgegevens. In de praktijk houdt dit dus in dat als toestemming eenmaal is ingetrokken, er geen persoonsgegevens meer mogen worden verwerkt voor het betreffende doel. Dit mag alleen als de persoonsgegevens nog kunnen worden verwerkt op grond van een andere grondslag, zoals een wettelijke plicht om bepaalde persoonsgegevens te bewaren. Dat betekent dat verlenen en/of intrekken van toestemming geadministreerd moet worden, zodat het moment hiervan duidelijk kan worden aangetoond. Let op: vraag niet om toestemming als dit eigenlijk niet nodig is, er moet dan immers ook een onnodige administratie gevoerd worden.

2.2 UITVOERING VAN OVEREENKOMST

Sommige gegevens zijn noodzakelijk om overeenkomsten, zoals een huurovereenkomst, goed te kunnen uitvoeren. Wanneer een woning wordt verhuurd, dan mogen woningcorporaties daarvoor bepaalde persoonsgegevens opvragen bij de huurder, zoals NAW-gegevens, gezinssamenstelling en rekeningnummer.[6] Zonder deze gegevens kunnen immers de afspraken uit de huurovereenkomst (zoals het betalen respectievelijk ontvangen van huurpenningen) niet worden uitgevoerd. Deze grondslag geldt alleen voor die gegevens die daadwerkelijk noodzakelijk zijn voor het uitvoeren van de (huur)overeenkomst. Met andere woorden, de verkregen gegevens mogen alleen worden gebruikt voor zover dat nodig is voor de woningverhuur.

2.3 WETTELIJKE PLICHT

In het geval de wet voorschrijft dat gegevens voor een bepaald doel ***moeten*** worden verwerkt, kan een woningcorporatie niet anders dan hier gevolg aan geven. Op grond van wet- en regelgeving in het kader van belastingen bijvoorbeeld moeten allerlei gegevens verwerkt worden.

2.4 GERECHTVAARDIGD BELANG

In bepaalde situaties is het noodzakelijk om persoonsgegevens te verwerken, omdat de woningcorporatie een gerechtvaardigd (bedrijfs-, of economisch) belang heeft dat zwaarder weegt dan het privacybelang van de betrokkene. Deze grondslag wordt in de praktijk bijvoorbeeld gebruikt om persoonsgegevens uit te wisselen met anderen om woonfraude, hennepteelt en overlast te bestrijden. Het belang van de woningcorporatie om niet het slachtoffer te worden van misbruik en woonfraude kan in dat geval zwaarder wegen dan het recht op privacy van de betrokkene. Misbruik en woonfraude hebben bovendien een negatieve invloed op de samenleving als geheel.

Er is alleen sprake van een gerechtvaardigd belang, wanneer rekening is gehouden met de vereisten van proportionaliteit en subsidiariteit én wanneer voldoende privacywaarborgen zijn getroffen. Het enkele feit dat er een gerechtvaardigd belang bestaat, is dus niet voldoende om persoonsgegevens te mogen verwerken! Om de noodzaak van de uitwisseling van persoonsgegevens in bijvoorbeeld samenwerkingsverbanden aan te tonen en privacywaarborgen te kunnen garanderen worden vaak convenanten gesloten of protocollen vastgesteld. Hierin is onder meer geregeld met wie de persoonsgegevens worden gedeeld, welke gegevens worden gedeeld en hoe de gegevens zijn beveiligd (zie over het uitwisselen van persoonsgegevens met derden meer in paragraaf 7). Het gerechtvaardigd belang kan ook dienen als de grondslag voor het gebruik van zwarte lijsten. Hierover meer in paragraaf 12.2.

3. DOELBINDING

Het enkele feit dat er een grondslag is voor gegevensverwerking, betekent nog niet dat de gegevens overal voor mogen worden gebruikt. Artikel 9 Wbp bepaalt namelijk dat de persoonsgegevens niet ***verder*** mogen worden verwerkt als dit onverenigbaar is met het oorspronkelijke doel waarvoor de gegevens zijn verkregen. Als er bijvoorbeeld persoonsgegevens worden verzameld voor de woningverhuur, dan mogen de verzamelde persoonsgegevens niet zomaar verder worden verwerkt voor een ander doel. Van de Belastingdienst verkregen inkomensgegevens voor het doorvoeren van de inkomensafhankelijke huurverhoging mogen alleen voor dat doel gebruikt worden en dus niet om bijvoorbeeld mensen met een hoog inkomen te selecteren en hen aan te schrijven met de vraag of zij hun huurwoning willen kopen. Voor de vaststelling of er sprake is van verenigbaar gebruik moet rekening gehouden worden met (artikel 9 lid 2 Wbp):

6 Zie voor een overzicht van gegevens die mogen worden verzameld voor de verhuur ook artikel 14 lid 3 Vrijstellingsbesluit Wbp.

a. de *verwantschap* tussen het doel van de beoogde verwerking en het doel waarvoor de gegevens oorspronkelijk zijn verkregen.Naarmate de doelen meer verwant zijn aan elkaar, is verdere verwerking eerder gerechtvaardigd.
b. de *aard* van de betreffende gegevens. Hierbij moet ook worden gekeken of het gaat om 'gewone' persoonsgegevens of juist om bijzondere of privacygevoelige persoonsgegevens, zoals gegevens over gezondheid, inkomen, et cetera (zie verder paragraaf 12). In het algemeen geldt, dat hoe gevoeliger het gegeven, hoe minder snel er sprake is van verenigbaar gebruik. Gegevens mogen dan dus niet verder worden verwerkt.
c. de *gevolgen* van de beoogde verwerking voor de betrokkene. Als de betrokkene gevolgen ondervindt van de verdere verwerking, dan zal het verdere gebruik van de gegevens eerder onverenigbaar zijn. Een betrokkene zal bijvoorbeeld niet veel merken van het gebruik van de gegevens voor intern onderzoek, maar wel als hij/zij zich niet meer kan inschrijven als woningzoekende of geen woning krijgt toegewezen. In het laatste geval zal er minder snel sprake zijn van verenigbaar gebruik.
d. de *wijze* waarop de gegevens zijn *verkregen*. Als er zonder medeweten van de betrokkene gegevens zijn verkregen, dan zal in dat geval eerder sprake zijn van onverenigbaar gebruik.
e. de mate waarin jegens de betrokkene wordt voorzien in *passende waarborgen*. Een voorbeeld van een waarborg is het vooraf inlichten van de betrokkene of het vragen van een zienswijze van de betrokkene over de verdere verwerking. Of de gekozen waarborg 'passend' is, hangt af van de omstandigheden van het geval.

Het is aan de corporatie om af te wegen of in het concrete geval sprake is van (on)verenigbaar verder gebruik. Als er bij de afweging van de bovengenoemde factoren sprake blijkt te zijn van onverenigbaar verder gebruik, dan mogen de persoonsgegevens niet verder worden verwerkt voor het andere doel.

3.1 UITZONDERINGEN

Als uitzondering op het verbod op verdere verwerking bij onverenigbaar gebruik bepaalt artikel 9 lid 3 Wbp dat een verdere verwerking van persoonsgegevens voor historische, statistische of wetenschappelijke doeleinden wel is toegestaan. Er moeten dan wel technische, organisatorische en/of juridische voorzieningen zijn getroffen om ervoor te zorgen dat de gegevens alleen voor deze doeleinden kunnen worden gebruikt. Te denken valt aan het opstellen van een contract met daarin een nadere uitwerking van het gebruik.

Persoonsgegevens mogen ook verder worden verwerkt als een van de uitzonderingen van artikel 43 Wbp van toepassing is. Artikel 43 bepaalt dat de persoonsgegevens verder mogen worden verwerkt als dit noodzakelijk (zie voor het begrip 'noodzaak' paragraaf 2) is in het belang van:
a. de veiligheid van de staat;
b. de voorkoming, opsporing en vervolging van strafbare feiten;
c. gewichtige economische en financiële belangen van de staat en andere openbare lichamen;
d. het toezicht op de naleving van wettelijke voorschriften die zijn gesteld ten behoeve van de belangen, bedoeld onder b en c, of
e. de bescherming van de betrokkene of van de rechten en vrijheden van anderen.

Deze uitzonderingen kunnen niet zomaar worden toegepast. De hoofdregel is dat de toepassing van deze uitzonderingen per individueel geval moet worden bekeken. Het zijn dus geen algemene uitzonderingsgronden voor de verwerking van gegevens.

4. KWALITEIT EN DATAMINIMALISATIE

Artikel 11 Wbp gaat zowel over kwalitatief goede (lees: juiste) en up-to-date informatie over een betrokkene als over dataminimalisatie. Dataminimalisatie betekent dat persoonsgegevens ter zake dienend en niet bovenmatig zijn. Zo heeft het bijvoorbeeld geen enkel nut om iemands e-mailadres te registeren als er toch geen gebruik van wordt gemaakt of om persoonsgegevens over kinderen te registreren als alleen maar het aantal bewoners in een woning hoeft te worden geregistreerd. Het zal van het doel van de gegevensverwerking afhangen of de verwerking ter zake dienend en niet bovenmatig is. Weten waarom persoonsgegevens zijn verzameld (doel) is dus ook hier weer van belang.
De juistheid en nauwkeurigheid van persoonsgegevens speelt ook een grote rol voor het functioneren van

woningcorporaties. In de toekomst zal dit alleen maar een grotere rol gaan spelen door verdere en meer omvangrijke samenwerking in ketens en koppeling van verschillende databases. Juist aan die koppeling en uitwisseling kleeft het risico op vervuiling. In samenwerkingsketens is het daarom van belang om afspraken te maken zodat de gegevens in de hele keten worden gewijzigd, aangevuld en waar nodig worden vernietigd.

5. MELDING VAN GEGEVENSVERWERKINGEN

Verwerkingen van persoonsgegevens moeten in een aantal gevallen verplicht worden gemeld bij de Autoriteit Persoonsgegevens (artikel 27 Wbp). De AP houdt een openbaar register bij van alle meldingen, om betrokkenen te kunnen informeren over de bedrijven en organisaties die hun gegevens verwerken.[7] Het meldingenregister van de AP is niet bedoeld om te controleren of men zich aan de regels houdt. De AP keurt de meldingen dan ook niet goed of af. Gemelde gegevensverwerkingen zijn daarom niet per se rechtmatig, omdat er geen controle plaatsvindt. Wel kunnen er bij de AP naar aanleiding van een melding vragen rijzen over bepaalde gegevensverwerkingen. In dat geval kan de AP een inlichtingenverzoek doen. Dit kan bijvoorbeeld het geval zijn als de inhoud van de melding onvoldoende duidelijk is, of als er indicaties zijn dat verwerkingen plaatsvinden die niet gemeld zijn, maar wel gemeld hadden moeten worden.

Het Vrijstellingsbesluit Wbp geeft een overzicht van een aantal veelvoorkomende verwerkingen van persoonsgegevens waarvoor het melden onder de daar genoemde voorwaarden niet noodzakelijk is. De reden hiervoor is dat deze verwerkingen niet of nauwelijks inbreuk maken op de persoonlijke levenssfeer en/of het melden van alle afzonderlijke gegevensverwerkingen te grote administratieve lasten met zich meebrengt. Openbare registers en verplichte verstrekkingen aan bestuursorganen zijn bij wet eveneens vrijgesteld van de plicht tot melding. Dit betekent overigens niet dat u niet ***mag*** melden; het staat woningcorporaties vrij om ook vrijgestelde gegevensverwerkingen te melden.

In plaats van het melden van een verwerking aan de AP, kan ook worden gemeld bij de eigen functionaris voor de gegevensbescherming (FG). Deze functionaris moet wel als zodanig zijn geregistreerd bij de AP in het openbare register. Zie over de functionaris voor de gegevensbescherming meer in paragraaf 9.

De meldplicht van gegevensverwerkingen zal komen te vervallen met ingang van de AVG in 2018 (zie paragraaf 5.5). Tot die tijd is het, behoudens vrijstellingen, verplicht om gegevensverwerkingen te melden bij de AP.

5.1 MELDEN

Of bepaalde gegevensverwerkingen gemeld moeten worden staat ter beoordeling van de woningcorporatie zelf. Om dit te kunnen beoordelen moet ten minste duidelijk zijn welke verwerkingen er binnen de organisatie plaatsvinden om te kunnen beoordelen of een melding moet worden gedaan. Hierbij geldt als uitgangspunt dat elke gebundelde verwerking van persoonsgegevens voor een of meer doeleinden moet worden gemeld bij de AP, tenzij de verwerking valt onder het Vrijstellingsbesluit Wbp.

De verantwoordelijke hoeft niet elke verwerkingshandeling apart te melden; de samenhang tussen de doeleinden zal bepalen of er meerdere meldingen dienen plaats te vinden. Handelingen zoals het vastleggen, wijzigen en verspreiden hoeven dus niet apart te worden gemeld. In plaats daarvan hoeft alleen de eenheid van handelingen te worden gemeld, bijvoorbeeld een klachtenregistratie of personeelsadministratie. Liggen de verwerkingsdoelen teveel uiteen (bijvoorbeeld enerzijds cameratoezicht voor de beveiliging van personeel en anderzijds het analyseren van de camerabeelden voor statistisch onderzoek), dan moeten er wel meerdere meldingen worden gedaan.

Voor de beoordeling of een verwerking vrijgesteld is van melding, kan gebruikgemaakt worden van de Handreiking Vrijstellingsbesluit Wbp.[8] Op grond van het Vrijstellingsbesluit Wbp zijn voor woningcorporaties onder meer de volgende verwerkingen van persoonsgegevens vrijgesteld van melding:

- gegevensverwerkingen met betrekking tot sollicitanten (artikel 5 Vrijstellingsbesluit);
- gegevensverwerkingen voor personeels- en salarisadministratie (artikelen 7 en 8 Vrijstellingsbesluit);

7 Het meldingenregister kunt u online raadplegen op de website van de AP: https://www.collegebeschermingpersoonsgegevens.nl/asp/orsearch.asp.
8 Online te raadplegen op de website van de AP: https://autoriteitpersoonsgegevens.nl/nl/melden/handreiking-vrijstellingsbesluit-wbp.

- gegevensverwerkingen in het kader van een verhuurovereenkomst die betrekking heeft op roerende of onroerende zaken, inclusief de gegevensverwerkingen met betrekking tot het aanvragen en verstrekken van huurtoeslag (artikel 14 Vrijstellingsbesluit);
- gegevensverwerkingen in het kader van de beveiliging, met behulp van duidelijk zichtbare videocamera's, van personen, gebouwen, terreinen, zaken en productieprocessen die zijn toevertrouwd aan de zorg van de verantwoordelijke (artikel 38 Vrijstellingsbesluit);[9]
- gegevensverwerkingen over personen die een bezwaarschrift of een klacht hebben ingediend bij de verantwoordelijke of ten aanzien waarvan een gerechtelijke procedure aanhangig is bij een rechterlijk college (artikel 39 Vrijstellingsbesluit);
- gegevensverwerkingen die nodig zijn voor communicatie met de betrokkene (artikel 42 Vrijstellingsbesluit).

Let op: in het Vrijstellingsbesluit wordt specifiek omschreven welke persoonsgegevens mogen worden verzameld, voor welk doel, aan welke partijen deze mogen worden verstrekt en hoe lang deze mogen worden bewaard. Er moet aan al deze criteria zijn voldaan. In geval van afwijkingen dient de verwerking alsnog gemeld te worden. Zo mogen gegevens van sollicitanten zonder toestemming van de sollicitant maar vier weken worden bewaard. Worden de gegevens langer bewaard, dan moet alsnog worden gemeld aan de AP.

5.2 MELDINGSPROCES

Melden kan zowel digitaal als schriftelijk[10] en de volgende gegevens bevatten (artikel 28 Wbp):

- de naam en het adres van de verantwoordelijke;
- het doel of de doeleinden van de verwerking waarvoor de gegevens of de categorieën van gegevens zijn of worden verzameld;
- een beschrijving van de categorieën van betrokkenen (zoals huurders of personeel) en van de gegevens of categorieën van gegevens (zoals NAW-gegevens) die daarop betrekking hebben;
- de ontvangers of categorieën van ontvangers aan wie de gegevens kunnen worden verstrekt;
- de voorgenomen doorgiften van gegevens naar landen buiten de Europese Unie;
- een algemene beschrijving over de genomen beveiligingsmaatregelen.

Melding van de verwerking dient plaats te vinden vóórdat de gegevens worden verzameld, omdat verzamelen al een vorm van verwerken is. Als een bepaalde gegevensverwerking nog niet is gemeld, dan is het raadzaam deze zo snel mogelijk te melden bij de AP. De melding is geldig vanaf het moment dat deze ontvangen is door de AP (u ontvangt een bevestiging).

Het is mogelijk om meldingen te wijzigingen of in te trekken. Wijzigingen dienen binnen een week gemeld te worden. Wijzigingen op de inhoud dienen binnen een jaar gemeld te worden, als ze structureel van aard zijn. Verwerkingen die afwijken van hetgeen eerder gemeld is, dienen te worden geregistreerd en voor minstens drie jaar te worden bewaard. Het moment van ontvangst van de wijziging of intrekking is de datum van inwerkingtreding.

5.3 DOCUMENTEREN

Gedane meldingen over gegevensverwerkingen moeten intern goed worden gedocumenteerd:

- Zorg dat de melding altijd onder dezelfde bedrijfsnaam wordt gedaan. Het meldingenregister heeft geen goede zoekfunctie, waardoor meldingen niet snel terug te vinden zijn voor betrokkenen als de naam iets afwijkt van bijvoorbeeld de handelsnaam.
- Houd altijd zelf een overzicht bij van de gedane meldingen met de daarbij behorende interne documentatie. Het kan voorkomen dat de inhoud van de melding er anders uitziet dan de gegevens die u intern heeft verzameld. Bewaar het bij elkaar!
- Houd een overzicht bij van de data waarop de meldingen zijn gedaan en/of gewijzigd en/of ingetrokken.

Voor een compleet overzicht van verwerkingen is het nuttig om ook de van melding vrijgestelde verwerkingsactiviteiten intern te administreren.

9 De Autoriteit Persoonsgegevens heeft begin 2016 beleidsregels omtrent cameratoezicht gepubliceerd: Beleidsregels cameratoezicht, Autoriteit Persoonsgegevens van 2 februari 2016, Stcrt. 2016, 4971. Online te raadplegen via: https://autoriteitpersoonsgegevens.nl/nl/nieuws/autoriteit-persoonsgegevens-publiceert-beleidsregels-cameratoezicht.

10 Meer informatie over het melden van gegevensverwerkingen op de website van de AP: https://autoriteitpersoonsgegevens.nl/nl/melden/meldingsprogramma.

5.4 VOORAFGAAND ONDERZOEK

Bepaalde verwerkingen van persoonsgegevens zijn dusdanig privacygevoelig dat deze voorafgaand moeten worden onderzocht door de AP (artikel 31 Wbp). De AP toetst dan of de verwerkingen in overeenstemming zijn met de wet. De verantwoordelijke is verplicht om zelf een dergelijk voorafgaand onderzoek aan te vragen via het meldingsformulier (artikel 32 lid 1 Wbp).[11] In sommige gevallen kan de AP naar aanleiding van een melding ook zelf besluiten dat een voorafgaand onderzoek verplicht is.

Een voorafgaand onderzoek moet, zoals al blijkt uit de bewoordingen, voorafgaand aan de daadwerkelijke gegevensverwerking worden aangevraagd en uitgevoerd. Gedurende het voorafgaand onderzoek moeten eventuele lopende verwerkingen dus worden gestaakt, totdat het onderzoek is afgerond of bericht is ontvangen dat er geen nader onderzoek zal plaatsvinden. Wordt de verwerking goedgekeurd, dan hoeven andere partijen dezelfde gegevensverwerkingen niet nogmaals voorafgaand te laten onderzoeken. De resultaten van het onderzoek gelden dan voor alle partijen. Denk bijvoorbeeld aan de goedkeuring van een gedeelde zwarte lijst. Sluit een andere corporatie zich ook aan bij deze zwarte lijst, dan hoeft de betreffende corporatie die zwarte lijst niet opnieuw te laten onderzoeken.

De volgende gegevensverwerkingen moeten in ieder geval worden onderworpen aan een voorafgaand onderzoek door de AP:

1. **Het gebruik van persoonsnummers voor een ander doel dan waarvoor de nummers specifiek bestemd zijn.**
   Het gaat hierbij niet alleen om de wettelijk voorgeschreven persoonsnummers, zoals een bsn, maar ook om alle persoonsnummers die bedoeld zijn om personen te identificeren, zoals IBAN-nummers. Als IBAN-nummers bijvoorbeeld niet alleen worden gebruikt om betalingen af te handelen maar ook om bestandskoppelingen mogelijk te maken met gegevens van andere organisaties, dan is een voorafgaand onderzoek waarschijnlijk verplicht. Zie voor meer informatie over burgerservicenummers paragraaf 12.4.2.

2. **Eigen onderzoek zonder inlichting van de betrokkene.**
   Normaal gesproken moet de verantwoordelijke de betrokkene informeren over gegevensverwerkingen (artikelen 33 en 34 Wbp). Gaat de verantwoordelijke op basis van eigen onderzoek gegevens verzamelen, dan blijft deze gegevensverwerking vaak ongemerkt voor de betrokkene. In die gevallen is een voorafgaand onderzoek verplicht. De term 'eigen onderzoek' is een ruime definitie. Hieronder vallen in ieder geval alle vormen van heimelijke observatie en heimelijk toezicht, zoals verborgen camera's en het in het geheim monitoren van communicatie. Ook *internetonderzoek* kan een vorm van heimelijke waarneming zijn, omdat hierbij ook gericht informatie wordt verzameld zonder de betrokkene daarvan op de hoogte te stellen. Het is aan te raden internetonderzoeken wél voor voorafgaand onderzoek aan te melden. De AP kan op basis van de melding altijd nog besluiten dat er geen nader onderzoek wordt gedaan.

3. **Verwerking van strafrechtelijke gegevens voor derden.**
   Worden voor derden strafrechtelijke gegevens verwerkt of gegevens over onrechtmatig of hinderlijk gedrag (zie voor de definitie paragraaf 12.1), dan moet eveneens een voorafgaand onderzoek worden ingesteld. Het gaat hierbij om het delen van kennis over onrechtmatig of strafrechtelijk gedrag, zoals een veroordeling voor hennepteelt. Een bekend en veelvoorkomend voorbeeld is het gebruik van zwarte lijsten die door meerdere organisaties kunnen worden ingezien. Zie voor meer informatie over grijze/zwarte lijsten paragraaf 12.2.

De AP zal na aanvraag van het voorbereidend onderzoek binnen vier weken nagaan of een voorbereidend onderzoek nodig is. Tegen het besluit naar aanleiding van dit voorafgaande onderzoek kan binnen zes weken bezwaar worden ingesteld. Indien nodig volgt na deze stap het nadere onderzoek. Op basis van het nadere onderzoek neemt de AP eerst een ontwerpbesluit waarop men kan reageren. Na zes weken volgt het definitieve besluit. Tegen dit besluit kan beroep worden ingesteld bij de rechtbank.

Let op: het uitvoeren van voorafgaande onderzoeken kan erg veel tijd in beslag nemen. Gedurende het onderzoek kunnen de gegevens niet worden verwerkt.

11 Het melden bij de FG is dan niet voldoende: een voorafgaand onderzoek moet altijd worden aangevraagd bij de AP.

5.5 MELDINGEN IN DE AVG

De verplichting om gegevensverwerkingen te melden vervalt met de inwerkingtreding van de AVG, omdat de Europese wetgevers vinden dat de verplichting teveel lasten oplevert en niet in alle gevallen bijdraagt aan een betere bescherming van persoonsgegevens. Wel moeten woningcorporaties met meer dan 250 werknemers een *intern register* bijhouden met een overzicht van alle verwerkingen die binnen de organisatie plaatsvinden (artikel 28 AVG). Woningcorporaties met minder dan 250 werknemers hoeven geen intern register bij te houden, tenzij:

- de verwerking die wordt verricht een risico zijn voor de rechten en vrijheden van de betrokkene en deze vaker dan incidenteel plaatsvinden, of;
- er bijzondere persoonsgegevens (zoals gezondheidsgegevens, biometrische gegevens en politieke opvattingen) of strafrechtelijke gegevens worden verwerkt. Let dus op! Als u zwarte of grijze lijsten heeft moet u per definitie een register bijhouden, ook al heeft u minder dan 250 medewerkers in dienst.

In het register wordt bijgehouden (artikel 28 lid 1 AVG):

1. de naam van de organisatie;
2. de doelen van de verwerkingen;
3. een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
4. de categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt, onder meer ontvangers in derde landen;
5. indien van toepassing, doorgiften van gegevens aan een derde land;
6. indien mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van gegevens moeten worden gewist;
7. indien mogelijk, een algemene beschrijving van de genomen beveiligingsmaatregelen.

Op verzoek moet het register ter beschikking worden gesteld aan de AP voor toezichtdoeleinden (artikel 28 lid 3 AVG).

6. BEVEILIGINGSMAATREGELEN

Persoonsgegevens moeten passend worden beveiligd. In de Wbp is deze plicht als een open norm geformuleerd. De wet spreekt van 'passende technische en organisatorische beveiligingsmaatregelen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking, of ter voorkoming van onnodige verzameling en verdere verwerking van persoonsgegevens' (artikel 13 Wbp). De wet vereist dus niet dat persoonsgegevens absoluut worden beveiligd, de beveiliging moet *passend* zijn.

Om vast te stellen wat passende beveiligingsmaatregelen zijn moet een afweging worden gemaakt op basis van de risico's van de verwerking aan de hand van onder meer de volgende punten:

- Het soort persoonsgegevens dat verwerkt wordt (normaal, bijzonder of gevoelig) en eventueel de daarbij behorende (risico)classificatie die de organisatie zelf aan de gegevens heeft gegeven.
- De hoeveelheid betrokkenen van wie gegevens worden verwerkt.
- Het doel waarvoor gegevens worden verwerkt.
- De duur en de wijze waarop gegevens bewaard moeten worden.

Eventueel kan dan nog worden meegewogen wat het eigen compliancedoel is. Wil de corporatie meer doen dan alleen de wet naleven? Dan is meer beveiliging misschien op zijn plaats. Zie voor een voorbeeld van de compliancedoelen bijlage 3.

Na het in kaart brengen van deze punten moet worden vastgesteld:

- wat de laatste stand van de techniek is, en;
- wat de kosten zijn.

Op basis van al deze informatie kan een afweging gemaakt worden over de wijze waarop de gegevens organisatorisch en technisch moeten worden beveiligd. De Autoriteit Persoonsgegevens heeft in 2013 een

uitgebreid document gepubliceerd over de beveiliging van persoonsgegevens.[12] Ook worden regelmatig onderzoeken en adviezen gepubliceerd die de 'stand van de techniek' verder invullen.[13]

Naast technische beveiliging zoals encryptie, zijn ook organisatorische beveiligingsmaatregelen relevant. Een voorbeeld van organisatorische beveiligingsmaatregelen (met een technische component) is het bepalen wie er toegang tot welke persoonsgegevens heeft en de mogelijkheid heeft om deze aan te passen (lees- en schrijfrechten).

Een onderdeel van organisatorische beveiliging van persoonsgegevens is ook dat de woningcorporatie met het personeel afspraken maakt over de plicht tot geheimhouding. Het is logisch om dergelijke geheimhoudingsverklaringen te laten tekenen voor aanvang van de arbeidsovereenkomst of wijziging van de functie. De verklaring moet dan in ieder geval in het personeelsdossier worden opgenomen. Personeelsleden die te maken hebben met extra gevoelige persoonsgegevens kunnen worden onderworpen aan een extra screening om de integriteit te waarborgen. Zo kan bijvoorbeeld het kunnen overleggen van een Verklaring omtrent gedrag (VOG) onderdeel uitmaken van de arbeidsovereenkomst.

6.1 BEVEILIGINGSBELEID

Een informatiebeveiligingsbeleid (hierna: IB-beleid) bevat de minimale beveiligingseisen van de woningcorporatie. Een gebruikelijk startpunt om een IB-beleid op te kunnen stellen is een risicoanalyse, zodat in kaart wordt gebracht waar de kwetsbaarheden en gevoelige gegevensverwerkingen in een woningcorporatie plaatsvinden. Bij deze risico's gaat het niet alleen om beveiligingsrisico's, maar ook om vragen als wat de gevolgen zijn als een systeem niet beschikbaar is, hoe lang een systeem niet beschikbaar mag zijn en tot welk niveau informatieverlies geaccepteerd kan worden. Op basis daarvan kan een gericht informatiebeveiligingsbeleid worden opgesteld die inspeelt op de specifieke behoefte van de woningcorporatie.

Naast het uitvoeren van een risicoanalyse moeten woningcorporaties rekening houden met eventuele andere van toepassing zijnde wet- en regelgeving op het gebied van informatiebeveiliging. Ook kunnen uit contractuele afspraken (bijvoorbeeld samenwerkingsverbanden over het uitwisselen van persoonsgegevens in het kader van hennepbestrijding) specifieke eisen voortvloeien over informatiebeveiliging. Deze dienen allemaal mee te worden genomen in het IB-beleid of daarvan afgeleid deelbeleid.

Op basis van de bevindingen van de risicoanalyse is het van belang om de beveiligingsmaatregelen te selecteren en te implementeren die erop gericht zijn de risico's te verlagen tot een acceptabel niveau. Te denken valt aan een autorisatiebeleid om te bepalen wie welke rechten heeft binnen een systeem of het gebruik van fysieke en omgevingsmaatregelen, zoals sloten, pasjes en alarmsystemen. Deze beveiligingsmaatregelen kunnen gebaseerd zijn op een bestaande standaard, zoals de ISO 27002, of ontworpen zijn voor de specifieke securityeisen van een organisatie.

Op welke wijze de risico's uiteindelijk aangepakt worden is een strategische keuze die onder andere afhankelijk is van de soort organisatie, de typen risico's, de toepasselijke wetgeving en de financiële middelen. Van belang is dat de implementatie van beveiligingsmaatregelen wordt uitgevoerd door de CISO of een andere soortgelijke functie waarbij informatiebeveiliging een kernverantwoordelijkheid is. Dit om te voorkomen dat informatiebeveiliging een ondergeschoven kindje wordt.

In een IB-beleid moeten, afhankelijk van de toepasselijke wet- en regelgeving, ten minste de volgende essentiële elementen terugkomen:

- bescherming van persoonsgegevens en privacy;
- bescherming van bedrijfsinformatie;
- bescherming van intellectuele eigendommen.

12 Richtsnoeren identificatie en verificatie van persoonsgegevens (Gebruik van 'kopietje paspoort' in de private sector), College Bescherming Persoonsgegevens van 12 juli 2012, Stcrt. 2012, 14741. Online te raadplegen via: https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/rs/rs_kopie-identiteitsbewijs.pdf.

13 Zoals verscherpt toezicht op het verouderde beveiligingsprotocol SSLv2: https://autoriteitpersoonsgegevens.nl/nl/nieuws/verscherpte-aandacht-ap-voor-verouderd-beveiligingsprotocol-sslv2.

Daarnaast maken ook de volgende aspecten onderdeel uit van een doorsnee IB-beleid:

- beleidsdocument met betrekking tot IB;
- vaststellen van verantwoordelijkheden met betrekking tot IB;
- IB awareness, training en opleiding;
- voorschriften met betrekking tot gegevensverwerkingen in systemen;
- management met betrekking tot technische kwetsbaarheden;
- management met betrekking tot IB-incidenten en verbeteringen.

Organisatiespecifieke risico's – die kenbaar gemaakt worden door een risicoanalyse – dienen ook mee te worden genomen in het IB-beleid. Daarnaast moeten, om te voorkomen dat het IB-beleid verouderd raakt, periodieke risicoanalyses uitgevoerd worden om de actuele risico's in kaart te brengen. Er is dus ook hier niet zoiets als een één-op-één toepasbaar IB-beleid. Het hierboven beschreven 'plan van aanpak' kan wel een uitgangspunt zijn voor het opstellen van een deugdelijk IB-beleid, maar het ontslaat woningcorporaties er niet van de eigen specifieke securityeisen en -wensen te onderzoeken en in beleid te omschrijven.

Baseline Informatiebeveiliging (woning)Corporaties (BIC)
In april 2016 is de Baseline Informatiebeveiliging (woning)Corporaties door NetwIT geïntroduceerd. Deze Baseline bevat richtlijnen en maatregelen op het gebied van informatiebeveiliging die voor iedere woningcorporatie geldt. Woningcorporaties hoeven nu dus niet langer Baselines van andere sectoren (zoals de Baseline Informatiebeveiliging Gemeenten, BIG) als handreiking te gebruiken.

De BIC is aan te vragen via bic@netwit.nl. Leden kunnen de BIC online raadplegen via: http://www.netwit.nl/publicaties/bic-en-meer.

6.2 PRIVACY BY DESIGN EN PRIVACY BY DEFAULT

Bij de aanschaf of ontwikkeling van nieuwe producten, systemen of processen dient de bescherming van persoonsgegevens steeds te worden meegenomen als een van de factoren om rekening mee te houden bij de beoordeling van de geschiktheid ervan. Deze factoren, ook wel bekend als privacy by design en privacy by default, zijn daarbij een pre.

Privacy by design heeft als doel het zo goed mogelijk beschermen van de privacy van betrokkenen. Bij privacy by design wordt al bij de eerste fase van de bouw van een informatiesysteem, product of proces rekening gehouden met alle relevante privacyaspecten. Het gaat daarbij om vragen als welke gegevens worden verzameld voor welke doelen, of deze gegevens daadwerkelijk nodig zijn voor het beoogde doel, welke bewerkingen er plaatsvinden, wie welke lees-, schrijf- en beheerrechten heeft en een bewaar- en verwijderbeleid met betrekking tot de verwerkte persoonsgegevens. Door bij het ontwerp al privacy te verankeren in het project is men goedkoper en efficiënter uit dan wanneer dit pas achteraf wordt onderzocht.

Privacy by design bestaat uit verschillende facetten die elk cruciaal zijn om persoonsgegevens zo goed mogelijk te beschermen. Bekende vormen daarvan zijn *Privacy Design Strategies* en *Privacy Enhancing Technologies* (PET's). Privacy Design Strategies zijn richtlijnen die aangeven hoe een systeemarchitectuur zo privacyvriendelijk mogelijk kan worden ingericht. Enkele kernprincipes daarbij zijn: dataminimalisatie, aggregatie en informeren. PET's zijn technische maatregelen gericht op het beschermen van de privacy door het elimineren of minimaliseren van (de uitwisseling van) persoonsgegevens, zoals het gescheiden opslaan van gegevens, toegangsbeveiliging en *logging* (waarmee wordt bijgehouden wie welke persoonsgegevens bewerkt en/of inziet).

Privacy by default gaat over de standaardinstellingen van een informatiesysteem, proces, dienst of product. Deze dienen zodanig te zijn ingesteld dat de privacy van de gebruiker optimaal wordt beschermd, zonder dat dit ten koste gaat van de algehele gebruiksvriendelijkheid. Denk bijvoorbeeld aan mobiele apps waarbij het delen van informatie standaard is uitgeschakeld, en het een actieve handeling van de gebruiker vereist om gegevens te delen. Het verschil met privacy by design is dat privacy by default ook in een latere fase kan worden meegenomen. Bovendien heeft privacy by default betrekking op de mogelijkheden voor de eindgebruiker om zijn privacy te beschermen, terwijl privacy by design wordt geïmplementeerd door de ontwikkelaars en beheerders van het informatiesysteem.

Privacy by design en default: voorbeelden

- Het oprichten van een online gebruiksportaal waarin de huurder zijn eigen persoonsgegevens kan inzien en wijzigen. Hiermee wordt het voor de huurder makkelijker om zijn recht op inzage en correctie uit te oefenen (zie ook paragraaf 11 over de rechten van betrokkenen).
- Registratieformulieren beperken tot het strikt noodzakelijke. Gegevens als een pasfoto en bsn hoeven bij de inschrijving als woningzoekende nog niet te worden opgevraagd. Door de woningzoekende bij registratie alleen te vragen naar de gegevens die nodig zijn voor woonruimtebemiddeling, wordt het principe van dataminimalisatie toegepast.
- Opt-in in plaats van opt-out. Als de betrokkene de mogelijkheid krijgt om deel te nemen aan een bepaalde regeling (bijvoorbeeld een niet-geanonimiseerd onderzoek), dan dient er een standaard te worden ingesteld. Bij opt-out doet de betrokkene automatisch mee, tenzij anders bepaald, terwijl bij opt-in de betrokkene standaard niet mee doet, tenzij hij zelf bepaalt wel mee te doen. Door het toepassen van opt-in in plaats van opt-out wordt de privacy van de betrokkene optimaal gewaarborgd.

6.3 BEVEILIGINGSMAATREGELEN IN DE AVG

Met ingang van de AVG is het verplicht om de beginselen van privacy by design en privacy by default toe te passen bij het nemen van beveiligingsmaatregelen (artikel 23 Wbp).[14] De AVG noemt enkele voorbeelden, waaronder het zo snel mogelijk pseudonimiseren van persoonsgegevens en het bieden van transparantie over de verwerking van persoonsgegevens. De beginselen van privacy by design en privacy by default moeten niet alleen worden toegepast bij nog te ontwikkelen systemen, maar ook bij bestaande systemen.

7. VERSTREKKING AAN DERDEN

Woningcorporaties wisselen veel persoonsgegevens uit met derde partijen. Het gaat dan vooral om gegevensuitwisselingen met de Belastingdienst, het Centraal Bureau voor de Statistiek (CBS), gemeenten, wijkteams, politie en andere ketenpartners – onder meer in het kader van preventie van woonfraude – maar ook met commerciële partijen, zoals Woningnet voor de uitvoering van een overeenkomst. Deze uitwisseling zal soms gebaseerd zijn op een wettelijke plicht en in sommige gevallen op aparte afspraken zoals convenanten.

Voor woningcorporaties is het steeds van belang om goed in kaart te brengen met wie, voor welk doel en op welke grond gegevens met derden worden uitgewisseld. Een goed voorbeeld biedt een woningcorporatie die de relaties met de verschillende partijen overzichtelijk in kaart gebracht heeft in een tabel, inclusief bijbehorende interne verantwoordelijken. Het maakt niet uit *hoe* uitwisselingen in kaart worden gebracht als ze maar in kaart *zijn* gebracht.

7.1 RECHTMATIGHEID VAN GEGEVENSUITWISSELING

Het delen van gegevens met derden is een verwerking van persoonsgegevens. Dit heeft tot gevolg dat aan alle normen van de Wbp voldaan moet worden. Zo is vereist dat er een grondslag is voor de verstrekking van persoonsgegevens, de gegevens alleen worden verstrekt voor een specifiek en vooraf bepaald doel, er voldoende beveiligingsmaatregelen zijn getroffen, de betrokkenen zijn geïnformeerd, et cetera. De Autoriteit Persoonsgegevens heeft een factsheet uitgebracht met daarin alle aandachtspunten over het delen van informatie in samenwerkingsverbanden.[15]

Het hangt helemaal van het doel, de grondslag en de soort persoonsgegevens af of de uitwisseling van de persoonsgegevens is toegestaan en welke specifieke waarborgen er moeten worden getroffen. De uitwisseling van strafrechtelijke gegevens heeft bijvoorbeeld vaak het karakter van zwarte/grijze lijsten en zijn daarom pas toegestaan na voorafgaand onderzoek. Ook over de uitwisseling van andere categorieën van bijzondere persoonsgegevens, zoals gezondheidsgegevens, heeft de wet bepaalde regels vastgesteld. Zie hiervoor paragraaf 11.

14 'The protection of the rights and freedoms of individuals with regard to the processing of personal data require that appropriate technical and organisational measures are taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures, which meet in particular the principles of data protection by design and data protection by default.'

15 Autoriteit Persoonsgegevens, Informatie delen in samenwerkingsverbanden, februari 2012. Online te raadplegen via: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/031_informatie_delen_in_samenwerkingsverbanden_feb_2012.pdf.

Als de woningcorporatie persoonsgegevens wil delen met andere partijen op grond van een gerechtvaardigd belang, dan kan dat alleen als de betrokkene daarvan op de hoogte is gesteld en het recht op verzet tegen verwerking van zijn persoonsgegevens kenbaar is gemaakt (artikel 40 Wbp). Zie voor nadere informatie de paragrafen over de informatieplicht en de rechten van betrokkenen.

Bij elk samenwerkingsverband waarbij persoonsgegevens worden uitgewisseld zijn (schriftelijke) afspraken over de uitwisseling van deze gegevens verplicht. Dit geldt ook voor gegevensuitwisselingen met overheidsinstellingen en gezondheids- en welzijnsorganisaties. Veel van deze uitwisselingen zijn namelijk niet wettelijk verplicht, waardoor de partijen zelf verplicht zijn om voldoende waarborgen vast te stellen bij de gegevensuitwisseling. Afspraken (in de vorm van bijvoorbeeld convenanten) alleen zijn echter niet voldoende om te handelen in overeenstemming met de Wbp, omdat de Wbp bepaalde eisen stelt aan het uitwisselen van persoonsgegevens. Een convenant alleen is daarom **geen garantie** voor compliance met de Wbp. Zo kunnen er bijvoorbeeld wel afspraken zijn gemaakt over de beveiliging, maar niet over de rechten van betrokkenen (zie paragraaf 11). In dat geval voldoet een convenant maar deels aan de Wbp.

Uit te wisselen gegevens
Een probleem dat in de praktijk vaak voorkomt bij het uitwisselen van gegevens is dat er door de samenwerkende partijen meer informatie wordt verstrekt dan nodig. Dit is niet alleen risicovol voor de verstrekker van de informatie, die mogelijk meer gegevens verstrekt dan toegestaan is op grond van de Wbp, maar ook voor de ontvanger van de informatie. Met name gevoelige gegevens (zie paragraaf 12) brengen namelijk een zware zorgplicht met zich mee om de gegevens zorgvuldig te bewaren.

Om deze problemen te voorkomen is het aan te raden om van tevoren in het samenwerkingsconvenant te bepalen welke partijen welke persoonsgegevens verstrekken. Met name bij gevoelige onderwerpen en persoonsgegevens, zoals de bemoeizorg, wordt het belang van het maken van dergelijke afspraken groter. Als er veel verschillende partijen zijn betrokken bij de informatie-uitwisseling kunnen de onderlinge afspraken ook worden weergegeven in een matrix. Een voorbeeld hiervan is de *Matrix gegevensuitwisseling bij uitvoering fraude Wmo en Jeugdwet* van de Vereniging van Nederlandse Gemeenten: https://vng.nl/files/vng/publicaties/2016/20160225_opzet_matrix_gegevensuitwisseling-fraudepreventie-jan_2016_v2.pdf.

7.2 BEWERKERSOVEREENKOMSTEN

Bewerkersovereenkomsten moeten worden afgesloten wanneer derden in opdracht van een verantwoordelijke persoonsgegevens verwerken. Deze derden worden bewerkers genoemd: degene die onder verantwoordelijkheid en in opdracht van de verantwoordelijke (de woningcorporatie) persoonsgegevens verwerkt, maar niet onder het gezag, of in hiërarchie ondergeschikt, van de verantwoordelijke staat. Te denken valt aan een softwareleverancier die software levert voor het beheer van het huurdersbestand en toegang heeft tot de persoonsgegevens van deze huurders. Ook andere externe dienstverleners, zoals deurwaarders en onderhoudsbedrijven kunnen bewerkers zijn als deze persoonsgegevens van de woningcorporatie verwerken. De gedachte achter deze bewerkersovereenkomst is dat de uitbesteding van de verwerking van persoonsgegevens de verantwoordelijke (zoals een woningcorporatie) niet ontslaat van zijn zorgplicht ten aanzien van de betrokkene. De Wbp noemt deze afspraken bewerkersovereenkomsten, maar bewerkersafspraken kunnen in verschillende andere overeenkomsten zijn opgenomen. De afspraken kennen dus niet altijd het opschrift 'bewerkersovereenkomst'.

Bewerkersovereenkomsten komen in vele soorten en maten voor, afhankelijk van de soort verwerkingen die plaatsvinden, de partij die optreedt als bewerker en de keuze voor gedetailleerdheid van de onderlinge afspraken. Zo ziet een bewerkersovereenkomst die wordt gesloten met een softwareleverancier er anders uit dan een bewerkersovereenkomst met een drukker. Ook de wijze waarop een bewerkersovereenkomst wordt gesloten kan verschillen. In de meeste gevallen wordt een losse bewerkersovereenkomst gesloten, met daarin uitgebreide afspraken over de verwerking van persoonsgegevens. In andere gevallen maken de afspraken met de bewerker onderdeel uit van een andere overeenkomst, zoals de algemene inkoopvoorwaarden of een geheimhoudingsovereenkomst.[16]

16 Om deze reden is het lastig om te verwijzen naar een modelbewerkersovereenkomst. Om toch een idee te krijgen van een bewerkersovereenkomst kan bijvoorbeeld worden gekeken naar die van het Rijk, de Model Bewerkersovereenkomst ARVODI. Online te raadplegen op: https://www.pianoo.nl/document/9596/modelbewerkersovereenkomst-arvodi.

De Wbp bepaalt niet precies wat er in de bewerkersovereenkomsten moet staan. In de praktijk komen in de verschillende bewerkersovereenkomsten globaal genomen wel dezelfde basiselementen voor, namelijk over de/het:

- onderwerp en doel van de overeenkomst;
- te verwerken persoonsgegevens;
- beveiligingsmaatregelen;
- bewaar-, back-up- en vernietigingsprocessen;
- verstrekking van persoonsgegevens aan derden;
- doorgifte van persoonsgegevens buiten de EU;
- overdracht en vernietiging van persoonsgegevens na afloop van de overeenkomst;
- geheimhouding;
- auditmogelijkheden;
- aansprakelijkheid.

Bij de bewerkersovereenkomsten moet ook rekening worden gehouden met de meldplicht datalekken. De verantwoordelijke (de woningcorporatie) moet er namelijk sinds 1 januari 2016 voor zorgen dat de bewerker maatregelen treft om aan de meldplicht datalekken te kunnen voldoen en toezien op de naleving hiervan (artikel 14 lid 1 en lid 3 sub c Wbp). Hierover meer in paragraaf 13.

7.2.1 Bewerkersovereenkomsten in de AVG

De bewerkersovereenkomsten zijn in de AVG uitgebreider geregeld dan in de Wbp. Artikel 26 AVG bepaalt in lid 1a bijvoorbeeld dat de bewerker (in de AVG aangeduid als de 'verwerker') geen andere bewerker (de 'subbewerker') in dienst mag nemen dan zonder voorafgaande toestemming van de verantwoordelijke. In bewerkersovereenkomsten zien we dit overigens nu ook al veel terugkomen in de vorm van een verplichting tot het verstrekken van informatie over subbewerkers.

In lid 2 is uitgewerkt welke elementen er verplicht in een bewerkersovereenkomst moeten worden opgenomen. Deze elementen komen grotendeels overeen met de bovengenoemde basiselementen, maar bevatten ook een aantal geëxpliciteerde plichten voor de bewerker, zoals de plicht om:

- de persoonsgegevens uitsluitend te verwerken op basis van de schriftelijke instructies van de verantwoordelijke;
- de vertrouwelijkheid in acht te nemen;
- bijstand te verlenen als de betrokkene een van zijn rechten uitoefent (zie over de rechten van betrokkenen meer in paragraaf 11);
- medewerking te verlenen bij audits;
- de verantwoordelijke op de hoogte te stellen indien de bewerker van mening is dat een bepaalde instructie in strijd is met de AVG;
- met een eventuele subbewerker dezelfde afspraken te maken als die gelden tussen de verantwoordelijke en de bewerker.

Het gros van deze elementen komen nu ook al terug in bewerkersovereenkomsten. Met de AVG komt hier echter een wettelijke verankering voor.

8. BEWAARTERMIJNEN

Op grond van artikel 10 Wbp mogen persoonsgegevens niet langer worden bewaard dan noodzakelijk. Hoe lang noodzakelijk is, is afhankelijk van de doelen van het verzamelen van de persoonsgegevens. Bij het bepalen van de bewaartermijnen zal daarom steeds moeten worden beargumenteerd waarom het bewaren van de gegevens daadwerkelijk nodig is voor het oorspronkelijke doel of andere, verenigbare doeleinden. Onder bepaalde voorwaarden mogen persoonsgegevens langer dan noodzakelijk bewaard worden, zoals voor statistisch of wetenschappelijk onderzoek.[17]

In de Wbp worden geen concrete bewaartermijnen genoemd. Specifieke bewaartermijnen zijn in afzonderlijke wetten geregeld. In het Vrijstellingsbesluit Wbp worden wel indicatie-bewaartermijnen genoemd voor een aantal veelvoorkomende verwerkingen van persoonsgegevens, zoals een personeelsadministratie (tot vijf jaar na

17 De Archiefwet is alleen van toepassing op documenten van de overheid.

beëindiging van het dienstverband, artikel 7 lid 5). Voor persoonsgegevens die worden verwerkt over huurders geldt een indicatietermijn van twee jaar nadat de huur is geëindigd (artikel 14 lid 5 Vrijstellingsbesluit Wbp). Wanneer persoonsgegevens niet langer worden bewaard dan de termijn genoemd in het Vrijstellingsbesluit, dan hoeft de verwerking niet te worden gemeld bij de AP. Worden de gegevens langer bewaard, dan moet de verwerking alsnog worden gemeld bij de AP.

Daarnaast moet er rekening worden gehouden met specifieke wetten die minimale bewaarplichten voorschrijven. Een belangrijke bewaarplicht is bijvoorbeeld de fiscale bewaarplicht van zeven jaar (artikel 47 Awr). Ook in de Woningwet zijn bewaartermijnen vastgesteld met betrekking tot de inkomensgegevens van huurders (artikel 55 Woningwet). Een overzicht van de belangrijkste wettelijke bewaarplichten is opgenomen in bijlage 1.

Wanneer persoonsgegevens onderworpen zijn aan verschillende bewaartermijnen, geldt als uitgangspunt dat per soort verwerking van persoonsgegevens de langste bewaartermijn aangehouden moet worden. Dit geldt uitdrukkelijk niet voor verschillende soorten persoonsgegevens die samen worden bewaard, bijvoorbeeld in een systeem. Een voorbeeld: wanneer de wet aangeeft dat persoonsgegevens vijf jaar bewaard moeten worden, maar er is een noodzaak om de persoonsgegevens langer te bewaren omdat er een juridisch geschil is, dan geldt deze langere termijn. Het is daarbij van belang dat alleen die gegevens (langer) worden bewaard die noodzakelijk zijn voor het doel. Het gaat niet per definitie om *alle* persoonsgegevens.

Bij het bepalen van de bewaartermijn zal aldus rekening moeten worden gehouden met de volgende factoren:
- het doel/de doelen waarvoor de persoonsgegevens verzameld zijn (de noodzaak om de gegevens voor dat doel te bewaren);
- vrijstellingsbesluit Wbp;
- wettelijke bewaartermijnen.

Bewaartermijnen in de praktijk: huurgegevens
Artikel 14 lid 5 Vrijstellingsbesluit Wbp voorziet in de specifieke bewaartermijn van twee jaar, nadat de huur is geëindigd voor het bewaren van gegevens omtrent huur en verhuur. De persoonsgegevens die zijn verstrekt voor het aanvragen en verstrekken van huurtoeslagen moeten worden bewaard tot uiterlijk vijf jaar nadat de huurtoeslag is geëindigd. Dit alles geldt tenzij het bewaren van de persoonsgegevens noodzakelijk is om te voldoen aan een (andere) wettelijke bewaarplicht. Een voorbeeld hiervan is de wettelijke fiscale bewaarplicht van zeven jaar van artikel 47 Awr. Deze regel geldt dus niet voor het complete dossier omtrent de verhuur van een woning, maar slechts voor een deel van de gegevens die voor belastingdoeleinden moet worden bewaard.

Juist omdat er zoveel verschillende bewaartermijnen zijn die zich uitstrekken over de verschillende werkprocessen, is een bewaar- en vernietigingsbeleid geen overbodige luxe.

8.1 VERNIETIGEN

Na afloop van de bewaartermijn dienen de gegevens op de juiste wijze te worden vernietigd. Dit kan op vele manieren. Met name bij gevoelige informatie moet de vernietiging zodanig zijn dat de gegevens niet meer kunnen worden teruggehaald. Er dient sprake te zijn van een zodanige vernietiging dat de kans dat de persoonsgegevens worden hersteld onmogelijk is (lees: slechts een theoretische kans bestaat dat dat mogelijk is). Hierbij gaat het dus niet om het plaatsen van de bestanden in de prullenbak en de prullenbak legen, maar om het overschrijven van data (*data wiping*). Standaard digitale verwijderprocessen op Windows-computers zijn dus vaak niet voldoende, omdat de gegevens dan nog kunnen worden teruggehaald.[18] Daarnaast moeten niet alleen de gegevens zelf, maar ook kopieën en back-ups na afloop van de bewaartermijn worden vernietigd.

In sommige gevallen is het niet praktisch om documenten te vernietigen, bijvoorbeeld omdat documenten voor meerdere doeleinden moeten worden bewaard en daardoor onderworpen zijn aan verschillende bewaartermijnen. Een alternatief voor vernietigen is het anonimiseren van gegevens. Deze anonimisering moet op zodanige wijze

18 Programma's als Recuva en Puran File Recovery maken het eenvoudig om verwijderde bestanden terug te halen. Met bepaalde software, zoals Eraser, is het terughalen van verwijderde gegevens kennelijk onmogelijk, doordat bestanden met data worden overschreven.

plaatsvinden dat de gegevens op geen enkele manier tot de persoon te herleiden zijn.[19] Dit is een strenge toets. Wordt bijvoorbeeld alleen de naam weggehaald maar niet het dossiernummer, dan is van anonimisering mogelijk geen sprake, omdat de betreffende persoon aan de hand van dat nummer nog te identificeren is.

Het bepalen van de bewaartermijn alleen is niet voldoende. Er dient daarnaast ook periodiek te worden gecontroleerd of het bewaren van persoonsgegevens in documenten nog noodzakelijk is. Voor die gevallen moet er een proces ingericht zijn om de persoonsgegevens voor het einde van de vooraf bepaalde bewaartermijn te vernietigen.

8.2 BEWAARTERMIJNEN IN DE AVG

Evenals de huidige Wbp bepaalt ook de AVG dat het verplicht is om bewaartermijnen te hanteren (artikel 5 sub e AVG). Nieuw ten opzichte van de Wbp is dat de AVG expliciet verplicht de bewaartermijnen bekend te maken aan de betrokkenen (artikel 14 e.v. AVG). Dit betekent dat in onder meer privacystatements en inzageverzoeken moet worden uitgelegd hoe lang de verzamelde gegevens worden bewaard of, als de bewaartermijn niet kan worden gegeven, de criteria die worden gehanteerd voor het bepalen van de bewaartermijn. Het is dus van belang om de bewaartermijnen expliciet vast te leggen in de organisatie, zodat deze in de toekomst ook kunnen worden gecommuniceerd naar huurders en andere partijen.

9. FUNCTIONARIS VOOR DE GEGEVENSBESCHERMING (FG)

Een aantal Nederlandse organisaties – voornamelijk grotere bedrijven en overheidslichamen – hebben een functionaris voor de gegevensbescherming (FG) ingesteld. Op grond van de Wbp staat het particuliere organisaties vrij om een FG aan te stellen. Een FG is een onafhankelijke persoon die toezicht houdt op naleving van de Wbp en adviseert over privacyvraagstukken binnen de organisatie. De FG moet bij de AP geregistreerd zijn (artikel 63 lid 3 Wbp).[20] Niet iedereen kan zomaar FG worden. De wet eist dat het gaat om een natuurlijk persoon 'die voor de vervulling van zijn taak over toereikende kennis beschikt en voldoende betrouwbaar kan worden geacht' (artikel 63 lid 1 Wbp). De onafhankelijkheid van de FG blijkt onder meer uit de wettelijke ontslagbescherming, dat de FG in de gelegenheid moet worden gesteld om zijn taken te kunnen uitoefenen en uit het feit dat hij geen aanwijzingen mag ontvangen van de organisatie die hem heeft benoemd (artikel 63 lid 2 Wbp).

De toezichthoudende bevoegdheden die normaal bij de AP liggen, worden met de inschrijving van de FG in het register van de AP in feite overgeheveld aan de FG. Zo hoeven gegevensverwerkingen niet te worden gemeld bij de AP, maar bij de FG. De FG is dus een interne toezichthouder, maar hij is *geen* verlengde arm van de Autoriteit Persoonsgegevens. Hij treedt enkel over bepaalde zaken in overleg met de AP en vormt het aanspreekpunt voor de AP.[21] De AP blijft bovendien in alle gevallen wettelijk bevoegd om haar bevoegdheden uit te oefenen. In de praktijk stelt de AP zich terughoudend op tegenover organisaties met een FG.[22]

9.1 FUNCTIONARIS VOOR DE GEGEVENSBESCHERMING IN DE AVG

De FG krijgt in de AVG een prominentere rol. Voor een aantal organisaties wordt de aanstelling van een FG verplicht (artikel 35 AVG).[23] Het gaat daarbij om:

- overheidsinstanties en overheidsorganen, met uitzondering van rechtbanken;
- organisaties die hoofdzakelijk belast zijn met verwerkingen die vanwege hun aard, hun omvang en/of hun doel regelmatige en stelselmatige observatie op grote schaal van betrokkenen vereisen;
- organisaties die hoofdzakelijk belast zijn met bijzondere categorieën van gegevens (bijvoorbeeld biometrische gegevens, gezondheidsgegevens, strafrechtelijke gegevens, et cetera).

Woningcorporaties lijken niet te vallen onder een van deze organisaties en zijn daarom ook met ingang van de AVG niet verplicht om een FG aan te stellen. De AP kan echter vaststellen dat voor corporaties wel een FG verplicht is.

19 CBP-richtsnoeren: beveiliging van persoonsgegevens van 1 maart 2013, Stcrt. 2013, 5174, p. 10, 25-26. Online te raadplegen via: https://autoriteitpersoonsgegevens.nl/nl/nieuws/cbp-publiceert-richtsnoeren-beveiliging-van-persoonsgegevens.
20 Zie voor het register: https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/functionaris-voor-de-gegevensbescherming.
21 Nederlands Genootschap van Functionarissen voor de Gegevensbescherming, 'Informatieblad – Relatie FG – CBP'. Online te raadplegen via: http://www.ngfg.nl/download.php?id=13.
22 Zie voor meer informatie: Autoriteit Consument & Markt, Veelgestelde vragen over de cookiebepaling, 14 juli 2015. Online te raadplegen via: https://www.acm.nl/nl/download/publicatie/?id=14496.
23 In eerdere versies van de AVG stond nog dat het aanstellen van een FG verplicht is bij organisaties met meer dan 250 werknemers of organisaties die van meer dan 5.000 betrokkenen persoonsgegevens verwerken. Deze zijn vervallen in de laatste versie van de AVG.

Ook in de AVG blijft het uitgangspunt dat de FG een onafhankelijke persoon is die moet beschikken over alle middelen en budgetten die nodig zijn om zijn toezichthoudende taken goed uit te kunnen voeren. Nieuw is dat in de verordening expliciet wordt bepaald dat de FG andere taken en plichten kan vervullen, maar dat deze taken niet tot een belangenconflict kunnen leiden (artikel 36 lid 4a AVG). Zo kan de FG waarschijnlijk niet ook security officer of compliance officer zijn: de FG zou dan immers zijn eigen beveiligingsbeleid kunnen goedkeuren.

Verder functioneert de FG als het communicatiekanaal tussen de betrokkene en de verantwoordelijke. Betrokkenen kunnen met de FG contact opnemen 'over alle aangelegenheden die verband houden met de verwerking van hun gegevens en met de uitoefening van hun rechten uit hoofde van deze verordening' (artikel 36 lid 2a AVG).

9.2 AANSTELLEN VAN EEN FUNCTIONARIS VOOR DE GEGEVENSBESCHERMING IN DE PRAKTIJK

Hoewel de AVG een FG niet verplicht stelt, kan het inzetten van een FG wel degelijk nuttig zijn om privacy compliant te blijven.

9.2.1 Profiel

De persoon voor de FG-functie moet in ieder geval beschikken over de volgende kwalificaties:

- uitgebreide kennis van het recht en de toepassing daarvan, inclusief kennis over technische en organisatorische maatregelen, privacy by design en default en over beveiliging;
- werkveld-specifieke kennis zowel qua grootte van de organisatie als met betrekking tot de gevoeligheid van de data;
- moet in staat zijn om inspecties en consultaties uit te voeren en documenten en logbestanden te analyseren;
- moet kunnen werken met de ondernemingsraad.

9.2.2 Taken

De functie van FG kan op verschillende manieren worden ingevuld. De eerste mogelijkheid is die van de FG als toezichthouder. De tweede mogelijkheid is dat de werkzaamheden van de FG een uitgebreidere reikwijdte krijgen. Beide taakverdelingen van de FG worden hieronder kort besproken.

Treedt de FG alleen op als *toezichthouder*, dan oefent de FG enkel de wettelijke bevoegdheden uit. De FG is dan uitdrukkelijk niet operationeel verantwoordelijk voor de implementatie en compliancereview van privacy in de organisatie: dit is de taak van andere medewerkers binnen de organisatie (zoals compliance officers). Deze personen zijn met andere woorden verantwoordelijk voor het advies en de implementatie van privacy en gegevensbescherming. De FG kan (afhankelijk van de grootte van de organisatie) ook een parttime positie zijn of een externe FG.

Indien de FG optreedt als toezichthouder, behoort tot het takenpakket van de FG:

- betrokkenheid bij alle zaken die bescherming van persoonsgegevens raken (artikel 36 AVG);
- zorgen voor awareness (artikel 37 AVG);
- monitoren van het beleid, de implementatie en de toepassing van het wettelijk kader (artikel 37 AVG);
- adviseren bij risicovolle projecten (arikel 34 en 37 AVG);
- monitoren van compliance en betrokkenheid bij compliance review (artikel 37 AVG);
- monitoren van de uitvoering van PIA's (artikelen 33 en 37 AVG);
- monitoren en updaten van documentatie, notificaties en communicaties met betrekking tot inbreuken op de beveiliging en kan optreden als woordvoerder (artikel 31 AVG);
- samenwerken met en optreden als contactpersoon voor de Autoriteit gegevensbescherming (artikel 37 AVG);
- optreden als contactpersoon voor de betrokkenen (artikel 36 AVG).

Treedt de FG op als toezichthouder, dan is het aan te raden om ook goed te kijken naar de inrichting van de compliance-afdeling. De FG treedt immers alleen op als toezichthouder en niet als uitvoerende verantwoordelijke. Deze uitvoerende functie wordt steeds belangrijker met de aanzienlijke boetedreigingen uit de AVG en de Wbp. Het financieel risico van non-compliance stijgt en daarmee dus ook het belang van een goed functionerende compliance office(r) naast een FG.

In de *uitgebreide reikwijdte* is de FG naast toezichthouder ook meer betrokken bij de ontwikkeling en implementatie van privacybeleid. Daarbij moet worden gedacht aan taken als:

- brede adviseringstaken, bijvoorbeeld over inzageverzoeken;
- de ontwikkeling van het privacybeleid, procedures en processen;
- het verrichten van periodieke onderzoeken met betrekking tot naleving van de wet;
- het verzorgen van cursussen en opleidingen voor de medewerkers.

Wordt ervoor gekozen om de FG ook verantwoordelijk te maken voor de implementatie van privacy en het daaropvolgende 'lifecycle management', houd er dan rekening mee dat de FG niet zomaar kan worden ontslagen bij disfunctioneren. Een ander nadeel is dat de FG door het uitgebreide takenpakket zowel als uitvoerder als toezichthouder optreedt en daarmee zijn eigen vlees keurt. Dit is een potentieel risico.

9.2.3 Intern of extern

Ten slotte biedt de wet de mogelijkheid om te kiezen voor interne of externe FG. Het zal afhangen van de inrichting en de keuze van de woningcorporatie welke situatie de voorkeur geniet.

Wat betreft de *interne* FG zijn de volgende voor- en nadelen:

Voordelen	Nadelen
+ De FG is veel aanwezig en dus zichtbaar in de organisatie + De FG kent de organisatie goed en dus ook de politieke gevoeligheden in een organisatie + Een voor de hele groep (bijvoorbeeld samenwerkende corporaties) aangestelde FG kan ook het groepsbelang behartigen	- De FG heeft mogelijk maar beperkte kennisopbouw, omdat er geen kennis is over de gang van zaken bij andere organisaties - De FG vervult mogelijk geen fulltime functie. Daardoor kunnen er moeilijkheden ontstaan bij het prioriteren van niet-FG-gerelateerde activiteiten. Hier kan belangenverstrengeling ontstaan.

Wat betreft de *externe* FG gelden de volgende voor- en nadelen:

Voordelen	Nadelen
+ De kennisopbouw is breder, omdat de FG ook kennis heeft over de gang van zaken bij andere organisaties + Kosteneffectiviteit, omdat de functie van FG niet altijd een fulltime baan is + De FG heeft als extern persoon geen enkel persoonlijk belang bij politieke gevoeligheden, en kan daardoor een meer onafhankelijke rol innemen + Een externe FG die ook voor andere corporaties werkzaam is, heeft veel sector-specifieke kennis en vaardigheden in huis en kan daarmee wellicht ook het groepsbelang beter overzien	- Minder een band met de organisatie en de gevoeligheden - Mogelijk conflict van belangen als de FG ook bij andere organisaties als FG optreedt. De FG kan bijvoorbeeld (onbedoeld) gevoelige bedrijfsinformatie delen met andere bedrijven waar hij ook werkzaam is als FG - De FG moet actief bij alle zaken betrokken worden, dit vereist een actievere rol van management

10. INFORMATIEPLICHT

Op basis van het transparantieprincipe hebben betrokkenen recht op informatie over de verwerking van hun persoonsgegevens. Dit is een uitwerking van de plicht tot zorgvuldige en behoorlijke verwerking van persoonsgegevens (zie paragraaf 1).

Op grond van artikel 33 Wbp geldt dat de verantwoordelijke vooraf informatie moet verstrekken over de details van de verwerking, tenzij de betrokkene hiervan reeds op de hoogte is. Dit is niet van toepassing als de verwerking wettelijk is voorgeschreven. In dat geval moet de verantwoordelijke alleen op verzoek mededelingen doen over het wettelijk voorschrift dat tot verwerking van de gegevens heeft geleid (artikel 34 lid 4 Wbp).

Toegepast op het verwerken van persoonsgegevens over huurders: zowel ten aanzien van het inschrijven van de persoon als woningzoekende, als het verzamelen van persoonsgegevens via het gebruik van de website, als bij het (voornemen tot het) sluiten van een huurovereenkomst moeten de betrokkenen dus duidelijk vooraf worden geïnformeerd over de verwerking van hun persoonsgegevens. Deze plicht geldt eveneens als huurders en woningzoekenden zelf de gegevens aanleveren. Ook als woningcorporaties een deel van hun diensten hebben uitbesteed aan een derde (bijvoorbeeld Woningnet of een andere intermediair), ontslaat hun dat niet van de verantwoordelijkheid om ook bij die derde te controleren of de informatievoorziening op orde is.

Het is uiteraard niet verboden om ook over het wettelijk voorschrift te informeren dat tot verwerking van persoonsgegevens heeft geleid. Dat verdient wellicht zelfs de voorkeur als ook andere informatie wordt verstrekt en voorkomt verwarring bij de betrokkene.

10.1 WIJZE VAN INFORMEREN

De wijze van informeren is niet voorgeschreven bij wet. Het is aan de individuele woningcorporaties zelf om daar een keuze in te maken. Een logische en voor de hand liggende keuze hiervoor is informeren door middel van een privacyverklaring, ook wel een privacystatement genoemd. Met name bij websites is het van belang dat het statement wordt getoond op een duidelijk zichtbare plek, en beschikbaar blijft op die plek wanneer binnen de website genavigeerd wordt door de gebruiker. Meestal wordt de voettekst (footer) van de website gekozen voor dit soort informatie.

Informeren via de website

Informeren kan op vele manieren. Een van de manieren die in de praktijk nog weleens voorkomt is het verwijzen naar het privacystatement op de website. Dit is niet altijd de beste manier als de huurovereenkomst schriftelijk wordt gesloten. Privacystatements op websites zien meestal specifiek op de persoonsgegevens die worden verzameld via de website en niet op de gegevens die worden verzameld voor het uitvoeren van de huurovereenkomst. Bovendien heeft nog niet elke huurder toegang tot internet, zoals ouderen. In plaats van het informeren van de website kan ervoor worden gekozen om het privacystatement te voegen aan de huurovereenkomst en mee te geven aan de huurder.

Het informeren via de website is overigens niet in alle gevallen af te raden. Als de woningzoekende zich online inschrijft als woningzoekende via bijvoorbeeld Woningnet of een andere website is het juist aan te raden om bij het inschrijfproces te verwijzen naar een privacystatement op de website (en te vragen om toestemming als dit nodig is!).

Het statement moet in duidelijke en heldere bewoordingen zijn geschreven, zodat het voor de gemiddelde huurder en woningzoekende te begrijpen is hoe zijn persoonsgegevens worden verwerkt. In de meeste gevallen is één privacystatement voor de hele organisatie voldoende. Als er voor verschillende activiteiten toch aparte privacystatements worden gemaakt, let dan extra goed op bij het beheer van de teksten, zodat generieke elementen steeds in alle statements gelijk zijn. Zorg dus voor goed versiebeheer, en zorg ook voor documenten met een datum!

10.2 MOMENT VAN INFORMEREN

Worden de persoonsgegevens bij de betrokkene zelf verkregen, dan is het van belang dat de betrokkene *vooraf* wordt geïnformeerd over de verwerking van zijn gegevens. Als persoonsgegevens over de betrokkene niet bij de betrokkene zelf worden verkregen maar elders, dan hoeft de betrokkene pas te worden geïnformeerd:

1. op het moment dat de betreffende persoonsgegevens worden vastgelegd, of
2. op het moment van de eerste verstrekking, wanneer de gegevens bestemd zijn om te worden verstrekt aan een derde.

Als gegevens worden verkregen van derden, dan is het niet altijd mogelijk om de betrokkene te achterhalen, bijvoorbeeld als uit de verkregen gegevens de identiteit of contactgegevens van de betrokkene niet direct blijken. In die gevallen, of in de gevallen waarin het onevenredig veel moeite zou kosten om de betrokkene te achterhalen,

hoeft de betrokkene niet te worden geïnformeerd (artikel 34 lid 4 Wbp). In dat geval moet de herkomst van de gegevens wel worden vastgelegd, zodat de betrokkene kan achterhalen welke keten van verstrekkingen heeft plaatsgevonden. De betrokkene hoeft ook niet te worden geïnformeerd als woningcorporaties gegevens verkrijgen op grond van een wettelijke bepaling (artikel 34 lid 5 Wbp). Uit de wet kan de betrokkene namelijk afleiden wie zijn of haar gegevens verwerkt.

10.3 INHOUD INFORMATIE

De verantwoordelijke moet de betrokkenen in ieder geval informeren over zijn identiteit en de doeleinden van de gegevensverwerking. Welke nadere informatie moet worden verstrekt bepaalt de Wbp niet specifiek. Artikel 33 en 34 lid 3 bepalen namelijk dat alle informatie moet worden verstrekt 'voor zover dat nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen'. Welke informatie verstrekt moet worden hangt af van de aard van de gegevens (maken de gegevens een grote inbreuk op de privacy?), de omstandigheden waaronder deze worden verkregen (wordt er uitdrukkelijk om gevraagd?) en het gebruik dat wordt gemaakt van de gegevens (ligt het gebruik voor de hand?). De verwachtingen van de betrokkenen zijn daarbij eveneens van belang: worden de gegevens bijvoorbeeld gebruikt voor doeleinden die niet direct voor de hand liggen, dan moet hierover uitgebreider worden geïnformeerd.

In de praktijk wordt meestal informatie verstrekt over de:

- identiteit en contactgegevens (zowel het fysieke adres als e-mailadres);
- doelen van de verwerkingen;
- (bijzondere) persoonsgegevens die worden verwerkt voor deze doelen;
- persoonsgegevens van minderjarigen;
- verstrekking aan derden;
- rechten van betrokkenen en de wijze waarop de betrokkenen hun rechten kunnen uitoefenen;
- bewaartermijnen;
- beveiliging;
- meldingsnummer van de gegevensverwerking(en) bij de AP (indien van toepassing), of althans een verwijzing naar het feit dat melding is gedaan.

In privacystatements of daarvoor apart opgestelde cookiestatements op websites moet ook aandacht worden besteed aan cookies, indien de website van de woningcorporatie daar gebruik van maakt. Cookies vallen niet alleen onder de Wbp, maar ook onder de Telecommunicatiewet en worden hier daarom niet besproken.[24]

Privacyverklaring generator

De overheid heeft begin 2016 in samenwerking met onder meer de Autoriteit Persoonsgegevens een website gelanceerd voor het genereren van een privacyverklaring. Deze is te vinden op: https://veiliginternetten.nl/privacyverklaring/. De generator is ook te gebruiken voor persoonsgegevens die worden verwerkt via een website (met uitzondering van cookies).

10.4 INFORMATIEPLICHT IN DE AVG

Privacystatements zullen moeten worden uitgebreid zodra de AVG in werking treedt. In tegenstelling tot de huidige wet bepaalt de AVG namelijk wél specifiek over welke elementen de betrokkene moet worden geïnformeerd (artikel 14 lid 1 en 1a, artikel 14a lid 1 en 2 AVG):

1. De identiteit van de verantwoordelijke en contactgegevens van de FG.
2. De doeleinden van de verwerking en de grondslag(en).
3. De categorieën persoonsgegevens die worden verwerkt.
4. De (categorieën van) ontvangers van de persoonsgegevens.
5. Doorgifte naar een derde land zonder passend beschermingsniveau.
6. Bewaartermijnen of de criteria voor het vaststellen van deze termijnen.
7. Indien gegevens worden verwerkt op basis van een gerechtvaardigd belang: een omschrijving van dit belang.

24 Zie voor meer informatie: Autoriteit Consument & Markt, Veelgestelde vragen over de cookiebepaling, 14 juli 2015. Online te raadplegen via: https://www.acm.nl/nl/download/publicatie/?id=14496.

8. Het bestaan van het recht op inzage, rectificatie, verwijdering, restrictie, verzet en dataportabiliteit.
9. Het recht om toestemming in te trekken.
10. Het recht om een klacht in te dienen bij de bevoegde autoriteit.
11. Het bestaan van geautomatiseerde besluitvorming en profilering (artikel 4 lid 3aa AVG).

Deze informatie hoeft, net als in de Wbp, niet te worden verstrekt als de betrokkene hier al van op de hoogte is.

Indien persoonsgegevens worden verkregen bij de betrokkene zelf (artikel 14 AVG), dan moeten woningcorporaties – naast de bovenstaande informatie – duidelijk aangeven of het aanleveren van bepaalde categorieën persoonsgegevens verplicht is en wat de mogelijke gevolgen zijn als deze gegevens niet worden verstrekt. Daarbij moet ook worden aangegeven of het verstrekken van de persoonsgegevens verplicht is op grond van de wet of de uitvoering van een contract of dat het aanleveren van bepaalde persoonsgegevens een noodzakelijke voorwaarde is om een overeenkomst te sluiten (artikel 14 lid 1a sub g AVG).

Worden persoonsgegevens niet verkregen bij de betrokkene zelf maar elders (artikel 14a AVG), dan moet de betrokkene – naast de bovenstaande informatie – ook worden geïnformeerd over de bron waar deze persoonsgegevens vandaan komen, ook als het gaat om openbare bronnen (artikel 14a lid 2 sub g AVG). Het moment waarop de betrokkene moet worden geïnformeerd als de persoonsgegevens elders worden verkregen verandert ook in de AVG. Artikel 14 lid 3 noemt de volgende momenten:
1. binnen een redelijke termijn, maar uiterlijk binnen één maand na het verkrijgen van de gegevens, afhankelijk van de concrete omstandigheden waarin de gegevens worden verwerkt; of
2. indien de gegevens zullen worden gebruikt voor communicatie met de betrokkene, uiterlijk op het moment van het eerste contact met de betrokkene; of
3. indien verstrekking van de gegevens aan een andere ontvanger wordt overwogen, uiterlijk op het tijdstip waarop de gegevens voor het eerst worden verstrekt.

De betrokkene hoeft net als in de Wbp niet te worden ingelicht als de betrokkene al over de informatie beschikt, het verstrekken van de informatie onevenredig veel inspanning kost of het verkrijgen of verstrekken van de gegevens wettelijk is voorgeschreven (art. 14a lid 4 AVG).

Worden de persoonsgegevens (bij de betrokkene verkregen of niet) verder verwerkt voor een ander doel dan waarvoor deze zijn verkregen, dan moet de verantwoordelijke vóór die verdere verwerking informatie over dat andere doel en alle relevante informatie uit punt 6 tot en met 11 uit bovenstaande opsomming verstrekken.

11. RECHTEN VAN BETROKKENEN

In het verlengde van de plicht tot informeren over de gegevensverwerking, heeft de betrokkene ook recht op inzage (artikel 35 Wbp), verbetering, aanvulling, verwijdering en afscherming (artikel 36 Wbp) en het recht op verzet (artikelen 40 en 41 Wbp) ten aanzien van de verwerking van diens persoonsgegevens. Daarnaast heeft de betrokkene het recht niet te worden onderworpen aan geautomatiseerde individuele besluiten (artikel 42 Wbp).

11.1 INZAGE

Betrokkenen hebben recht op inzage in hun persoonsgegevens die de verantwoordelijke van hem verwerkt. De betrokkene hoeft geen reden op te geven voor zijn inzageverzoek ('vrijelijk'), maar hij mag niet onevenredig veel verzoeken in korte tijd indienen ('met redelijke tussenpozen'). Als een betrokkene vraagt om inzage, dan heeft de betrokkene recht op een *volledig overzicht* van de verwerkte gegevens, de herkomst van de gegevens, de ontvangers van de gegevens en de doelen van de verwerking van de persoonsgegevens. In de praktijk gebeurt dit vaak door een kopie van de documenten (digitaal) te verstrekken.

De informatie moet in begrijpelijke vorm worden verstrekt. Het moet met andere woorden duidelijk zijn voor de betrokkene wat er in de overhandigde documenten staat. Met name bij bepaalde technische gegevens moet dit aspect goed in het oog worden gehouden.

De volgende informatie hoeft *niet* te worden overhandigd bij een inzageverzoek:

- *Persoonlijke werkaantekeningen en notities voor intern gebruik*. Te denken valt aan interne e-mails voor overleg. Maken de gegevens uit deze e-mails onderdeel uit van het dossier, dan moeten deze gegevens wel worden overhandigd. Houd er rekening mee dat deze aantekeningen in het dossier netjes zijn geformuleerd.
- Documenten waarin *persoonsgegevens van derden* zijn opgenomen, bijvoorbeeld een klacht over een huurder die is ingediend door de buurman. In deze gevallen moet een afweging worden gemaakt tussen enerzijds het recht van de betrokkene (de huurder) om de persoonsgegevens in te zien en anderzijds de privacyinbreuk op de derde (de buurman). Weegt het belang van de derde zwaarder, dan kan inzage in de persoonsgegevens worden geweigerd. Afschriften van deze documenten mogen dan alleen worden verstrekt als de persoonsgegevens van de derde voldoende zijn afgeschermd. Het kan ook zijn dat de betrokkene een zwaarwegend belang heeft en daardoor wel recht heeft op inzage. In dat geval moeten de betreffende derden eerst op de hoogte worden gesteld van het verstrekken van de documenten en moet hen de mogelijkheid worden gegeven om hun zienswijze aan te leveren (artikel 35 lid 3 Wbp).
- Persoonsgegevens die worden gebruikt in het kader van de *voorkoming, opsporing en vervolging van strafbare feiten* en andere gevallen genoemd in de uitzonderingen van artikel 43 Wbp.

11.2 CORRECTIE EN VERWIJDERING

Naast een recht op inzage heeft de betrokkene ook recht op correctie en verwijdering van de persoonsgegevens. Dit houdt in dat hij kan verzoeken om de gegevens te verbeteren, aan te vullen, te verwijderen of af te schermen. Zo'n verzoek hoeft alleen te worden gehonoreerd als de gegevens onjuist zijn, onvolledig zijn voor het doel waarvoor de gegevens worden verzameld of als deze niet ter zake dienend zijn of in strijd met de wet (zoals de Wbp) worden verwerkt. De betrokkene moet in zijn verzoek duidelijk aangeven welke gegevens om welke reden moeten worden aangepast. Het recht kan niet worden gebruikt om meningen of onderzoeksresultaten te wijzigen. Als het correctieverzoek wordt gehonoreerd, dan moeten de wijzigingen zo snel mogelijk worden doorgevoerd.

Wijzigt of verwijdert een verantwoordelijke persoonsgegevens, dan moet deze wijziging of verwijdering ook worden doorgegeven aan andere partijen aan wie de gegevens in het verleden zijn verstrekt (artikel 38 Wbp). In ketensamenwerkingen betekent dit dat niet alleen dat de gegevens in de eigen database moeten worden aangepast, maar ook bij de andere ketenpartners. Deze plicht hoeft niet te worden uitgevoerd als deze kennisgeving onmogelijk is of onevenredige inspanning kost. Hoeveel moeite de verantwoordelijke moet doen, hangt af van de soort verbetering en de gevoeligheid van de gegevens. Hierover kunnen ook afspraken worden gemaakt in bewerkersovereenkomsten. Zoals eerder aangegeven wordt datakwaliteit steeds belangrijker bij uitwisseling van gegevens. Als doorgifte van wijziging of verwijdering van informatie procesmatig goed is doorgevoerd, zorgt dit ook voor het in stand houden van het kwaliteitsniveau van de informatie.

11.3 VERZET

De betrokkene heeft in sommige gevallen de mogelijkheid om zich te verzetten tegen het verwerken van zijn persoonsgegevens: de betrokken organisatie mag de gegevens dan niet meer gebruiken, ook al is de gegevensverwerking op zich gerechtvaardigd. Er zijn twee vormen van verzet: een relatief recht van verzet en een absoluut recht van verzet.

Het relatieve recht van verzet is mogelijk bij bijzondere persoonlijke omstandigheden van de betrokkene en de grondslag voor gegevensverwerking is gebaseerd op artikel 8 sub e (publieke taak) of sub f (gerechtvaardigd belang). De verantwoordelijke moet hierbij binnen vier weken na ontvangst van het verzet beoordelen of hij het verzet al dan niet honoreert, en maakt daarbij een belangenafweging tussen zijn belang tot verwerking en het belang van de betrokkene. Er kan geen verzet worden aangetekend tegen openbare registers die bij wet zijn ingesteld.

Het absolute recht van verzet houdt in dat de betrokkene zich altijd kan verzetten bij het gebruik van zijn persoonsgegevens voor direct marketing-doeleinden (het individueel benaderen van personen voor commerciële of liefdadigheidsdoelen). Honorering van het verzet geschiedt dus per definitie. Een voorbeeld hiervan is het bericht onderaan een digitale nieuwsbrief waarin staat dat uitgeschreven kan worden voor de nieuwsbrief. Huis-aan-huisbladen en marktonderzoeken vallen hier niet onder, omdat deze niet vallen onder de definitie van direct marketing.

11.4 GEAUTOMATISEERDE INDIVIDUELE BESLUITVORMING

In tegenstelling tot de vorige drie rechten is de vierde bepaling niet zozeer een recht dat de betrokkene kan uitoefenen, maar eerder een verbod voor de verantwoordelijke. Artikel 42 Wbp bepaalt dat er geen finale besluiten mogen worden genomen op basis van profielschetsen die geautomatiseerd tot stand zijn gekomen en deze besluiten de betrokkene 'in aanmerkelijke mate' treffen. Te denken valt aan profielen die automatisch worden gegenereerd ('profiling') en iemands betrouwbaarheid beoordelen. Als een dergelijk geautomatiseerd profiel er direct toe leidt dat iemand bijvoorbeeld niet in aanmerking komt voor een huurwoning (bijvoorbeeld omdat hij op basis van het gegenereerde profiel als onbetrouwbaar wordt aangemerkt), dan is dit in strijd met artikel 42. Met andere woorden: het geautomatiseerd opgestelde profiel mag niet de enige reden zijn voor een bepaald besluit over een persoon zonder daadwerkelijke menselijke tussenkomst. Reden hiervoor is dat een profiel mogelijk voor andere interpretatie vatbaar is.

Het een en ander betekent overigens *niet* dat geautomatiseerde profielen niet mogen worden gebruikt bij de besluitvorming. De wet stelt alleen dat het gegenereerde profiel niet zomaar het enige aspect is dat de besluitvorming kan bepalen. De betrokkene moet in staat gesteld worden om zijn zienswijze naar voren te brengen om een eventuele herbeoordeling te krijgen, hierbij is menselijke tussenkomst dus van belang. Voorbeelden van dergelijke besluitvormingsprocessen zijn onder meer kredietwaardigheidsprofielen (credit scores), toe-of afwijzingen van subsidies en betrouwbaarheidsanalyses.

11.5 ALGEMENE OPMERKINGEN

Ten aanzien van de rechten van betrokkenen is het van belang dat:

- de betrokkene zich identificeert (artikel 37 Wbp, zie ook hierna, onder paragraaf 11.6);
- binnen vier weken wordt gereageerd op het verzoek. Wordt het verzoek geweigerd, dan moet ook gemotiveerd worden aangegeven waarom;
- niet alleen documenten, maar ook beeld- en geluidsmateriaal onder de regels vallen[25];
- inzage- en correctieverzoeken die zien op persoonsgegevens van minderjarigen (kinderen onder de 16) of onder curatele gestelden worden ingediend door hun wettelijke vertegenwoordigers (de ouders of de curator);
- alleen bij inzageverzoeken en verzetverzoeken (beperkte) kosten in rekening mogen worden gebracht. De hoogte van de kosten die in rekening mag worden gebracht, is geregeld in het Besluit kostenvergoeding rechten betrokkene Wbp.[26] Als naar aanleiding van het inzageverzoek wordt overgegaan tot correctie of verwijdering van de gegevens, dan moet de vergoeding worden teruggegeven.

11.6 RECHTEN VAN BETROKKENEN IN DE PRAKTIJK

Bij de afhandeling van verzoeken van betrokkenen in de praktijk is het van belang dat hiervoor een proces is ingericht, waarbij ook de taken en verantwoordelijkheden zijn vastgelegd. Dit proces moet niet alleen intern helder zijn, het is verstandig om ook tegenover de betrokkene duidelijk te maken hoe verzoeken worden afgehandeld. Houd er bij het opstellen van het interne proces rekening mee dat er te allen tijde medewerkers klaar moeten staan om het verzoek in ontvangst te nemen en af te handelen. De termijn van vier weken geldt immers ook als medewerkers op vakantie zijn!

Houd rekening met de volgende aspecten:

1. **Intake**
   Het moet zowel binnen de organisatie als voor de betrokkene duidelijk zijn bij welke personen verzoeken kunnen worden ingediend. De communicatie naar de betrokkene vindt meestal plaats door contactgegevens op te nemen in het privacystatement (op de website).

2. **Self service**
   Met behulp van online gebruikersportalen is het steeds eenvoudiger om betrokkenen hun eigen gegevens in te laten zien, te wijzigen en te laten verwijderen. Dit levert ook werkbesparing op: de ontwikkeling van dergelijke portalen is soms economisch voordeliger dan het inschakelen van meer medewerkers. Indien er al gebruik wordt gemaakt van gebruikersportalen is het verstandig om betrokkenen erop te wijzen welke gegevens zij zelf kunnen inzien en aanpassen.

25 Deze moeten dan wel onderdeel uitmaken van een 'bestand' in de zin van de Wbp.
26 Zie http://wetten.overheid.nl/BWBR0012565/2012-07-01.

3. **Samenwerking met derden**
   Bij elke procesbeschrijving is het van belang dat van tevoren helder is welke medewerkers of afdeling(en) verantwoordelijk is/zijn voor de afhandeling van bepaalde taken. Daarnaast moet in het oog worden gehouden met welke derde partijen samengewerkt moet worden om het verzoek af te kunnen handelen. Indien er bijvoorbeeld gegevens moeten worden gewijzigd bij Woningnet, dan is het van belang dat er een contactpersoon bij Woningnet is aangewezen die in staat is de gegevens te wijzigen. Deze medewerkingsplicht bij de afhandeling van verzoeken van betrokkenen wordt vaak ook opgenomen in bewerkersovereenkomsten. Houd er verder rekening mee dat goedgekeurde correctie- en verwijderverzoeken ook moeten worden gecommuniceerd naar andere partijen aan wie de gegevens in het verleden zijn verstrekt. Het verdient aanbeveling om een contactenlijst van alle ketenpartners op te stellen die moet worden geraadpleegd bij bepaalde gegevensverwerkingen.

4. **Identificatie**
   Voordat een verzoek in behandeling wordt genomen moet de betrokkene zich eerst hebben geïdentificeerd. Maak duidelijk naar zowel de medewerkers (bijvoorbeeld door middel van callscripts) als de betrokkene dat verzoeken niet in behandeling worden genomen als de betrokkene zich niet goed heeft geïdentificeerd. In de praktijk gebeurt dit meestal door inlogpagina's van gebruiksportalen of door te vragen om een kopie van het ID-bewijs waarbij het bsn onzichtbaar is gemaakt. Burgerservicenummers mogen namelijk maar zeer beperkt worden verwerkt (zie paragraaf 12.4.2). Om te voorkomen dat ID-kopietjes nodeloos worden bewaard kan het ook een goed alternatief zijn om de betrokkene te vragen langs te laten komen en zijn ID-kaart te tonen; het is dan niet meer nodig een kopie van het ID-bewijs te maken, een notitie van een medewerker dat het ID-bewijs is getoond is dan voldoende.

5. **Klachtenregeling**
   Sommige verantwoordelijken bieden een klachtenregeling aan voor betrokkenen. De klacht wordt dan in behandeling genomen door personen die niet betrokken zijn geweest bij de eerste beoordeling van het verzoek. Een dergelijke regeling voor de rechten van betrokkenen is juridisch gezien niet verplicht: betrokkenen hebben de mogelijkheid om de Autoriteit Persoonsgegevens in te schakelen of om hun recht bij de rechter af te dwingen. Niettemin kan een klachtenprocedure zowel voor een woningcorporatie als een betrokkene voordelig zijn. Woningcorporaties hebben namelijk de mogelijkheid rechtszaken te voorkomen en eventuele fouten te herstellen, terwijl betrokkenen een lagere drempel hebben om hun rechten af te dwingen. Het is aan de woningcorporatie om hier een afweging in te maken.

11.7 RECHTEN VAN BETROKKENEN IN DE AVG

De rechten van betrokkenen worden uitgebreid en versterkt in de AVG. Bij het recht op inzage moet naast informatie over de verwerkte categorieën persoonsgegevens en de doelen waarvoor deze zijn verzameld ook informatie verstrekt worden over onder meer de bewaartermijn van de gegevens, het recht op rectificatie en of de persoonsgegevens zijn doorgegeven buiten de Europese Unie (artikel 15 AVG). Wanneer de betrokkene zijn inzageverzoek elektronisch indient, moet de informatie ook in elektronische vorm (bijvoorbeeld in pdf-formaat) worden aangeleverd.

Het correctierecht (artikel 16 AVG) is nauwelijks veranderd in de verordening, terwijl het recht op verwijdering (arikel 17 AVG) flink op de schop is gegaan. De verantwoordelijke is op grond van het verwijderrecht (ook wel aangeduid als het recht om vergeten te worden) namelijk verplicht zo snel mogelijk de persoonsgegevens uit te wissen als:

1. de gegevens niet langer nodig zijn voor de doelen waarvoor ze zijn verwerkt;
2. toestemming is ingetrokken door de betrokkene en er geen andere grond is voor de verwerking van de gegevens;
3. de betrokkene bezwaar heeft gemaakt tegen de verwerking van de gegevens;
4. de gegevens onrechtmatig zijn verwerkt;
5. verwijdering verplicht is op grond van de wet;
6. de gegevens zijn verzameld in verband met een aanbod van diensten van de informatiemaatschappij.

Zijn de gegevens in kwestie door de verantwoordelijke openbaar gemaakt, dan is de verantwoordelijke ook verplicht andere verantwoordelijken die de gegevens hebben verwerkt op de hoogte te stellen van het verzoek van de betrokkene.

In de AVG worden een tweetal nieuwe rechten geïntroduceerd. Het gaat daarbij om het recht op beperking van de verwerking van zijn persoonsgegevens (artikel 17a AVG) en het recht op gegevensoverdraagbaarheid, ofwel dataportabiliteit (artikel 18 AVG). Bij het eerstgenoemde recht kan de betrokkene elke vorm van verwerking (met uitzondering van opslag) beperken, bijvoorbeeld als hij de gegevens nodig heeft in een rechtszaak of als de juistheid van de gegevens door de betrokkene wordt betwist. Het recht op gegevensoverdraagbaarheid houdt in dat de betrokkene de persoonsgegevens – die hij in het verleden aan de verantwoordelijke heeft verstrekt – in een overdraagbaar bestandsformaat aangeleverd kan krijgen van de verantwoordelijke. Zo kan de betrokkene de gegevens eenvoudig overdragen naar een andere verantwoordelijke.

12. BIJZONDERE PERSOONSGEGEVENS

Op grond van artikel 16 Wbp worden bepaalde soorten persoonsgegevens aan een speciaal regime onderworpen. Deze zogenaamde bijzondere persoonsgegevens zijn gegevens die naar hun aard heel gevoelig zijn; gegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag. De wet verbiedt de verwerking van deze gegevens behoudens wettelijke uitzonderingen. Deze uitzonderingen zijn neergelegd in artikel 17 tot en met 23 van de Wbp. In artikel 17 tot en met 22 gaat het om uitzonderingen die elk zien op een specifieke categorie van persoonsgegevens. Artikel 23 biedt nog een aantal algemene uitzonderingen op het verwerkingsverbod op bijzondere persoonsgegevens.

Daarnaast zijn er verwerkingen die weliswaar niet onder het bijzonder regime van artikel 16 Wbp vallen, maar wel als gevoelig kunnen worden aangemerkt, zoals de gegevens van bepaalde doelgroepen – bijvoorbeeld kinderen –, gegevens rondom iemands financiële situatie en burgerservicenummers. Ook kunnen op zichzelf niet-gevoelige gegevens in een gevoelige context als gevoelig aangemerkt worden, zoals naam en adres in een patiëntenbestand. Met al deze gegevens moet zeer vertrouwelijk worden omgegaan gelet op de hoge privacygevoeligheid van de gegevens.

Een aspect dat extra aandacht verdient bij het verwerken van bijzondere en gevoelige persoonsgegevens in zijn algemeen is de geheimhoudingsplicht.[27] De wet legt ook aan woningcorporaties een geheimhoudingsplicht op ten aanzien van vele categorieën van bijzondere en gevoelige gegevens. Zo geldt een wettelijke geheimhoudingsplicht ten aanzien van politiegegevens (artikel 7 Wet Politiegegevens) en het huishoudinkomen (artikel 55 lid 4 Woningwet). Deze geheimhoudingsplicht houdt tevens in dat de verstrekking van gegevens aan derden buiten de woningcorporatie maar beperkt mogelijk is.

12.1 STRAFRECHTELIJKE GEGEVENS

Een belangrijke categorie van bijzondere persoonsgegevens is de categorie strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod. De term ‘strafrechtelijke gegevens’ wordt ruim gedefinieerd. Hieronder vallen niet alleen alle gegevens die betrekking hebben op rechterlijke veroordelingen, maar ook de min of meer gegronde verdenkingen (concrete aanwijzingen dat een persoon een strafbaar feit heeft gepleegd). Strafrechtelijke gegevens zijn ook gegevens over strafbaar gesteld gedrag dat niét tot politieoptreden heeft geleid.

Een belangrijke uitzondering om strafrechtelijke gegevens te verwerken is te vinden in artikel 22 lid 2 en 3 Wbp. Lid 2 maakt het mogelijk om strafrechtelijke gegevens te verwerken als de verantwoordelijke slachtoffer is of dreigt te worden van een derde, zoals een huurder. Als de woningcorporatie bijvoorbeeld te maken heeft met een notoire fraudeur, dan mag de woningcorporatie de gegevens van deze persoon verwerken voor zover dat noodzakelijk is ter zelfbescherming. Lid 3 biedt de mogelijkheid om strafrechtelijke gegevens te verwerken over het eigen personeel. Hiertoe moeten regels worden vastgesteld in overleg met de ondernemingsraad.

Voor alle uitzonderingen op het verwerken van strafrechtelijke gegevens geldt dat deze gegevens alleen voor *intern gebruik* bestemd zijn. Met andere woorden, als er strafrechtelijke gegevens worden verwerkt ter zelfbescherming, dan mogen deze gegevens alleen intern worden geregistreerd. De gegevens mogen niet worden gedeeld met

27 De geheimhoudingsplicht moet los worden gezien van het verschoningsrecht, die bepaalde beroepsbeoefenaars ontslaat van de plicht om een verklaring af te leggen tegenover de rechter of de politie. Koninklijke Nederlandsche Maatschappij ter bevordering der Geneeskunst, Richtlijnen inzake het omgaan met medische gegevens, 1 januari 2010, p. 14 e.v. Online te raadplegen via: http://www.knmg.nl/web/file?uuid=22fc4006-11c8-4d00-8086-806e4a016a8c&owner=a8a9ce0e-f42b-47a5-960e-be08025b7b04&contentid=71232.

andere woningcorporaties. Artikel 22 lid 4 Wbp biedt hierop een aantal uitzonderingsmogelijkheden. Zo is het delen van gegevens mogelijk binnen een concern toegestaan (artikel 22 lid 4 sub b Wbp). Overkoepelende brancheorganisaties zoals Aedes vallen hier echter *niet* onder! Het delen van strafrechtelijke gegevens met andere organisaties is toegestaan als er 'passende en specifieke waarborgen zijn getroffen en de procedure is gevolgd, bedoeld in artikel 31'. Zie hierover meer in de volgende paragraaf over gedeelde grijze/zwarte lijsten.

12.2 GRIJZE/ZWARTE LIJSTEN

Woningcorporaties maken soms gebruik van waarschuwingslijsten (ook wel zwarte of grijze lijsten genoemd) om problematische huurders in kaart te brengen. Het kan daarbij gaan om huurders die woonfraude, huurachterstand en/of hinderlijk gedrag hebben gepleegd. Hierbij worden vrijwel altijd strafrechtelijke gegevens van huurders verwerkt. Zoals hierboven reeds is uitgelegd zijn dit bijzondere persoonsgegevens, die volgens de Wbp extra bescherming verdienen.

12.2.1 Gedeelde grijze/zwarte lijsten

Het gebruiken van een grijze/zwarte lijst voor intern gebruik is toegestaan als wordt voldaan aan de voorwaarden van artikel 22 lid 2 Wbp (zie hierboven). Als een grijze/zwarte lijst niet alleen intern wordt gebruikt, maar ook wordt gedeeld met anderen, dan is de woningcorporatie verplicht een voorafgaand onderzoek aan te vragen bij de AP (en de gegevensverwerking te melden bij de AP). Dit blijkt uit artikel 22 lid 4 sub c Wbp, waarin is bepaald dat het delen van strafrechtelijke gegevens ten behoeve van derden moet worden onderzocht door de AP. Zoals onder 12.1 al is aangestipt geldt deze regel niet alleen voor zwarte lijsten, maar ook voor strafrechtelijke gegevens die voor andere doeleinden worden gedeeld met derden. Te denken valt aan samenwerkingsverbanden met gemeenten, de politie en gebiedsteams.

Maakt een woningcorporatie dus al gebruik van een zwarte lijst die wordt gedeeld met andere woningorganisaties, wees er dan van bewust dat een voorafgaand onderzoek naar deze lijst verplicht is als deze nog niet heeft plaatsgevonden. Naar de letter van de wet houdt dit in dat eventuele lopende activiteiten onmiddellijk moeten worden gestaakt en pas mogen worden hervat zodra de AP het gebruik van de lijst heeft goedgekeurd. Op het moment van schrijven heeft de AP na voorafgaand onderzoek de volgende lijsten goedgekeurd in de woningverhuursector:[28]

- zwarte lijst woningcorporaties De Maaskoepel;
- Meldpunt Keurmerk Verhuurdersbelangen;
- zwarte lijst Nationaal Meldpunt Ongewenst Huurdersgedrag.

Volgens de AP hebben de woningcorporaties die betrokken zijn bij deze lijsten voldoende duidelijk gemaakt dat de waarschuwingslijsten een noodzakelijke maatregel is om ontruimingen te reduceren (Maaskoepel) of om de gevolgen van moeilijk plaatsbare huurders zoveel als mogelijk in te perken (Nationaal Meldpunt). Daarmee is de verwerking van bijzondere persoonsgegevens voor dit doel gerechtvaardigd.

12.2.2 Protocol grijze/zwarte lijsten

Grijze/zwarte lijsten moeten volgens de AP – ook als het gebruik van deze lijsten in overeenstemming is met de Wbp – altijd worden voorzien van een protocol.[29] Hierin wordt vastgelegd wat het doel is van de lijst, hoe de persoonsgegevens worden gebruikt voor de lijst en welke waarborgen er zijn vastgelegd voor de betrokkenen. Zo moet nader worden bepaald wanneer huurders worden geregistreerd op een zwarte of grijze lijst, wat de gevolgen zijn van plaatsing op deze lijst, welke gegevens daarbij worden geregistreerd en de duur van de registratie. Wanneer een registratie plaatsvindt dienen huurders hierover schriftelijk te worden geïnformeerd. De precieze eisen die de AP heeft gesteld aan deze protocollen zijn vastgelegd in de *Handleiding protocol zwarte lijst*.[30] Hierin is ook uitgewerkt hoe de procedure voor het melden van het protocol in zijn werk gaat. De AP heeft een checklist samengesteld met toetsingsvragen die moeten worden beantwoord om te kunnen voldoen aan de normen van de Wbp.[31]

28 Zie voor de actuele lijst van goedgekeurde zwarte lijsten en bijbehorende protocollen de website van de AP: https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/register-zwarte-lijsten/.
29 Autoriteit Persoonsgegevens, Handleiding protocol zwarte lijst, p.1. Online te raadplegen via: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/handleiding_protocol_zwarte_lijst.pdf.
30 Idem.
31 Autoriteit Persoonsgegevens, Checklist zwarte lijst. Online te raadplegen via: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/checklist_zwarte_lijst_0.pdf.

Een aspect dat niet duidelijk in de checklist van de AP naar voren komt is dat in het protocol ook duidelijk moet worden aangegeven welke personen binnen welke organisaties toegang hebben tot de grijze/zwarte lijst, zodat niet iedereen zomaar inzage heeft in de lijst. Dit hoeft niet noodzakelijkerwijs op niveau van naam, autorisatieprofielen kunnen ook op functieniveau worden weergegeven. Daarnaast verdient het aanbeveling om ook op de eigen website duidelijkheid te bieden over het gebruik van zwarte of grijze lijsten en wie de contactpersoon is als er vragen zijn over de lijsten. Bij een gedeelde zwarte lijst kan het voor de informatievoorziening naar de betrokkene handig zijn om daarnaast een aparte website in te richten.[32]

Voorbeeld: Klachten- en Kansenregister
Een voorbeeld van een juiste toepassing van grijze/zwarte lijsten is het Klachten- en Kansenregister, dat is opgezet door de stichting Nationaal Meldpunt Ongewenst Huurdersgedrag. Het register en bijbehorende protocol zijn na voorafgaand onderzoek goedgekeurd door de AP (zie: https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/register-zwarte-lijsten/zwarte-lijst-nmoh).

Het register stelt zich tot doel om een goede beoordeling te maken of, en zo ja onder welke voorwaarden, een huurovereenkomst zal worden aangegaan met de betrokkene. Zo kunnen moeilijk plaatsbare huurders een passende woning worden geboden en kunnen corporaties schade voor zichzelf en huurders voorkomen.

Bij het aangaan van de huurovereenkomst geven deelnemers van het register aan dat huurders kunnen worden opgenomen in het register als zij de overeenkomst overtreden en voldoen aan de opnamecriteria van het register. Bestaande huurders worden ook geïnformeerd. Wordt de huurder opgenomen in het register, dan wordt de huurder daarvan op de hoogte gesteld.

Alleen bepaalde functionarissen van de deelnemers van het register hebben toegang tot het register. In het register worden vastgelegd:
1. identificatiegegevens van de betrokkene (voorletters, geboortenaam, tussenvoegsel, achternaam en geboortedatum);
2. de naam van de woningcorporatie;
3. adresgegevens van betrokkene;
4. de W-categorie(ën) van betrokkene (type toerekenbare tekortkoming/reden plaatsing);
5. de (laatste) ingangsdatum van de betreffende termijn, zijnde de datum van ontruiming;
6. de datum en uitkomst van de (eventuele) begeleidingsprocedure.

De betrokkene (huurder) heeft het recht om een klacht in te dienen en zijn gegevens in te zien en/of te corrigeren. In afwijking van het normale inzageregime krijgt een betrokkene binnen zes weken een schriftelijke reactie van de woningcorporatie op zijn klacht of verzoek tot inzage en/of correctie. Op de website van het Klachten- en Kansenregister wordt uitleg gegeven aan betrokkenen.

12.3 GEZONDHEIDSGEGEVENS

Wanneer een woningcorporatie woningen verhuurt voor speciale doelgroepen, dan kan het nodig zijn om gegevens betreffende de gezondheid van huurders te verwerken. Denk bijvoorbeeld aan aangepaste woningen voor mensen met een lichamelijke beperking. In het huurdossier worden in dat geval gegevens opgenomen die betrekking hebben op de gezondheid, zoals CIZ-indicaties, en indicaties als 'rolstoeltoegankelijkheid' om zo de noodzaak voor een dergelijke woning te kunnen aantonen.

Gegevens die in dit kader ook bijzondere aandacht verdienen zijn gegevens over psychische aandoeningen en verslavingsproblematiek, maar ook over verwarde personen en meer in het algemeen zogenaamde 'bijzondere doelgroepen'. Het kan bijvoorbeeld zijn dat er een aantekening in het huurdossier wordt gemaakt dat een huurder door een bepaalde psychische aandoening anders moet worden benaderd of zelfs gevaarlijk kan zijn.

32 Zie bijvoorbeeld http://www.klachtenenkansenregister.nl/ik-ben-huurder/.

In bovengenoemde gevallen gaat het om een verwerking van gezondheidsgegevens. Hieronder vallen niet alleen medische gegevens, maar ook alle andere gegevens die betrekking hebben op de gezondheid van de betrokkene.

Gezondheidsgegevens vallen onder het bijzondere verwerkingsregime van de Wbp en mogen daarom in principe niet worden verwerkt. De Wbp biedt voor woningcorporaties zeer weinig uitzonderingsmogelijkheden op dit verwerkingsverbod, omdat de uitzonderingsbepalingen van artikel 21 alleen gelden voor partijen die daadwerkelijk zorg verlenen. Daardoor zijn in de praktijk alleen de algemene uitzonderingsbepalingen uit artikel 23 Wbp van belang, en met name toestemming en een zwaarwegend algemeen belang (sub f). Sectorspecifieke wetten kunnen dan een uitkomst bieden.

In de eerstgenoemde situatie (het verwerken van persoonsgegevens voor aangepaste woningen) is het op grond van bijvoorbeeld de WMO toegestaan om gezondheidsgegevens te verwerken om een aangepaste woning te kunnen leveren. Wel geldt daarbij steeds de plicht om alleen een beperkt aantal gegevens te verwerken die noodzakelijk zijn voor het toewijzen van de juiste woning. De exacte zorgbehandeling of aandoening zijn dus niet relevant en mogen niet worden verwerkt. Indien een bepaalde huurder bijvoorbeeld recht heeft op een aangepaste woning, dan hoeft enkel te worden vastgesteld dat de huurder daar recht op heeft. Niet hoeft te worden verwerkt dat de handicap het gevolg is van bijvoorbeeld een dwarslaesie.

In de tweede situatie worden er gezondheidsgegevens verwerkt om een andere reden, namelijk het belang van de woningcorporatie zelf. Het kan immers zijn dat een bepaalde huurder door zijn gezondheidssituatie een bedreiging vormt voor het personeel of overlast veroorzaakt voor de buurt. Voor deze gegevensverwerkingen geldt ook een verwerkingsverbod. Daarom moeten verwerkingen over de gezondheid zoveel mogelijk vermeden worden. Een aantekening in het huurdossier dat een bepaalde huurder lijdt aan psychoses is vanuit wettelijk oogpunt dus niet toegestaan. Het een en ander betekent overigens niet dat dergelijke verwerkingen wel zijn toegestaan als een beschrijving van de gezondheid wordt weggelaten. Aantekeningen over het feit dat een huurder gevaarlijk is, kan namelijk ook vormen aannemen van persoonsgegevens over onrechtmatig of hinderlijk gedrag (zie hierboven). Ook om deze reden moet zeer terughoudend omgegaan worden met dergelijke aantekeningen in huurdossiers. Een middenweg kan worden gevonden door bijvoorbeeld op te nemen dat een huurder onvoorspelbaar gedrag vertoont. Op deze manier worden er geen gezondheidsgegevens verwerkt en ook geen strafrechtelijke gegevens, terwijl de gegevens wel noodzakelijk kunnen zijn bij het bestrijden of voorkomen van overlast.

In het kader van hulpverlening en overlastbeperking bij bijzondere doelgroepen werken corporaties vaak samen met politie, gemeenten en GGZ. Hoe de rol van de woningcorporatie vorm gaat krijgen bij bijzondere doelgroepen is echter nog steeds onderwerp van discussie.[33]

12.4 KOPIE ID

De AP maakt onderscheid tussen het maken van een kopie van een paspoort (bewaren) en het tonen van een identificatiebewijs (verificatie). Het maken van een kopie van een identiteitsbewijs of paspoort is om twee redenen in de regel niet toegestaan. Ten eerste worden er met de kopieën pasfoto's verwerkt, welke in bepaalde gevallen zijn aan te merken als gegevens over iemands ras. Ten tweede worden ook burgerservicenummers (bsn) verwerkt, die vallen onder een streng beschermingsregime (artikel 24 Wbp). Het vragen van een identificatiebewijs is volgens de AP aan minder regels gebonden en daardoor in de regel wel toegestaan (zie hiervoor de Richtsnoeren 'kopietjes paspoort').

Richtsnoeren 'kopietje paspoort'
De Autoriteit Persoonsgegevens heeft in 2012 richtsnoeren over het gebruik van een 'kopietje paspoort' gepubliceerd (zie: https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/rs/rs_kopie-identiteitsbewijs.pdf).

33 Zie hiervoor ook de in februari 2016 aan de Tweede Kamer aangeboden tussenrapportage Samen doorpakken: op weg naar een meer persoonsgerichte aanpak voor en met mensen met verward gedrag; http://www.aedes.nl/binaries/downloads/bijzondere-doelgroepen/20160223-samen-doorpakkentussenrapportage.pdf.

Omdat bij veel woningcorporaties de vraag speelt of het maken van een kopie van het identiteitsbewijs of paspoort is toegestaan, zal vooral deze situatie nader worden besproken. De categorieën van persoonsgegevens die worden verwerkt (rasgegevens en bsn) worden hieronder apart besproken. De regels over deze persoonsgegevens gelden overigens ook in alle andere gevallen dat deze gegevens worden verwerkt zonder dat er een kopie van een identiteitsbewijs wordt gemaakt (bijvoorbeeld bij het opvragen van het bsn via de website voor woningzoekenden).

12.4.1 Pasfoto's

Pasfoto's werden in het verleden door de Autoriteit Persoonsgegevens gezien als rasgegevens en zijn daarmee bijzondere persoonsgegevens. De laatste jaren is de AP hier soepeler in geworden en ook in de AVG is bepaald dat het verwerken van pasfoto's niet per definitie een verwerking van bijzondere persoonsgegevens oplevert. Gelet hierop beschouwt de AP camerabeelden en pasfoto's van een persoon niet als bijzondere persoonsgegevens als:[34]

- het doeleinde van de verwerking niet gericht is op het verwerken van bijzondere persoonsgegevens dan wel op het onderscheid maken op grond van een bijzonder persoonsgegeven;
- het voor de verantwoordelijke redelijkerwijs niet voorzienbaar is dat de verwerking zal leiden tot het maken van onderscheid op grond van een bijzonder persoonsgegeven, en;
- de verwerking van die bijzondere persoonsgegevens onvermijdelijk is bij die verwerking.

Indien de verwerking van camerabeelden en pasfoto's echter identificatie tot doel heeft, dan worden deze beelden volgens de AP wel als een rasgegeven aangemerkt. Het doel waarvoor de pasfoto wordt opgeslagen zal daarom bepalen of sprake is van een bijzonder persoonsgegeven of niet.

Rasgegevens mogen op grond van artikel 18 Wbp, als uitzondering op het verwerkingsverbod, worden verwerkt als deze worden gebruikt voor identificatie en identificatie onvermijdelijk is voor het doel waarvoor de pasfoto wordt gebruikt. Een andere grondslag die van toepassing kan zijn is de uitdrukkelijke toestemming van de huurder. Pasfoto's mogen ook worden verwerkt als deze vrijelijk, uit eigen beweging openbaar zijn gemaakt door de betrokkene.

Ten slotte mogen rasgegevens ook worden verwerkt om een bevoorrechte positie toe te kennen aan minderheidsgroeperingen. Zo kunnen sommige woningen exclusief zijn voorbehouden aan mensen van een bepaalde afkomst. Voor de registratie en toetsing van dit voorkeursbeleid mogen rasgegevens (aan de hand van een pasfoto) worden verwerkt.

12.4.2 Burgerservicenummers

Burgerservicenummers zijn geen bijzondere persoonsgegevens in de zin van artikel 16 Wbp, maar het gaat hier wel om zeer privacygevoelige gegevens die bij misbruik kunnen leiden tot identiteitsfraude. De Wbp bepaalt daarom in artikel 24 dat het bsn en andere wettelijke persoonsnummers (zoals kentekengegevens) niet mogen worden verwerkt, tenzij een wet de verplichting bevat om het nummer te verwerken.[35] Is er sprake van een wettelijke plicht, dan mag het bsn alleen worden gebruikt voor het in die wet omschreven doel. Deze regel houdt in dat als er geen wettelijke basis is, het bsn niet mag worden verwerkt. Zelfs toestemming van de betrokkene geeft geen rechtvaardiging om het bsn te verwerken.

Wettelijke plicht

Wat betekent dit nu voor woningcorporaties? De woningcorporatie heeft als werkgever in ieder geval een verificatie- en bewaarplicht bij nieuwe werknemers. Dit betekent dat de identiteit moet worden gecontroleerd aan de hand van een geldig ID-bewijs en een kopie van dit ID-bewijs (inclusief bsn!) moet worden opgeslagen in de loonadministratie. Dit is wettelijk vastgelegd in artikel 28 lid 1 sub f Wet op de Loonbelasting.

Met betrekking tot huurders is de situatie de afgelopen jaren veranderd. Tot enkele jaren geleden konden woningcorporaties het bsn van de huurder verwerken, omdat de huurtoeslag van hun huurders aan hen kon worden uitgekeerd door de Belastingdienst op basis van dit bsn. Sinds begin 2014 is dit veranderd. De huurtoeslag loopt sindsdien namelijk niet meer via de woningcorporaties, maar wordt rechtstreeks overgemaakt aan de huurder. Woningcorporaties hebben dus niet langer de plicht om het bsn te verzamelen voor de uitkering van de huurtoeslag.

34 Beleidsregels cameratoezicht, Autoriteit Persoonsgegevens van 2 februari 2016, Stcrt. 2016, 4971, p. 25-27. Online te raadplegen via: https://autoriteitpersoonsgegevens.nl/nl/nieuws/autoriteit-persoonsgegevens-publiceert-beleidsregels-cameratoezicht.
35 De tekst hierna zal zich alleen toespitsen op het gebruik van burgerservicenummers.

Woningcorporaties hebben wel een andere wettelijke plicht om het bsn te verwerken. De Belastingdienst kan namelijk van tijd tot tijd huurdersgegevens, zoals de huurprijs, opvragen bij woningcorporaties. Zo kan worden gecontroleerd of een huurder recht heeft op huurtoeslag. De plicht voor woningcorporaties om op verzoek van de Belastingdienst huurdersgegevens te verstrekken is vastgelegd in artikel 38 Algemene wet inkomensafhankelijke regelingen (hierna: Awir) in verbinding met artikel 1a lid 1 sub a Uitvoeringsbesluit Awir. Op grond van artikel 1b lid 1 Uitvoeringsbesluit Awir zijn woningcorporaties verplicht om deze huurdersgegevens te verstrekken onder vermelding van het burgerservicenummer. Artikel 1b lid 2 Uitvoeringsbesluit Awir bevat een plicht voor burgers om hun bsn te verstrekken aan de woningverhuurder.

Gelet op deze wettelijke plicht mogen woningcorporaties burgerserviceummers dus **alleen** verwerken voor het verstrekken van huurdersgegevens aan de Belastingdienst ter controle van huurtoeslag.

Verder wordt het bsn in de praktijk ook gebruikt om de echtheid van een inkomensverklaring (vroeger: IB60-verklaring) te controleren. Let er wel op dat het *opslaan* van het burgerservicenummer (bijvoorbeeld door een kopie op te slaan van het paspoort) voor deze en andere identiteitscontroles *niet* is toegestaan. Er is namelijk geen wettelijke plicht om het bsn te verwerken voor dit doel. Bovendien kan in de praktijk ook worden volstaan met verificatie in plaats van het opslaan het bsn. Een medewerker kan dan in het dossier aangeven dat er een controle heeft plaatsgevonden.

Het bsn van de huurder wordt ook gevraagd als er een geschil wordt voorgelegd bij de Huurcommissie. Navraag leert dat er geen verplichting bestaat om het bsn aan te leveren, omdat de Huurcommissie zelf de gegevens kan controleren via de Basisregistratie Personen. Ook voor dit doel bestaat er dus geen plicht om het bsn op te slaan.

Mogelijk bestaan er nog andere (toekomstige) wettelijke plichten op grond waarvan woningcorporaties burgerservicenummers moeten verwerken.

Do's en don'ts
Op grond van het bovenstaande is het belangrijk om de volgende do's en don'ts in acht te nemen bij het opslaan van het bsn:

Do's:
- Vraag pas om verstrekking van het bsn zodra er een huurovereenkomst wordt gesloten.
- Informeer de huurder over het doel van het gebruik van het bsn en zijn rechten.
- Sla het bsn apart op, zodat het alleen kan worden geraadpleegd als het bsn nodig is voor de uitvoering van een wettelijke plicht (bijvoorbeeld bij communicatie met de Belastingdienst).
- Zorg voor goede beveiliging van de burgerservicenummers, zowel in technische als in organisatorische zin.
- Vernietig het bsn zodra het bsn niet meer nodig is voor het doel waarvoor het is verzameld.

Don'ts:
- Vraag het bsn niet al op in een vroeg stadium, zoals bij de inschrijving als woningzoekende.
- Gebruik het bsn niet als 'klantnummer' of unieke identifier om huurders mee te identificeren in het huurdersbestand.

Bovenstaande uitgangspunten gelden ook voor fysieke kopieën die in het verleden van identiteitsbewijzen zijn gemaakt en zijn opgeslagen in het archief. Het verdient aanbeveling om te achterhalen welk van deze kopieën nog noodzakelijk zijn voor bovengenoemde wettelijke taken en welke kunnen worden vernietigd.

12.5 FINANCIËLE GEGEVENS

Het is evident dat woningcorporaties financiële gegevens verwerken voor de uitvoering van hun taken. Financiële gegevens vallen niet onder het bijzondere regime van artikel 16 Wbp, maar worden wel als gevoelig beschouwd. Er moet met andere woorden meer zorgvuldigheid betracht worden dan bij verwerking van – in de context – minder gevoelige gegevens zoals persoonsnaam of woonadres. Denk bij financiële gegevens niet alleen aan zaken

als bankrekeningnummer, maar ook aan het recht op toeslag en de hoogte daarvan, de inhoud van loonstroken of studiefinancierings- en inkomensverklaringen.

Door de verhoogde privacygevoeligheid is het in ieder geval van belang dat er passende technische en organisatorische maatregelen zijn getroffen om de financiële gegevens te beschermen. Zeker als huurders in staat zijn zelf gegevens te wijzigen of aan te vullen via een huurdersportaal wordt dit belang groter.

Ook hiervoor geldt, dat u zich moet afvragen of verwerking van dergelijke informatie wel noodzakelijk is en op welk moment het noodzakelijk is om deze gegevens op te vragen.

12.6 GEGEVENS OVER KINDEREN

Wanneer gegevens over medebewoners worden verwerkt, worden nog wel eens alle medebewoners geregistreerd en daar kunnen ook persoonsgegevens van kinderen (minderjarigen jonger dan 16 jaar) tussen zitten. Juist de kwetsbaarheid van kinderen maakt dat het gaat om gevoelige gegevens. Het is daarom – behoudens noodzaak – aan te raden zo min mogelijk gegevens van kinderen te verwerken. Is verwerking wel noodzakelijk, dan moet deze verwerking met extra waarborgen worden omkleed, bijvoorbeeld door extra beveiligingsmaatregelen of kortere bewaartermijnen. Artikel 5 Wbp vereist bij persoonsgegevens van minderjarigen tot 16 jaar toestemming van de ouder of de wettelijk vertegenwoordiger. Houd er rekening mee dat deze toestemming ook kan worden ingetrokken.

Een alternatief voor verwerking van de persoonsgegevens van kinderen is om bijvoorbeeld alleen aantallen medebewoners onder de 16 jaar van een woning te registreren. Dit voorkomt ook dat een proces moeten worden ingericht om toestemming en intrekking daarvan door ouders/wettelijk vertegenwoordigers te administreren.

13. MELDPLICHT DATALEKKEN

Op 1 januari 2016 is de meldplicht datalekken in werking getreden. Woningcorporaties die een datalek ondervinden die voldoet aan de criteria van artikel 34a lid 1 Wbp, moeten bij de AP een melding maken van dit datalek. Onder omstandigheden moeten ook de betrokkenen wiens persoonsgegevens zijn gelekt, worden geïnformeerd over dit lek.

Men spreekt van een datalek indien er een inbreuk is op de beveiliging van persoonsgegevens (zoals bedoeld in artikel 13 Wbp). Bij een datalek zijn de persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking – dus aan datgene waartegen de beveiligingsmaatregelen bescherming moeten bieden. Als voorbeelden van datalekken worden genoemd: een zoekgeraakte USB-stick met persoonsgegevens, een gestolen of kwijtgeraakte laptop of een inbraak in een database door een hacker.

Beleidsregels meldplicht datalekken

De Autoriteit Persoonsgegevens heeft in 2015 een uitgebreid document gepubliceerd over de juridische gevolgen van de meldplicht datalekken. (Online te raadplegen via: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/beleidsregels_meldplicht_datalekken.pdf.) De inhoud van deze beleidsregels zijn meegenomen in deze paragraaf. Er wordt in de tekst dan gesproken van 'de beleidsregels'.

13.1 OP WIE RUST DE VERPLICHTING OM DATALEKKEN TE MELDEN?

Op basis van artikel 34a, lid 1, Wbp rust de plicht om datalekken te melden op de verantwoordelijke. In het geval dat de verantwoordelijke gebruikmaakt van een bewerker is het nog steeds de verantwoordelijke op wie de plicht rust om het datalek te melden. Wanneer bewerkers in opdracht van de woningcorporatie persoonsgegevens verwerken, dan is het nodig om hierover afspraken te maken in een bewerkersovereenkomst (paragraaf 7.2) en/of operationele werkafspraken. U wilt als woningcorporatie immers snel en goed geïnformeerd worden als er een datalek heeft plaatsgevonden bij een bewerker.

In een bewerkersovereenkomst moeten afspraken gemaakt worden over, onder meer, de beveiliging, maar ook over het melden van datalekken (artikel 14 lid 5 Wbp). Daarnaast moet de verantwoordelijke ervoor zorgen dat de bewerker maatregelen treft om aan de meldplicht datalekken te kunnen voldoen en toezien op de naleving hiervan (artikel 14 lid 1 en lid 3 sub c Wbp). Concreet houdt dit in dat een verantwoordelijke zijn bewerkers moet instrueren *welke informatie* over een datalek hij op *welke wijze* en binnen *welke termijn* wil ontvangen. Ook moeten er afspraken gemaakt worden over het op de hoogte houden van nadere ontwikkelingen rond het datalek en maatregelen die de bewerker treft om de negatieve gevolgen te beperken en herhaling te voorkomen. Tot slot zou een boetebeding kunnen worden opgenomen. Deze boete zou verbeurd kunnen worden wanneer bewerker deze informatieplicht jegens verantwoordelijke schendt. Een voorbeeldclausule voor datalekken is opgenomen in bijlage 2.

Los van de eventuele waarde van contracten en aansprakelijkheidsbepalingen, is het vooral van belang om tot goede procedures en werkafspraken te komen; voorkomen is immers beter dan genezen. Voor de gehele cyclus van de meldplicht datalakken zal in kaart moeten worden gebracht wie er verantwoordelijk is voor welk onderdeel en proces. Vanaf het moment dat het bericht van het datalek de organisatie binnenkomt, tot aan het onderzoek, de afwikkeling, melding en registratie van het datalek dienen er verantwoordelijkheden worden bepaald binnen de organisatie:

- Wie is verantwoordelijk voor de 'intake' van een datalek en het eventueel doorverwijzen naar een volgende behandelaar?
- Wie is verantwoordelijk voor het onderzoek naar de bron van het datalek (*'root cause'*)?
- Wie is verantwoordelijk voor het opstellen van de teksten aan de individuele betrokkene, en eventueel bij grootschalige datalekken de tekst op een webpagina?
- Wie is verantwoordelijk voor het doen van de melding aan de AP en aan betrokkene?
- Wie is verantwoordelijk voor het oplossen en voorkomen van het (toekomstige) datalek?
- Met wie kan contact worden opgenomen voor het verstrekken van meer informatie? Is er een functionaris voor de gegevensbescherming aangesteld?
- Wie is verantwoordelijk voor het opstellen van het protocol datalekken?
- Wie is verantwoordelijk voor de interne en externe communicatie over het datalek?

Veel woningcorporaties kennen al een vorm van incidentenmanagement. Dit kan een e-mailadres zijn waar men onregelmatigheden kan melden, of een geavanceerd systeem waarmee beveiligingsincidenten worden gemeld. De meldplicht datalekken zou in dit systeem kunnen worden geïmplementeerd.

13.2 WAT ZIJN DATALEKKEN?

Een datalek is een 'inbreuk op de beveiliging, bedoeld in artikel 13, die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens' (artikel 34a Wbp). In artikel 13 Wbp is bepaald dat de verantwoordelijke passende technische en organisatorische maatregelen moet nemen om persoonsgegevens te beveiligen tegen verlies of onrechtmatige verwerking.

Er is alleen sprake van een datalek als zich daadwerkelijk een *beveiligingsincident* heeft voorgedaan. Wanneer er enkel sprake is van een dreiging, is een melding niet verplicht.[36] Bij de term beveiligingsincident moet gedacht worden aan een het verlies van een USB-stick, de diefstal van een laptop of inbraak door een hacker. De Autoriteit Persoonsgegevens maakt onderscheid tussen de volgende termen die ook in het figuur terugkomen:

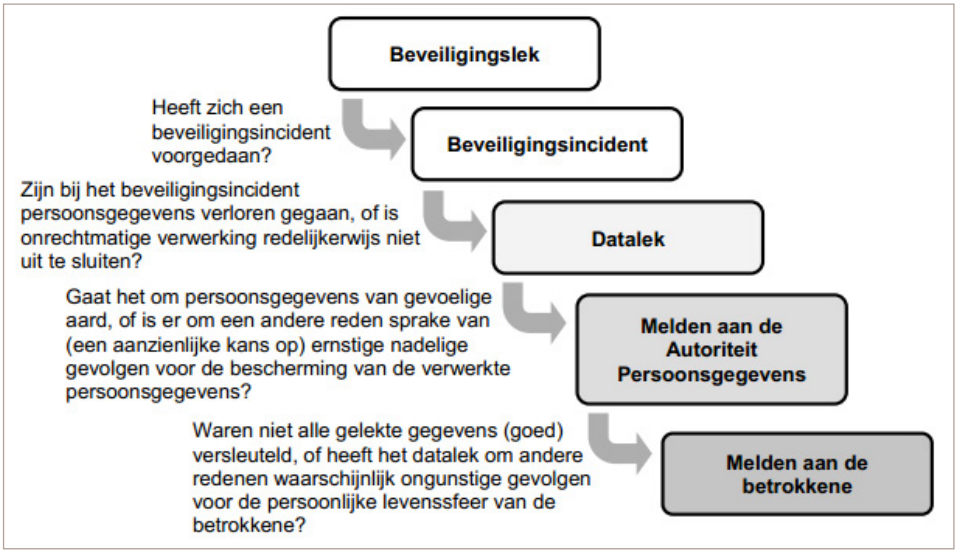
- **Beveiligingslek**
  Wanneer uitsluitend sprake is van een tekortkoming in de beveiliging die zou kunnen leiden tot een beveiligingsincident, wordt dit een beveiligingslek genoemd. Wanneer de mogelijke dreiging die van dit beveiligingslek uitgaat, zich ook daadwerkelijk verwezenlijkt, spreken we van een beveiligings*incident*.

- **Beveiligingsincident**
  Incident waarbij de getroffen preventieve maatregelen niet toereikend zijn gebleken. Als voorbeelden worden genoemd een kwijtgeraakte USB-stick, een gestolen laptop, een inbraak door een hacker, malware-besmetting en brand in een datacentrum.

36 Autoriteit Persoonsgegevens, *Beleidsregels meldplicht datalekken Wbp*, 8/12/2015, p. 20.

- **Datalek**
  Er is sprake van een datalek als er bij het beveiligingsincident persoonsgegevens verloren zijn gegaan, of wanneer verantwoordelijke onrechtmatige verwerking van de persoonsgegevens niet redelijkerwijs kan uitsluiten.

In de beleidsregels is het volgende figuur opgenomen ter verduidelijking van het begrip datalek:



Het gaat dus om incidenten waarbij specifieke beveiligingsmaatregelen die getroffen zijn tegen verlies of onrechtmatige verwerking, daadwerkelijk ontoereikend zijn gebleken en persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking. Een beveiligingsincident waarbij geen verlies van gegevens of geen onrechtmatige verwerking is opgetreden, levert geen datalek op volgens deze wet. De beleidsregels zeggen hierover het volgende:

'Een inbreuk op de beveiliging houdt in dat zich daadwerkelijk een beveiligingsincident heeft voorgedaan. Er is niet uitsluitend sprake van een dreiging, of van een tekortkoming in de beveiliging (ook wel aangeduid als een beveiligingslek) die zou kunnen leiden tot een beveiligingsincident. Er heeft zich daadwerkelijk een beveiligingsincident voorgedaan, en de preventieve maatregelen die u eventueel heeft getroffen waren niet toereikend om dit te voorkomen. Kenmerkend voor een inbreuk op de beveiliging is verder dat het beveiligingsincident daadwerkelijk gevolgen heeft voor de persoonsgegevens die u verwerkt. Er zijn persoonsgegevens verloren gegaan, of u kunt niet redelijkerwijs uitsluiten dat er persoonsgegevens onrechtmatig zijn verwerkt. De repressieve maatregelen en de herstelmaatregelen die u eventueel heeft getroffen waren niet voldoende om deze gevolgen geheel weg te nemen.'[37]

13.3 WANNEER MOET EEN DATALEK GEMELD WORDEN?

Er zijn twee soorten meldplichten: één aan de AP en één aan de betrokkene wiens persoonsgegevens zijn gelekt. Beide meldplichten hebben ogenschijnlijk verschillende 'privacydrempels'.

1. Voor de melding aan de *AP* is vereist dat het datalek (een 'aanzienlijke kans op) *ernstige nadelige gevolgen* voor de bescherming van persoonsgegevens' heeft (artikel 34a lid 1 Wbp).
2. Voor de melding aan de *betrokkene* is vereist dat het datalek *'waarschijnlijk ongunstige gevolgen* voor diens persoonlijke levenssfeer' heeft (artikel 34a lid 2 Wbp).

De kennisgeving aan betrokkenen is alleen nodig wanneer het datalek ook aan de AP gemeld dient te worden. Met andere woorden: de situatie waarin slechts aan betrokkene gemeld dient te worden en niet aan de AP, komt niet voor.

37 Autoriteit Persoonsgegevens, *Beleidsregels meldplicht datalekken Wbp*, 8/12/2015, p.21.

Van ernstige nadelige gevolgen voor de bescherming van persoonsgegevens (en dus een verplichting tot het doen van een melding bij de AP) is in ieder geval sprake indien gegevens van gevoelige aard zijn betrokken bij het datalek. Hierbij moet gedacht worden aan:

- bijzondere persoonsgegevens zoals bedoeld in artikel 16 Wbp. Bijvoorbeeld gegevens over godsdienst, ras, politieke gezindheid, seksuele leven, lidmaatschap vakbond, strafrechtelijke gegevens et cetera;
- gegevens over de financiële of economische situatie van de betrokken. Bijvoorbeeld schulden, salaris- en betalingsgegevens;
- (andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene. Bijv. verslavingen, schoolprestaties, relatieproblemen;
- gebruikersnamen, wachtwoorden en andere inloggegevens;
- gegevens die kunnen worden misbruikt voor (identiteits)fraude. Bijvoorbeeld biometrische gegevens, kopieën paspoort, bsn.

Indien informatie van bovenstaande aard is betrokken bij het datalek, kan ervan uitgegaan worden dat er sprake is van *waarschijnlijk ongunstige gevolgen* voor de persoonlijke levenssfeer van betrokkene. Het datalek moet in bovenstaande gevallen dus ook worden gemeld aan de betrokkene.

Indien geen gevoelige gegevens zijn gelekt, dan kan het toch zijn dat u moet melden aan de AP. De memorie van toelichting geeft aan dat de aard en omvang van de getroffen verwerking mede bepalend zijn voor de beantwoording van de vraag of er bij een datalek sprake is van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens.[38] Het criterium ernstige nadelige gevolgen valt uiteen in vier (niet-cumulatieve) deelcriteria:

1. **Omvang van de verwerking**
   De omvang van de hierboven beschreven verwerkingen betekent dat het bij datalekken kan gaan om veel persoonsgegevens per persoon, en om gegevens van grote groepen betrokkenen. Deze beide factoren maken een gelekte dataset aantrekkelijk voor misbruik in het criminele circuit. De kans dat de gelekte dataset wordt doorverkocht wordt daardoor ook groter, met als gevolg dat de betrokkenen langer last houden van het datalek. Dat betekent overigens niet dat een datalek met gegevens van één persoon niet meldenswaardig is.

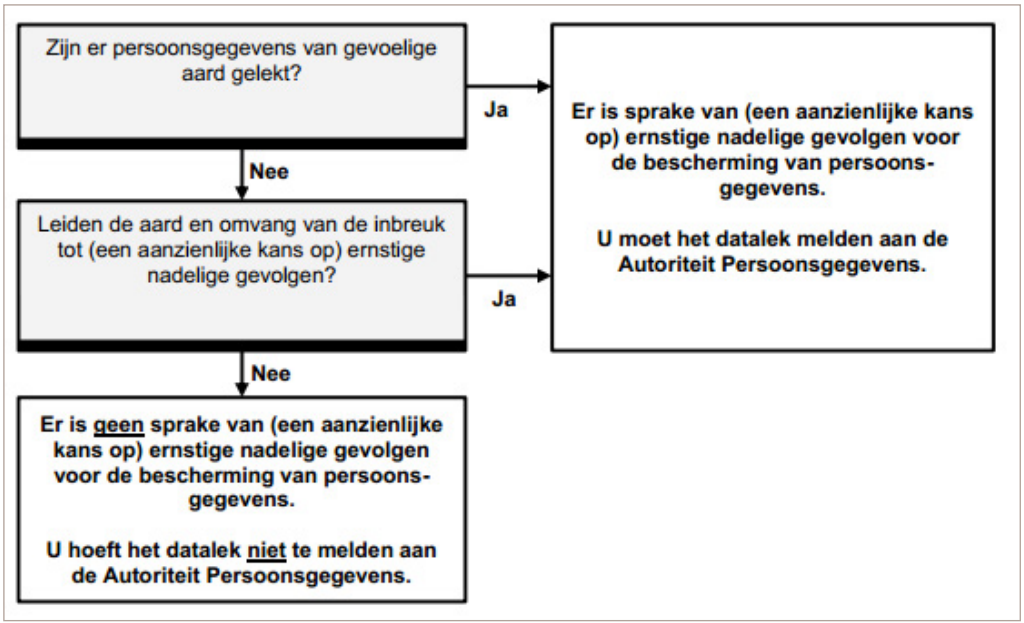
2. **Aard van de verwerking**
   Naarmate de beslissingen die op basis van de verwerkte persoonsgegevens worden genomen ingrijpender zijn, is ook de impact van verlies of onrechtmatige verwerking groter. Bijvoorbeeld: als een organisatie financiële gegevens gebruikt om iemands kredietwaardigheid te bepalen zijn de gevolgen van verlies en onbevoegde wijziging van de gegevens ingrijpender dan bij gebruik van dezelfde gegevens voor marketingdoeleinden.

3. **Onderdeel van ketens**
   Bij omvangrijke verwerkingen is vaak sprake van persoonsgegevens die binnen ketens worden gedeeld. Dit betekent dat de gevolgen van verlies en onbevoegde wijziging van persoonsgegevens door de hele keten heen kunnen optreden. Voor de betrokkenen wordt het hierdoor moeilijker om de mogelijke gevolgen van een datalek te overzien en om zich daar waar mogelijk aan te onttrekken.

4. **Kwetsbare groepen**
   Worden er persoonsgegevens verwerkt van mensen in kwetsbare groepen, bijvoorbeeld omdat de verwerking zich specifiek richt op betrokkenen die hiertoe behoren, dan moet u ervan uitgaan dat bij een datalek (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens aanwezig kan zijn. Bij kwetsbare groepen moet gedacht worden aan de inwoners van een blijf-van-mijn-lijfhuis, kinderen en mensen met een verstandelijke handicap.

38 *Kamerstukken II* 2012/13, 33 662, nr. 3, blz. 7.

Schematisch ziet het er als volgt uit:



13.4 NIET MELDEN

Als voorbeelden van gebeurtenissen die niet hoeven te worden gemeld, worden in de beleidsregels genoemd:

- De verkeerd geadresseerde brief die ongeopend retour komt.
- Een koffer met daarin persoonsgegevens wordt verloren in de trein. De koffer zit op slot en wordt zonder sporen van braak bij gevonden voorwerpen aangetroffen en teruggebracht naar de rechtmatige eigenaar.
- Het gebruikmaken van het wachtwoord van andere medewerkers om toegang te verkrijgen tot persoonsgegevens zal een schending van interne voorschriften opleveren maar niet zozeer een datalek.

Het melden aan de *betrokkene* mag uitblijven wanneer de 'verantwoordelijke passende technische beschermingsmaatregelen heeft genomen waardoor de persoonsgegevens die het betreft onbegrijpelijk of ontoegankelijk zijn voor eenieder die geen recht heeft op kennisname van de gegevens'. Voorbeelden hiervan zijn de encrypted of gepseudonimiseerde opslag van gegevens of op afstand wissen van persoonsgegevens door middel van *remote wiping*.

De redenering 'geanonimiseerde gegevens zijn geen persoonsgegevens', gaat niet altijd op. Volgens de AP kan het zo zijn dat gegevens die geanonimiseerd zijn, toch persoonsgegevens zijn. Door middel van spontane herkenning, vergelijking van gegevens en/of koppeling aan gegevens uit een andere bron, zou toch identificatie tot stand gebracht kunnen worden.[39] Wanneer hier sprake van zou kunnen zijn, moet het datalek aan de *AP* worden gemeld.

13.5 TERMIJN EN WIJZE VAN MELDEN

Datalekken moeten 'onverwijld' worden gemeld aan de AP en aan de betrokkene (artikel 34a lid 1 en 2 Wbp). Zodra het datalek is ontdekt, is er maar korte tijd om onderzoek te doen naar de oorzaak van het datalek. De termijn voor het doen van de melding is uiterlijk 72 uur na het ontdekken ervan.[40] De termijn voor het melden van het datalek begint te lopen op het moment dat de verantwoordelijke, of ingeschakelde bewerker, op de hoogte raakt van een beveiligingsincident dat mogelijk onder de meldplicht datalekken valt. De melding kan worden gedaan met behulp van het meldportaal van de AP of, in uitzonderlijke gevallen, door middel van een faxbericht.[41]

39 Autoriteit Persoonsgegevens, *Beleidsregels meldplicht datalekken Wbp*, 8/12/2015, p.31.
40 Autoriteit Persoonsgegevens, *Beleidsregels meldplicht datalekken Wbp*, 8/12/2015, p.31.
41 Het meldportaal kunt u raadplegen op de website van de Autoriteit Persoonsgegevens: https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0.

Wanneer een bedrijf niet alle in het meldformulier gevraagde informatie voorhanden heeft binnen 72 uur na ontdekking, moet toch gemeld worden. Door middel van vervolgmeldingen zal de ontbrekende informatie alsnog moeten worden verstrekt aan de AP.[42]

13.6 INHOUD MELDING

De wet verplicht om uitgebreide informatie te verstrekken over (artikel 34a lid 3 Wbp):

1. het soort datalek;
2. de instanties waar meer informatie kan worden gekregen over het datalek;
3. de aanbevolen maatregelen om de schade voor de privacy van de betrokkene te beperken.

Daarnaast zijn er aparte informatieverplichtingen ten aanzien van de AP en de betrokkene:

- **Aan de AP (artikel 34a lid 4 Wbp)**
  Een beschrijving van 1) de vastgestelde en de te verwachten gevolgen voor de privacy van de betrokkene en 2) de maatregelen die de organisatie heeft genomen of zal nemen om de schade te verhelpen.

- **Aan de betrokkene (artikel 34a lid 5 Wbp)**
  De betrokkene moet op zodanige wijze worden geïnformeerd dat 'een behoorlijke en zorgvuldige informatievoorziening is gewaarborgd'. Dit betekent dat de betrokkene zo veel mogelijk individueel geïnformeerd moet worden en als dat niet mogelijk is – bijvoorbeeld bij grootschalige datalekken – zal er gebruikgemaakt moeten worden van speciaal ingerichte websites of persberichten in de media.

13.7 DOCUMENTATIEPLICHT

Datalekken die leiden tot een aanzienlijke kans op ernstige nadelige gevolgen voor de persoonlijke levenssfeer van de betrokkene (dat wil zeggen: alle incidenten die gemeld zijn of gemeld hadden moeten worden) moeten gedocumenteerd worden in een register (artikel 34a lid 8 Wbp). Deze bescheiden moeten minimaal een jaar worden bewaard en drie jaar wanneer wordt besloten om de betrokkene niet te informeren omdat de technische beschermingsmaatregelen die zijn genomen voldoende bescherming bieden om de melding aan de betrokkene achterwege te kunnen laten (artikel 34a lid 6 Wbp) of wanneer dit niet gebeurt om zwaarwegende redenen.[43]

42 Het meldportaal van de AP biedt de mogelijkheid om bestaande meldingen te wijzigen.
43 Autoriteit Persoonsgegevens, Beleidsregels meldplicht datalekken Wbp, 8/12/2015, p.46.

14. SANCTIES

Met ingang van 1 januari 2016 is niet alleen de meldplicht datalekken ingevoerd, ook zijn de sanctiemogelijkheden van de Autoriteit Persoonsgegevens aanzienlijk uitgebreid. Daarbij kan de AP niet alleen boetes opleggen voor het schenden van de meldplicht datalekken, maar ook voor vrijwel alle andere overtredingen van de Wbp. De boetes kunnen hierbij oplopen tot 820.000 euro of 10 procent van de jaaromzet (artikel 66 Wbp).

Overtreding van regel	Maximale boete*
Wijze van kennisgeving datalek aan AP en betrokkene (artikel 34a lid 3, lid 4, lid 5 en lid 11)	€ 200.000,-
Inzageverzoek: zienswijze derde, mededeling over logica, vergoeding (artikel 35 lid 3, lid 4 en artikel 39 Wbp)	€ 200.000,-
Correctieverzoek bij onwijzigbare gegevensdrager, kennisgeving derden, informeren verzoeker (artikel 36 lid 4 en artikel 38 Wbp)	€ 200.000,-
Verzet: vergoeding en bekendmaking van het recht aan betrokkene (artikel 40 lid 3 en artikel 41 lid 3 Wbp)	€ 200.000,-
Uitvoeren persoonsgegevens buiten de EU: vergunning, opschorting (artikel 77 lid 2 en artikel 78 lid 4 Wbp)	€ 200.000,-
Profiling: ontbreken van mededeling logica geautomatiseerde verwerking (artikel 42 lid 4 Wbp)	€ 200.000,-
Verwerking in opdracht van verantwoordelijke, geheimhouding (artikel 12 Wbp) (boete afhankelijk van hoedanigheid overtreder)	€ 200.000,- of € 500.000,-
Verwijderen persoonsgegevens na verstrijken uiterste bewaartermijn (artikel 10 lid 1 Wbp)	€ 500.000,-
Plicht tot juiste, correcte en niet overmatige verwerking (artikel 11 Wbp)	€ 500.000,-
Verbod van uitvoeren persoonsgegevens buiten de EU (artikel 76 lid 1 Wbp)	€ 500.000,-
Informatieplicht aan betrokkene (artikel 33 en artikel 34 lid 1, lid 2 en lid 3 Wbp)	€ 500.000,-
Recht op inzage in eigen persoonsgegevens (artikel 35 lid 1, tweede volzin en lid 2 Wbp)	€ 500.000,-
Betrokkene mag verzet aantekenen tegen verwerking van persoonsgegevens (artikel 40 lid 2 en artikel 41 lid 2Wbp)	€ 500.000,-
Recht op correctie (artikel 36 lid 2 en lid 3 Wbp)	€ 500.000,-
Doelbinding (artikel 7 en 9 lid 1 Wbp)	€ 500.000,-
Adequate beveiliging (artikel 13 Wbp)	€ 500.000,-
Geen verwerking zonder grondslag in de wet (artikel 8 Wbp)	€ 500.000,-
Geen verwerking bij geheimhoudingsplicht (artikel 9 lid 4 Wbp)	€ 500.000,-
Melding datalek bij AP en betrokkene, bijhouden overzicht inbreuken op de beveiliging (artikel 34a lid 1, lid 2, lid 7, lid 8 Wbp)	€ 500.000,-
Zorgvuldige en behoorlijke verwerking (artikel 6 Wbp)	€ 820.000,-
Regels over verwerking wettelijk identificatienummer (artikel 24 Wbp)	€ 820.000,-
Profiling: onderwerping aan geautomatiseerd besluit (artikel 42 lid 1Wbp)	€ 820.000,-
Verbod van verwerking van bijzondere persoonsgegevens zoals godsdienst of levensovertuiging; ras; politieke gezindheid; gezondheid; seksuele leven; lidmaatschap van een vakvereniging en strafrechtelijk gedrag (artikel 16 Wbp)	€ 820.000,-
Niet-nakoming bindende aanwijzing (artikel 66 lid 5 Wbp)	€ 820.000,-
Medewerkingsplicht met de toezichthouder (artikel 5:20 Awb)	€ 820.000,-

* behoudens boeteverhogende omstandigheden

14.1 BINDENDE AANWIJZING

De AP kan niet elke overtreding direct bestraffen. Artikel 66 lid 3 bepaalt dat boetes pas kunnen worden opgelegd nadat de AP een bindende aanwijzing heeft gegeven. Een bindende aanwijzing is een beslissing van de AP met de plicht voor de geadresseerde om bepaalde handelingen te verrichten. Wordt binnen de opgegeven termijn alsnog voldaan aan de bindende aanwijzing van de AP, dan kan een boete worden ontlopen. Een boete kan wel direct, zonder bindende aanwijzing worden opgelegd als de overtreding opzettelijk is begaan of er sprake is van 'ernstige

verwijtbare nalatigheid'. Wat ernstige verwijtbare nalatigheid precies inhoudt in de praktijk, is op het moment van schrijven nog onduidelijk.

14.2 HOOGTE BOETES

De Autoriteit Persoonsgegevens heeft in de boetebeleidsregels nader bepaald hoe wetsovertredingen worden bestraft.[44] Dit heeft de Autoriteit gedaan door een opdeling te maken in verschillende categorieën (I tot en met III, opgedeeld van minst zware naar zwaarste overtredingen) waaraan bepaalde boetebandbreedtes zijn gekoppeld. Overtreding van artikel 24 lid 1 (gebruik bsn), welke volgens de beleidsregels valt onder categorie III, levert bijvoorbeeld een boete op van tussen de 350.000 en 820.000 euro.

Bij het bepalen van de hoogte van de boete binnen de boetebandbreedtes wordt rekening gehouden met:

- de aard en omvang van de overtreding;
- de duur van de overtreding;
- de impact van de overtreding op (de bescherming van persoonsgegevens en van de persoonlijke levenssfeer voor) de betrokkenen en/of de maatschappij;
- de mate waarin de overtreding aan de overtreder kan worden verweten.
- de omstandigheden waaronder de overtreding is gepleegd en de (financiële) omstandigheden van de overtreder.

De AP kan buiten de boetebandbreedtes treden als de boete niet voldoende preventieve werking heeft (boete verhoogd) of onevenredig hoog is (boete verlaagd). De AP past dan de boetecategorie van de naast hogere of naast lagere categorie toe. Een overtreding uit categorie III kan dus niet worden bestraft met 100.000 euro, omdat deze valt onder categorie I. Een boete van 150.000 euro is daarentegen wel toegestaan, omdat deze valt onder categorie II. Als de AP een boete van 820.000 euro niet passend acht, mag de AP een geldboete opleggen tot maximaal 10 procent van de jaaromzet van het voorgaande boekjaar. Bij meerdere, samenhangende overtredingen kan een boete voor alle overtredingen afzonderlijk of gezamenlijk worden opgelegd en kunnen de boetes worden gematigd.

Nadat rekening is gehouden met bovengenoemde omstandigheden, kijkt de AP naar de boeteverhogende en -verlagende omstandigheden:

Boeteverhogende omstandigheden	Boeteverlagende omstandigheden
■ Eerdere (zelfde of vergelijkbare) overtredingen of recidive[45] ■ Tegenwerking of belemmeringen van het onderzoek van de AP	■ Meer medewerking verlenen aan de AP dan wettelijk verplicht ■ Overtreding uit eigen beweging beëindigd, voor het onderzoek van de AP ■ Schadeloosstelling van de slachtoffer(s)

14.3 SANCTIES IN DE AVG

De AP beschikt ook op grond van de AVG over boetebevoegdheden (art. 79 AVG). De bedragen liggen flink hoger dan in de Wbp. Afhankelijk van de overtreding kunnen de boetes oplopen tot 20 miljoen euro of 4 procent van de totale wereldwijde omzet. Bij meerdere overtredingen kan de totale geldboete niet hoger zijn dan die voor de zwaarste inbreuk.

In tegenstelling tot in de Wbp is de AP met ingang van de verordening niet verplicht om eerst een bindende aanwijzing op te leggen voordat een boete kan worden opgelegd. Wel moet de AP op grond van artikel 79 lid 2a rekening houden met een groot aantal omstandigheden bij het opleggen van de boete, waaronder de getroffen beveiligingsmaatregelen, de categorieën persoonsgegevens die in het geding zijn en de mate waarin er met de toezichthoudende autoriteit is samengewerkt om de inbreuk te verhelpen en de mogelijke negatieve gevolgen ervan te beperken.

44 De Boetebeleidsregels Autoriteit Persoonsgegevens 2016 is online te raadplegen via: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebeleidsregels_autoriteit_persoonsgegevens_staatscourant_2016-2043_0.pdf.

45 In geval van recidive verhoogt de AP de boete met 50 procent, tenzij dat in het concrete geval onredelijk zou zijn (art. 9.1 sub a Boetebeleidsregels). Niet-nakoming van een bindende aanwijzing geldt niet als eenzelfde of soortgelijke overtreding (art. 9.2 Boetebeleidsregels).

IMPLEMENTATIE

Bescherming van persoonsgegevens draait niet alleen om het nemen van technische en organisatorische maatregelen en het zorgen voor een degelijk beleid. De maatregelen zullen verder moeten reiken dan een verdeling van rollen, taken en verantwoordelijkheden voor mensen die zich dagelijks actief met bescherming van persoonsgegevens bezighouden. Er moet ook worden nagedacht over de wijze waarop privacy wordt geïmplementeerd in de organisatie. Daarbij gaat het om aspecten als (risico)analyses en het creëren van bewustwording en bewustzijn.

Omdat elke woningcorporatie op een andere manier is ingericht en andere prioriteiten stelt, is het niet mogelijk om een blauwdruk op te stellen waaraan elke woningcorporatie kan voldoen. In plaats daarvan zullen hieronder een aantal korte handreikingen worden gedaan waarmee de Wbp kan worden geïmplementeerd in de woningcorporatie. In bijlage 3 vindt u tevens een algemeen stappenplan over de implementatie van privacy.

1. GAP-ANALYSE

Een eerste stap die kan worden gezet bij het implementeren van privacy in de organisatie is door het maken van een gap-analyse. Bij gap-analyses wordt de huidige stand van zaken en de gewenste stand van zaken geanalyseerd. Hetgeen daartussen overblijft is het 'gat' dat moet worden aangepakt. In plaats van de term 'gap-analyse' wordt ook wel de term 'quick scan' gebruikt.

Het uitvoeren van gap-analyses is bedoeld om snel in kaart te brengen waar de risico's voor de organisatie zich bevinden en om vast te stellen of er leemten zijn in de verwerking van persoonsgegevens. Op basis van deze analyses kunnen vervolgens allerlei activiteiten worden uitgevoerd, zoals Privacy Impact Assessments (zie hieronder) en risicoanalyses. Dergelijke analyses kunnen zowel organisatiebreed als op specifieke processen worden toegepast, en zijn vaak een resultaat van een audit, waarbij wordt vastgesteld waaraan een organisatie nog moet werken om te voldoen aan de auditeisen. Ook binnen de informatiebeveiliging komen gap-analyses veelvuldig terug.

Een complete inventarisatie van alle verwerkingen en persoonsgegevens binnen de organisatie is niet noodzakelijk voor het uitvoeren van een gap-analyse. Er kan ook gekeken worden welke gaten er in de bescherming van persoonsgegevens zitten door specifiek te kijken naar documenten en implementatie van documenten, of door bestaande activiteiten verder door te lichten. Er kan bijvoorbeeld worden onderzocht in hoeverre de afspraken in de bewerkersovereenkomst up to date zijn met het oog op de meldplicht datalekken. Leemten in de bescherming van persoonsgegevens kunnen ook worden opgespoord door het uitvoeren van steekproeven bij callcenters, beveiligers en andere medewerkers om de naleving en het privacybewustzijn vast te stellen.

Na het vaststellen van de gaten in de bescherming van persoonsgegevens moet de oplossingsrichting worden uitgewerkt en een keuze worden gemaakt welke gaten als eerste worden gedicht. De afweging welke oplossingen eerst gekozen worden, is van verschillende factoren afhankelijk; vaak is dit economisch gestuurd. Een andere manier om te kijken naar de oplossingsrichtingen is om te analyseren met welke oplossing het meeste resultaat behaald kan worden, in plaats van te kijken naar de kosten per op te lossen gat. Welke keuze ook wordt gemaakt, uiteindelijk moeten de maatregelen in een plan worden opgepakt en uitgevoerd.

In het kader van privacycompliance is het in ieder geval zinvol om, mede met het oog op de aanstaande AVG, de organisatie goed door te lichten om te kijken waar de komende jaren budget voor moet worden vrijgemaakt.

2. PRIVACY IMPACT ASSESSMENTS (PIA'S)

Met een Privacy Impact Assessment (PIA) wordt onderzocht welk effect een of meerdere gegevensverwerkingen hebben op de privacy van de betrokkenen. Het is daarmee een middel om te kijken of voldoende rekening wordt gehouden met de privacybelangen van betrokkenen en of verwerking(en) rechtmatig zijn. Het uitvoeren van PIA's geeft duidelijkheid over de mogelijke negatieve gevolgen van de verwerking van persoonsgegevens voor

de betrokkenen, brengt de risico's van de gegevensverwerking(en) in kaart en beoordeelt geïmplementeerde waarborgen. Daarnaast wordt bekeken of de verwerking past bij het bedrijfsbeleid. De Autoriteit Persoonsgegevens formuleert dit als volgt:

'De PIA stimuleert organisaties om proactief na te denken over vragen als:
a. Wat is de impact van het beoogde project op de privacy van betrokkenen?
b. Wat zijn de risico's voor de betrokkenen en voor de organisatie?
c. Is een aanpak die minder gevolgen heeft voor de privacy ook mogelijk, gegeven de doelstellingen van het project?'[46]

Op basis van de PIA wordt vervolgens besloten of de (voorgenomen) gegevensverwerking doorgang kan vinden, aanpassing nodig heeft, of te risicovol is. Het feit dat een PIA is uitgevoerd zegt op zichzelf overigens nog niets over de vraag of men handelt in overeenstemming met de geldende wet -en regelgeving. De uitkomsten van de PIA moeten immers nog worden verwerkt.

De PIA is een instrument om vooraf de risico's in te kunnen schatten van een verwerking van persoonsgegevens en geen nalevingsinstrument om achteraf te beoordelen of de verwerking in overeenstemming is met de wet. In de praktijk worden veel PIA's echter ook achteraf uitgevoerd om alsnog de risico's van de verwerking in te kunnen schatten en daarop te kunnen reageren. Feitelijk wordt de PIA dan als nalevingsinstrument ingezet. Dit is op zichzelf geen probleem, maar de uitkomsten van een PIA kunnen resulteren in kostbare of tijdrovende mitigerende maatregelen die te voorkomen waren geweest als *vooraf* was nagedacht over de privacyeffecten van de activiteiten.

De keuze voor een bepaalde PIA-methode en -model is afhankelijk van de soort verwerking van persoonsgegevens (complex of eenvoudig), of de PIA wordt uitgevoerd door experts of ook door 'leken' ingevuld moet kunnen worden en de gewenste diepgang van de PIA. Er is dus geen voorgeschreven model voor het uitvoeren van een PIA. Wel is er een aantal openbare modellen beschikbaar, zoals de NOREA PIA van de beroepsgroep IT-auditors[47] en het Toetsmodel PIA Rijksdienst[48]. Daarnaast worden maatwerk-PIA's aangeboden, simpelweg omdat een standaardmodel een handreiking is, maar, net als informatiebeveiligingsbeleid, passend moet worden gemaakt bij het product, de dienst, het systeem of het proces van de betreffende corporatie. Voordat een PIA passend wordt gemaakt moet ten minste duidelijk zijn wat de reikwijdte van de PIA is (of zou moeten zijn).

Neem de volgende zaken mee bij de beslissing om een PIA uit te voeren:
1. Bepaal in welk stadium de PIA wordt uitgevoerd. Ook wanneer de omstandigheden van een project tijdens de looptijd veranderen, is het raadzaam de PIA te herhalen en/of te evalueren bij de afsluiting van een project.
2. Kies een geschikt PIA-model. Een PIA-model bestaat vaak uit een meer of minder gedetailleerde vragenlijst. Op die lijst staan zowel feitelijke en technische vragen als vragen die zijn gebaseerd op nationale en Europese wetgeving. Een goed model is een overzichtelijk model. Hierbij worden de juiste vragen gesteld, zijn de vragen eenvoudig te beantwoorden door eigen medewerkers of waar nodig door iemand met specifieke kennis op het gebied van privacyrecht en informatiebeveiliging.
3. Bepaal wie de PIA uitvoert. Dit kan een multidisciplinair team zijn of een enkele persoon die verantwoordelijk is voor (het toezicht op) de verwerking van persoonsgegevens.
4. Bepaal de reikwijdte van de uit te voeren PIA. Bepaal ook wat niet onderzocht en beoordeeld wordt. Schrijf dit op in een aparte inleiding bij de PIA.

46 Autoriteit Persoonsgegevens, Advies concept Toetsmodel Privacy Impacy Assessment, 4/12/2012, p. 4. Online te raadplegen via: https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/adv/z2012-00847.pdf.
47 NOREA, Privacy Impact Assessment (PIA). Introductie, handreiking en vragenlijst, november 2015. Online te raadplegen via: http://www.norea.nl/readfile.aspx?ContentID=82987&ObjectID=1265283&Type=1&File=0000042779_PIA%20versie%201.2%20def.pdf.
48 Ministerie van Binnenlandse zaken, Toetsmodel Privacy Impact Assessment Rijksdienst, 24/06/2013. Online te raadplegen via: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/publicaties/2013/06/24/toetsmodel-privacy-impact-assessment-pia-rijksdienst/toetsmodel-privacy-impact-assessment-pia-rijksdienst.pdf.

PIA's bij bewerkers
PIA's zijn niet alleen nuttig voor interne gegevensverwerkingen, maar ook voor gegevensverwerkingen bij externe leveranciers (bewerkers). Met name bij het contracteren van bewerkers die omvangrijke of gevoelige gegevensverwerkingen verrichten kan het handig zijn om het uitvoeren van een PIA onderdeel te laten uitmaken van de overeenkomst. Dit kan bijvoorbeeld worden gerealiseerd door de bewerker een vragenlijst te laten invullen waarmee de risico's van de verwerkingen bij de leverancier in kaart worden gebracht. Gedurende de looptijd van de overeenkomst of wanneer de situatie rondom een product, dienst, systeem of proces wijzigt, moet een PIA opnieuw (deels) worden uitgevoerd. Op deze wijze blijft de corporatie op de hoogte van risicoveranderingen en kunnen risico's in zijn geheel makkelijker worden geanalyseerd.

2.1 PRIVACY IMPACY ASSESSMENTS IN DE AVG

Met de inwerkingtreding van de AVG wordt de uitvoering van PIA's nader ingebed (artt. 33 en 34 AVG).
Een PIA moet verplicht worden uitgevoerd in geval van:

- een verwerking dat een verhoogd risico voor de rechten en vrijheden van individuen vormt, gelet op de aard, de omvang, de context of de doelen van de gegevensverwerking. De verantwoordelijke moet daarbij een FG (indien aangesteld) consulteren;
- een systematische en uitgebreide beoordeling van persoonlijke aspecten, die is gebaseerd op geautomatiseerde verwerking (inclusief profiling), op grond waarvan besluiten met rechtsgevolgen worden genomen of die op andere wijze significante gevolgen hebben voor een individu (zie ook paragraaf 11.4 over geautomatiseerde individuele besluitvorming);
- verwerkingen van bijzondere of strafrechtelijke persoonsgegevens op grote schaal;
- een omvangrijke systematische surveillance van publiek toegankelijk gebied;
- een verwerking die op de lijst van de toezichthouder voorkomt waarvoor een PIA verplicht is gesteld.

Een PIA bevat ten minste:

- een beschrijving van de voorziene verwerkingen en de doelen die daarmee gediend zijn, inclusief een eventueel gerechtvaardigd belang;
- een beoordeling van de noodzakelijkheid en evenredigheid in verhouding tot de doelen van de verwerking;
- een beoordeling van de risico's voor de rechten en vrijheden van de betrokkenen, en;
- de voorgenomen maatregelen om deze risico's te adresseren en om compliance met de verordening aan te tonen.

De verantwoordelijke moet de toezichthouder consulteren over de verwerking, wanneer uit de PIA blijkt dat de verwerking hoge risico's kent als geen maatregelen worden genomen.

Wanneer een verwerking gebaseerd is op een wettelijke plicht of publiek(rechtelijk)e taak, hoeft een PIA niet nogmaals te worden uitgevoerd wanneer dit reeds is gebeurd in het kader van deze wettelijke grondslag.

3. BEWUSTWORDING EN BEWUSTZIJN

Privacy is een onderwerp dat de hele organisatie aangaat, en vanuit die positie is het creëren van bewustwording dan ook noodzakelijk. Wanneer iedereen in de organisatie zich bewust is van de eigen verantwoordelijkheid op het gebied van privacy, draagt dit ook bij aan verbetering van bescherming van persoonsgegevens. Werknemers vormen namelijk een belangrijke bron van inbreuken. Bewustzijn en permanente educatie is daarom hard nodig.

3.1 BEWUSTWORDING

Bewustwording en bewustzijn moeten los van elkaar worden gezien. In de eerste plaats is het van belang om voor bewustwording te zorgen binnen de organisatie. Dit is vaak de taak van degene die organisatorisch belast is met privacyzaken, zoals een privacy officer, jurist of security officer. Deze taak ligt bijvoorbeeld bij een beleidsmedewerker of bestuurssecretaris, afhankelijk van de inrichting van de organisatie. Wie de taak ook op zich neemt, hij/zij is verantwoordelijk voor het kweken van bewustwording.

Om bewustwording te bereiken zullen medewerkers iets moeten leren. Kennisverspreiding realiseer je door middel van training, beleid en procedures, maar ook door gebruik van technische middelen en regelmatige assessment. Zo wordt er binnen een organisatie fundamenteel begrip gekweekt van het belang van privacy in de dagelijkse processen. Privacybeleid en procedures gelden voor alle medewerkers die op de een of andere manier met persoonsgegevens in aanraking komen. Als er sprake is van sub-beleid (bijvoorbeeld specifiek voor HR, of leveranciers), dan is dit meestal bij de eigen afdeling ondergebracht. Deze afdeling moet ook zorgen voor de erkenning van het belang van deze procedures en het management moet het beleid zelf actief volgen. Er is immers een verschil tussen beleid hebben en beleid uitvoeren.

Bewustwordingscampagnes
Bewustwording kan op allerlei manieren worden gecreëerd. Een variant is die van phishing. Hierbij worden medewerkers via bijvoorbeeld een mail gevraagd om hun gebruikersnaam en wachtwoord achter te laten. De ingevulde gegevens komen dan in handen van de afdeling IT/IB, zodat precies kan worden gemeten welk deel van de medewerkers de nepmail niet heeft doorzien. Een ander voorbeeld is het inzetten van *mystery shoppers* die bijvoorbeeld proberen om met een inzageverzoek persoonsgegevens van anderen in te zien. Door medewerkers te voorzien van feedback, wordt op een effectieve manier bewustwording gecreëerd. Het is bij dergelijke campagnes wel van belang dat ook de privacy van de werknemer wordt gewaarborgd: het is bijvoorbeeld niet zomaar toegestaan om interne camerabeelden te gebruiken voor trainingsdoeleinden.

Het bijwonen van kennissessies is soms niet voldoende om bewustwording te creëren, er moet een min of meer blijvende herinnering zijn aan hetgeen geleerd is, zodat bewustzijn wordt aangewakkerd. Dit kan door middel van posters, flyers, periodieke toetsen (met resultaten in het personeelsdossier), het actief aanbieden van informatie via nieuwsbrieven of meer passief via een intern (privacy)portaal. De afdeling Communicatie is de aangewezen plek om dit soort activiteiten neer te leggen.

Vergeet niet dat veel privacyvraagstukken ook met informatiebeveiliging te maken hebben (plak geen wachtwoorden op het scherm, deel geen inlogcodes et cetera). Bij het inrichten van campagnes rondom bewustwording kunnen dan ook zowel informatiebeveiliging als privacy worden meegenomen.

3.2 BEWUSTZIJN

Op de tweede plaats is bewustzijn van belang. Dit is een uiting van de eerdere bewustwordingsfase, waarbij medewerkers actief knelpunten kunnen en durven signaleren. Bewustzijn vereist onderhoud. Dat betekent dat er ten minste moet worden nagedacht over herhaalde trainings- en kennissessies, maar ook dat (beleids)documenten periodiek herzien, gecommuniceerd én geïmplementeerd moeten worden. Bewustzijn kun je bovendien inzichtelijk maken door te meten wat medewerkers weten over privacy, en door te toetsen of men zich aan de regels houdt.

Ook door middel van technische maatregelen kan bewustzijn worden ondersteund. Door het slim inrichten van software kan ook worden voorkomen dat meer gegevens worden verzameld dan noodzakelijk (als je het niet hoeft te weten, vraag er dan niet om!). Ook kan goed onderhouden toegangscontrole zorgen dat mensen geen toegang hebben tot informatie waar ze gezien hun functie ook geen noodzaak voor hebben.

Zorg bijvoorbeeld voor up-to-date belscripts (werkinstructies) voor de klantenservice, en toets periodiek of medewerkers zich aan de regels houden bij het verstrekken van informatie. Test ook het proces rondom inzage- en correctieverzoeken.

3.3 ZONDER BETROKKENHEID GEEN BEWUSTWORDING (OF BEWUSTZIJN)

Bewustwording en bewustzijn creëren kan alleen maar als het hoogste management de noodzaak van bescherming van persoonsgegevens actief uitdraagt. Dit geldt onafhankelijk van de motivatie voor de bescherming van persoonsgegevens – van compliance-wens, privacy als *unique selling point*, tot het vermijden van boetes. Waarom zouden medewerkers anders het belang inzien van privacy?

Het creëren van bewustwording en het behouden van bewustzijn bij het hoger management is op zichzelf soms al een hele taak. Vanzelfsprekend moet immers budget worden vrijgemaakt om het privacyprogramma succesvol te kunnen implementeren. Door privacy meetbaar en privacyrisico's inzichtelijk te maken voor het hoger management komt privacy sneller op de agenda.

4. CHECKLIST VOOR SELF-ASSESSMENT

Om te bepalen of uw woningcorporatie voldoet aan de normen van de Wbp is hieronder een overzicht gemaakt van alle normen waaraan u moet voldoen. Zoals bij het onderdeel 'doelen en taken' hieronder is uitgelegd is het de bedoeling dat per gegevensverwerkingsdoel deze checklist wordt afgelopen. Dit betekent dat u voor bijvoorbeeld het doel personeelsadministratie de checklist moet doorlopen, maar ook apart voor het doel huuradministratie. Benadrukt moet worden dat het hier gaat om een sterk beknopt overzicht van de Wbp en alleen dient als quick scan.

Onderwerp	Toelichting
Persoonsgegevens Welke persoonsgegevens worden verwerkt?	Persoonsgegevens zijn alle gegevens die zo kenmerkend zijn voor een bepaalde persoon dat hij/zij aan de hand van die gegevens kan worden geïdentificeerd. Hoofdregel is dat een persoon identificeerbaar is als zijn identiteit zonder onevenredige inspanning vastgesteld kan worden. Hieronder vallen zowel gegevens die direct identificerend zijn (zoals namen) als indirect identificeerbare gegevens die alleen in combinatie met andere gegevens tot een bepaalde persoon herleidbaar zijn (unieke gegevens, zoals een burgerservicenummer en unieke combinaties, zoals geboortedatum en adres). Persoonsgegevens zien alleen op in leven zijnde, natuurlijke personen. Bedrijfsgegevens, met uitzondering van bepaalde namen van eenmanszaken, vallen hier dus niet onder.
Doelen en taken Voor welke doelen en taken worden er persoonsgegevens verwerkt? (Zorg dat voor elk van de doelen wordt gecontroleerd of voldaan wordt aan onderstaande normen!)	Persoonsgegevens mogen alleen voor bepaalde, uitdrukkelijk omschreven doeleinden worden verzameld (artikel 7 Wbp). Dit kan uiteenlopen van het uitvoeren van een huurovereenkomst tot aan het bestrijden van woonfraude en het versturen van nieuwsbrieven.
Grondslag Is er een grondslag voor het verwerken van de gegevens?	Persoonsgegevens mogen alleen worden verwerkt als er een wettelijke grondslag is. De wettelijk toegestane grondslagen zijn opgesomd in artikel 8 Wbp. De belangrijkste voor woningcorporaties zijn 1) de uitvoering van een overeenkomst, 2) gerechtvaardigd belang en 3) toestemming van de betrokkene.
Kwaliteit en dataminimalisatie Worden er niet meer gegevens verwerkt dan noodzakelijk is voor het doel?	Persoonsgegevens mogen alleen worden verwerkt als deze, gelet op het doel van de verwerking, toereikend, ter zake dienend en niet bovenmatig zijn. Dit wordt ook wel dataminimalisatie genoemd. De Wbp spreekt ook wel van het 'noodzakelijk' zijn van informatie. Is de noodzaak om bepaalde gegevens voor het betreffende doel te verwerken er niet, dan mogen de gegevens niet worden gebruikt. Daarnaast moeten persoonsgegevens juist en nauwkeurig zijn (artikel 11 Wbp).
Doelbinding Worden gegevens verder verwerkt voor andere doelen of taken?	Het principe van doelbinding bepaalt dat gegevens alleen mogen worden verwerkt voor het doel waarvoor ze zijn verzameld en voor verenigbare doeleinden. Of andere doeleinden verenigbaar zijn met het oorspronkelijke doel van verzameling, zal per geval moeten worden bepaald. Artikel 9 lid 2 Wbp noemt een vijftal factoren aan de hand waarvan de verenigbaarheid moeten worden beoordeeld.
Melding van gegevensverwerking Is de gegevensverwerking gemeld bij de AP?	Alle gegevensverwerkingen moeten worden gemeld bij de Autoriteit Persoonsgegevens (artikel 27 Wbp), tenzij de verwerking is vrijgesteld in het Vrijstellingsbesluit Wbp. Voor sommige gegevensverwerkingen is het verplicht om een voorafgaand onderzoek aan te vragen (artikel 31 Wbp).

Onderwerp	Toelichting
Beveiligingsmaatregelen Worden persoonsgegevens afdoende beveiligd?	Persoonsgegevens moeten afdoende worden beveiligd om onrechtmatig gebruik en verlies van persoonsgegevens tegen te gaan (artikel 13 Wbp). Het een en ander moet worden vastgelegd in een IB-beleid.
Verstrekking aan derden Worden er persoonsgegevens verstrekt aan derden?	Het verstrekken van gegevens is een verwerking van persoonsgegevens en moet dus voldoen aan de normen uit de Wbp. Verwerkt een partij persoonsgegevens in opdracht van de verantwoordelijke, dan is een bewerkersovereenkomst verplicht (artikel 14 Wbp).
Bewaren en vernietigen Worden gegevens niet langer bewaard dan noodzakelijk?	Persoonsgegevens mogen niet langer worden bewaard dan nodig is voor het doel waarvoor de gegevens zijn verzameld (artikel 10 Wbp). Als de bewaartermijn van persoonsgegevens voorbij is of gegevens niet meer noodzakelijk zijn voor het doel van de gegevensverwerking, dan moeten de persoonsgegevens worden vernietigd.
Functionaris voor de gegevensbescherming (FG) Is er een functionaris voor de gegevensbescherming (FG) aangesteld?	Een FG is een onafhankelijke persoon die toezicht houdt op naleving van de Wbp en aanbevelingen doet over privacyvraagstukken binnen de organisatie. Op grond van de Wbp staat het particuliere organisaties vrij om een FG aan te stellen (artikel 62 e.v. Wbp).
Informatieplicht Worden de betrokkenen geïnformeerd over de verwerking van hun persoonsgegevens?	Betrokkenen hebben recht op transparante informatie over de verwerking van hun persoonsgegevens. Dit is een uitwerking van de plicht tot zorgvuldige en behoorlijke verwerking van persoonsgegevens. De verantwoordelijke dient daarom heldere informatie te verstrekken over de verwerking van zijn persoonsgegevens (artikelen 33 en 34 Wbp).
Rechten van betrokkenen Kunnen betrokkenen hun rechten uitoefenen?	Betrokkenen hebben het recht hun persoonsgegevens in te zien, aan te passen en zonodig te laten verwijderen (artikelen 35 en 36 Wbp). Daarnaast hebben betrokkenen het recht om zich te verzetten tegen bepaalde gegevensverwerkingen (artikelen 40 en 41 Wbp). Het is van belang om interne processen vast te stellen over de wijze waarop betrokkenen hun rechten kunnen uitoefenen.
Bijzondere en gevoelige persoonsgegevens Worden er bijzondere en/of gevoelige persoonsgegevens verwerkt? (Let op: voor deze persoonsgegevens gelden extra zware normen!)	Bijzondere persoonsgegevens mogen niet worden verwerkt, tenzij de wet een uitzondering biedt (art. 16 Wbp). Bijzondere persoonsgegevens zijn gegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag. Gevoelige persoonsgegevens zijn gegevens die geen bijzondere persoonsgegevens zijn in de zin van de Wbp, maar wel privacygevoelig zijn zoals financiële gegevens. Burgerservicenummers zijn apart gereguleerd (art. 24 Wbp). Aan beide categorieën gegevens stelt de wet extra zware eisen, bijvoorbeeld bij de beveiligingsmaatregelen en de verstrekking aan derden.
Meldplicht datalekken Zijn er processen ingericht voor het melden van datalekken?	Datalekken moeten per 1 januari 2016 worden gemeld door de verantwoordelijke bij de AP en in sommige gevallen ook bij de betrokkene (artikel 34a Wbp). Om deze melding binnen de wettelijke termijn van 72 uur te kunnen melden, is het van belang dat de juiste processen zijn vastgesteld en afspraken zijn gemaakt met bewerkers.

Q&A

Wanneer treedt de Algemene Verordening Gegevensbescherming (AVG) in werking en waar moet ik rekening mee houden?
Op 25 mei 2018 zal de Europese Algemene Verordening Gegevensbescherming (hierna: AVG of verordening) van toepassing zijn en de Wbp vervangen. De AVG bevat vooral aanscherpingen en strengere eisen ten opzichte van de Wbp met hier en daar een aantal vernieuwingen. De optimale manier om voor te bereiden op de AVG is daarom om eerst te kijken naar de normen van de Wbp. Daar waar de AVG afwijkt ten opzichte van de Wbp is in dit handboek een nadere toelichting gegeven.

Wat houdt de meldplicht aan de Autoriteit Persoonsgegevens precies in?
De Wbp kent tegenwoordig twee verschillende meldplichten. De eerste meldplicht is de plicht om alle gegevensverwerkingen te melden bij de Autoriteit Persoonsgegevens. Deze worden bijgehouden in een openbaar register. Deze meldplicht van gegevensverwerkingen zal komen te vervallen zodra de AVG in werking is getreden. Zie voor meer informatie paragraaf 5. De tweede meldplicht die nieuw is per 1 januari 2016, is de plicht om datalekken te melden bij de Autoriteit Persoonsgegevens. Deze meldingen worden niet bijgehouden in een openbaar register. Zie voor meer informatie paragraaf 13.

Wat zijn goede beveiligingsmaatregelen?
De wet bepaalt dat persoonsgegevens moeten worden beveiligd met 'passende technische en organisatorische beveiligingsmaatregelen'. Door deze open norm is het niet op voorhand te zeggen welke beveiligingsmaatregelen wel of niet passend zijn volgens de Wbp. Dit zal onder meer afhangen van het doel waarvoor gegevens worden verwerkt, de gevoeligheid van de gegevens en de voor handen zijnde technieken om gegevens te beschermen. Het is daarom aan te raden om een risicoanalyse te maken en op basis daarvan de juiste beveiligingsmaatregelen te treffen. De Baseline Informatiebeveiliging (woning)Corporaties biedt eveneens een richtlijn voor informatiebeveiliging bij woningcorporaties. Zie voor meer informatie paragraaf 6.

Hoe bepaal ik de bewaartermijnen van persoonsgegevens?
Bij het bepalen van de bewaartermijn moet in ieder geval rekening worden gehouden met de volgende factoren:
- het doel/de doelen waarvoor de persoonsgegevens verzameld zijn (de noodzaak om de gegevens voor dat doel te bewaren);
- het vrijstellingsbesluit Wbp;
- de wettelijke bewaartermijnen.

Zie voor meer informatie paragraaf 8.

Is het verplicht om een functionaris voor de gegevensbescherming (FG) in dienst te hebben?
Nee, op grond van de Wbp is het niet verplicht om een FG in dienst te hebben. De aankomende AVG verplicht woningcorporaties waarschijnlijk ook niet om een FG in dienst te nemen. Niettemin kan het instellen van een FG wel voordelen bieden. Zie voor meer informatie paragraaf 9.

Mogen strafrechtelijke gegevens worden uitgewisseld met andere partijen?
Strafrechtelijke gegevens zijn bijzondere persoonsgegevens en mogen in de regel niet worden verwerkt, tenzij de Wbp een uitzondering biedt. Artikel 22 lid 4 Wbp bepaalt dat, in afwijking van het verwerkingsverbod, het delen van strafrechtelijke gegevens buiten een concern alleen is toegestaan als er passende en specifieke waarborgen zijn getroffen en de Autoriteit Persoonsgegevens een voorafgaand onderzoek heeft gedaan. Zie voor meer informatie paragraaf 12.1 en 12.2.

Wat zijn de regels voor het verwerken van burgerservicenummers?
De Wbp bepaalt in artikel 24 dat het bsn en andere wettelijke persoonsnummers (zoals kentekengegevens) niet mogen worden verwerkt, tenzij een wet de verplichting bevat om het nummer te verwerken. Is er sprake van een wettelijke plicht, dan mag het bsn alleen worden gebruikt voor het in die wet omschreven doel. Zo is het op grond van de Wet op de Loonbelasting verplicht om het bsn op te slaan van de medewerkers. Burgerservicenummers van huurders moeten worden opgeslagen voor communicatie met de Belastingdienst voor de controle van de huurtoeslag. Zie voor meer informatie paragraaf 12.4.2.

Welke boetes kunnen er worden opgelegd door de Autoriteit Persoonsgegevens?
De Autoriteit Persoonsgegevens is sinds 1 januari 2016 bevoegd om geldboetes op te leggen tot maximaal 820.000 euro of 10 procent van de jaaromzet bij overtreding van de Wbp. Bij het bepalen van de hoogte van de boete zal gekeken worden naar de soort overtreding en de omstandigheden van het geval. In de regel worden deze boetes pas opgelegd nadat er een zogenaamde bindende aanwijzing is opgelegd. Zie voor meer informatie paragraaf 14.

BIJLAGEN

1 MINIMALE WETTELIJKE BEWAARTERMIJNEN

Wet	Soort gegevens waarop de wettelijke bewaartermijn ziet	Minimale bewaartermijn
Art. 2:10 lid 1 en 3 Burgerlijk Wetboek	Gegevens over de vermogenstoestand van de rechtspersoon; van alles betreffende de werkzaamheden van de rechtspersoon	7 jaar
Art. 2:24 Burgerlijk Wetboek	De boeken, bescheiden en andere gegevensdragers van een ontbonden rechtspersoon	7 jaar
Art. 2:61 Burgerlijk Wetboek	De geschriften, waarbij het lidmaatschap van een coöperatie wordt aangevraagd	10 jaar
Art. 2:394 lid 6 Burgerlijk Wetboek	De jaarrekening van een rechtspersoon	7 jaar
Art. 3:15i Burgerlijk Wetboek	Gegevens over de vermogenstoestand van een bedrijf of zelfstandig een beroep	7 jaar
Art. 454 lid 3, boek 7 Burgerlijk Wetboek	Patiëntendossier	15 jaar
Art. 23 lid 5 Wet op de Loonbelasting 1964	Gegevens loonbelasting	5 jaar
Art. 52 Algemene wet inzake rijksbelastingen	Gegevens over de vermogenstoestand van een bedrijf of een zelfstandig beroep, waaronder: boeken, bescheiden en andere gegevensdragers die van belang zijn voor de heffing van belasting.	7 jaar (Fiscale bewaartermijn)
Art. 34a Wet op de Omzetbelasting 1968	Gegevens betreffende onroerende zaken en rechten waaraan deze zijn onderworpen, waaronder: boeken, bescheiden en andere gegevensdragers of de inhoud daarvan	9 jaar
Art. 6a Wet op de Loonbelasting 1964	Kopie identiteitskaart en identiteitskaartnummer	5 jaar
Art. 7.9 Uitvoeringsregeling Loonbelasting 2011	Gegevens van werknemers: a. zijn naam met voorletters; b. zijn geboortedatum; c. zijn burgerservicenummer; d. zijn adres met postcode; e. zijn woonplaats en, ingeval hij niet in Nederland woont, zijn woonland en regio	5 jaar
Art. 12.1 Uitvoeringsregeling Loonbelasting 2011	Loonbelastingverklaring werknemer	5 jaar
Art. 3.2:1 Arbeidstijdenbesluit	Arbeids- en rusttijden werknemer	52 weken
Art. 167 lid 3 Wet op het primair onderwijs	■ Het programma van de voorschoolse educatie dat een leerling heeft gevolgd ■ De duur van het programma dat is gevolgd	2 jaar
Art. 4:69 Algemene wet bestuursrecht	De administratie en de daartoe behorende bescheiden subsidieontvanger	7 jaar
Art. 5.3.4 Wet maatschappelijke ondersteuning 2015	De persoonsgegevens die op grond van deze wet worden verwerkt	15 jaar
Art. 86 lid 1 Zorgverzekeringswet	Het burgerservicenummer van de verzekerde	7 jaar

Wet	Soort gegevens waarop de wettelijke bewaartermijn ziet	Minimale bewaartermijn
Art. 7.3.8 en 7.3.9 Jeugdwet	Gegevens in het dossier; bestaande uit: ■ aantekening van de gegevens omtrent de geconstateerde opgroei- en opvoedingsproblemen, psychische problemen en stoornissen en de te diens aanzien uitgevoerde verrichtingen ■ en andere stukken, een en ander voor zover dit voor een goede hulpverlening aan de betrokkene noodzakelijk is	15 jaar of langer als het van belang is voor de belangen van een ander dan de betrokkene.
Art. 7.18 Mediawet 2008	Opnamen van door de publieke en commerciële media-instellingen, alsmede politieke partijen en de overheid verzorgde programma-aanbod	Tot 2 weken na de uitzending
Art. 169 Pensioenwet	Zakelijke gegevens en bescheiden die betrekking hebben op pensioenregelingen	7 jaar
Art. 15 Wet arbeid vreemdelingen	Gegevens over de identiteit van de vreemdeling	5 jaar
Art. 5 Wet controle op rechtspersonen	Aantekeningen van risicomeldingen rechtspersonen	2 jaar
Art. 4:90e Wet op het financieel toezicht	Relevante gegevens over de door een beleggingsonderneming verrichte transacties in financiële instrumenten	5 jaar
Art. 33 Wet ter Voorkoming van Witwassen en Financieren van Terrorisme (WWFT)	Alle gegevens die in het kader van een cliëntonderzoek (customer due diligence) zijn verkregen	5 jaar
Art. 34 WWFT	Meldingen over ongebruikelijke transacties	5 jaar
Art. 14 Besluit prudentiële regels Wet financieel toezicht (Wft)	Alle gegevens die in het kader van een cliëntonderzoek (customer due diligence) zijn verkregen	5 jaar
Art. 24 Wet op het notarisambt	Boeken, bescheiden en andere gegevensdragers betreffende de kantoor- en privé-administratie van een notaris	7 jaar

2 VOORBEELD STANDAARDCLAUSULES DATALEKKEN

DEFINITIE

Datalek: een inbreuk op de beveiliging, bedoeld in artikel 13 Wbp, die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van Persoonsgegevens.

1. DATALEKKEN

1.1 [invoegen bedrijfsnaam bewerker] dient uiterlijk binnen [##] uur nadat een Datalek is geconstateerd bij [invoegen bedrijfsnaam bewerker] of door haar aangestelde Sub-bewerker(s), [invoegen bedrijfsnaam verantwoordelijke] op de hoogte te stellen van ieder Datalek. Deze verplichting geldt gedurende 24 uur per dag en 7 dagen in de week. Het informeren van de verantwoordelijke hierover gebeurt op een wijze die gepast is, gelet op de omstandigheden van het geval. **Optioneel:** [invoegen bedrijfsnaam verantwoordelijke] en [invoegen bedrijfsnaam bewerker] wijzen elk een contactpersoon aan die verantwoordelijk is voor de onderlinge communicatie over Datalekken.

1.2 [invoegen bedrijfsnaam bewerker] dient [invoegen bedrijfsnaam verantwoordelijke] bij een Datalek binnen de termijn genoemd in 10.1, voor zover redelijkerwijs bekend, de volgende informatie te verstrekken:

- een samenvatting van de gebeurtenissen aangaande het Datalek;
- de datum waarop, of de periode waarin het Datalek heeft plaatsgevonden;
- de (vermeende) oorzaak van het Datalek;
- een beschrijving van de soort groep en het aantal personen waarvan de gegevens bij het Datalek (mogelijk) betrokken zijn en, indien bekend, de identiteit van deze Betrokkenen;
- de categorieën persoonsgegevens die (mogelijk) zijn getroffen door het Datalek;
- een beschrijving of de getroffen persoonsgegevens op enige wijze zijn versleuteld, geanonimiseerd, gepseudonimiseerd of op afstand kunnen worden gewist;
- de getroffen of te nemen maatregelen om de gevolgen van het lek te beperken en herhaling te voorkomen.
- **Optioneel:** informatie over de contactpersoon waarbij meer informatie over het Datalek verkregen kan worden. (Niet noodzakelijk als de optionele clausule in 1.1 wordt gebruikt.)
- **Optioneel:** [invoegen bedrijfsnaam bewerker] dient de informatie door middel van een standaardformulier, weergegeven in Bijlage [X], te verstrekken aan [invoegen bedrijfsnaam verantwoordelijke].

1.3 [invoegen bedrijfsnaam bewerker] dient [invoegen bedrijfsnaam verantwoordelijke] uit eigen beweging op de hoogte houden van alle relevante ontwikkelingen omtrent het Datalek die zich voordoen na het moment van het verstrekken van de informatie genoemd in 10.2. [invoegen bedrijfsnaam bewerker] dient binnen redelijke termijn te reageren op aanvullende vragen van [invoegen bedrijfsnaam verantwoordelijke] met betrekking tot het Datalek.

1.4 [invoegen bedrijfsnaam bewerker] dient, zodra een Datalek is geconstateerd, zo spoedig mogelijk en voor eigen rekening en risico alle maatregelen te treffen die redelijkerwijs noodzakelijk zijn om de schadelijke gevolgen van het Datalek te beperken en om herhaling te voorkomen.

1.5 [invoegen bedrijfsnaam bewerker] zal [invoegen bedrijfsnaam verantwoordelijke] alle medewerking en informatie verlenen die redelijkerwijs nodig is om de Autoriteit Persoonsgegevens, onderscheidenlijk de Betrokkene adequaat in te lichten over de oorzaak en omvang het Datalek. Het is [invoegen bedrijfsnaam bewerker] niet toegestaan het Datalek zelfstandig te melden bij de Autoriteit Persoonsgegevens en de Betrokkenen. **Optioneel:** Indien de omstandigheden daartoe aanleiding geven, verleent [invoegen bedrijfsnaam bewerker] [invoegen bedrijfsnaam verantwoordelijke] toegang tot het systeem van [invoegen bedrijfsnaam bewerker] en/of van door [invoegen bedrijfsnaam bewerker] ingeschakelde derden als bedoeld in 3.5.

1.6 **Optioneel:** Wanneer het Datalek is ontstaan door het niet-nakomen van [invoegen bedrijfsnaam bewerker] van deze Bewerkersovereenkomst, zijn alle kosten en schade ten gevolge van het Datalek voor rekening en risico van [invoegen bedrijfsnaam bewerker]. Dit zonder afbreuk van de mogelijkheid voor [invoegen bedrijfsnaam verantwoordelijke] voor het inschakelen van rechtsmiddelen.

2. CONTROLE

2.1 [invoegen bedrijfsnaam verantwoordelijke] en [invoegen bedrijfsnaam bewerker] bespreken minimaal een maal per jaar de naleving van de overeengekomen technische en organisatorische beveiligingsmaatregelen van [invoegen bedrijfsnaam bewerker], dan wel die van door [invoegen bedrijfsnaam bewerker] ingeschakelde derden. Op verzoek van [invoegen bedrijfsnaam verantwoordelijke] kan dit overleg frequenter plaatsvinden.

2.2 [invoegen bedrijfsnaam bewerker] zal alle redelijkerwijs benodigde medewerking verlenen aan de controle en er voor zorg dragen ook de door hem ingeschakelde derden hiertoe de redelijkerwijs benodigde medewerking zullen verlenen.

2.3 Het uitvoeren van een controle zal niet tot een vertraging van de door [invoegen bedrijfsnaam verantwoordelijke] in het kader van de Overeenkomst en deze Bewerkersovereenkomst te verrichten werkzaamheden mogen leiden. Indien dat onverhoopt toch het geval is, zullen Partijen in overleg treden teneinde daarvoor zo snel mogelijk een oplossing te vinden.

3 STAPPENPLAN IMPLEMENTATIE PRIVACY

Het implementeren van privacy in de organisatie kan grofweg in drie fases worden onderscheiden: de start, de inhoud en het beheer. In schematisch overzicht komt dit op het volgende neer:

1. Start	2. Inhoud	3. Beheer
■ Wat heeft de organisatie nu geregeld? ■ Waar wil de organisatie naartoe?	■ Inventarisatie gegevens en processen ■ Huidige compliancy met Wbp ■ Activiteiten om privacy te beheersen	■ Controleren van (nieuwe) activiteiten ■ Communicatie over privacy

In de eerste fase wordt geïnventariseerd wat de woningcorporatie grofweg allemaal al heeft geregeld op het gebied van privacy. Dit kunnen bijvoorbeeld documenten als standaardbewerkersovereenkomsten zijn, maar ook ingebedde processen zoals informatiebeveiliging. Daarna wordt op algemene wijze geformuleerd waar de woningcorporatie naartoe wil op het gebied van de bescherming van persoonsgegevens. De woningcorporatie kan bijvoorbeeld nastreven om de privacy integraal, in alle werkprocessen onder handen te nemen, maar er kan ook voor worden gekozen om alleen bepaalde probleempunten aan te pakken, zoals de meldplicht datalekken.
Een *maturity model* biedt een standaardkader om de mate van volwassenheid van het privacyprogramma te toetsen. Hiermee kan worden vastgesteld waar de organisatie nu staat, en waar de organisatie naartoe wil:

Niveau	Inhoud
1. Ad Hoc	Geen gestructureerde visie, voldoet nauwelijks aan de wet, geen regie. Informele, incomplete en inconsistente regels.
2. Repeatable	Geen gestructureerde visie, maar herhaling van zetten.
3. Defined	Bepaalde processen zijn netjes ingericht (privacy by design op organisatorisch niveau), maar oplossingen worden niet onderhouden.
4. Managed	Processen zijn ingericht conform privacyregels, oplossingen worden onderhouden, er is sprake van integraal risicomanagement. Om compliant te zijn met de Wbp is dit het meest logische niveau.
5. Optimized	Privacy is zo vanzelfsprekend dat mensen er zelf mee aan de slag gaan. De organisatie is zich permanent aan het optimaliseren. Lessen uit incidenten worden direct meegenomen in de organisatie. Er is sprake van een zelflerende organisatie. Dit is het hoogst haalbare niveau.

Voor het doorlopen van de startfase kan ook een gap-analyse worden toegepast.

In de tweede fase komt de inhoudelijke beoordeling van de gegevens en processen aan de orde. Hierbij moet inhoudelijk worden geïnventariseerd in hoeverre de organisatie handelt in overeenstemming met de Wbp. Dit betekent dat reeds bestaande gegevens en processen in kaart moeten worden gebracht en inhoudelijk moeten worden gecontroleerd om te onderzoeken of deze 'Wbp-bestendig' zijn. Ook ontbrekende documenten en processen, die verplicht zijn op grond van de Wbp (bijvoorbeeld het melden van een gegevensverwerking bij de AP), worden in kaart gebracht. Daarnaast moet worden geïnventariseerd welke activiteiten er nodig zijn om de privacy ook in de toekomst te kunnen beheersen. Te denken valt aan het opstellen en herzien van privacybeleid, het maken van werkinstructies, et cetera. Welke specifieke processen en documenten binnen de organisatie worden beoordeeld is afhankelijk van het doel dat de corporatie heeft bepaald in de eerste fase.

De laatste fase is de beheerfase. In deze fase wordt de continuïteit van de bescherming van persoonsgegevens gewaarborgd. Dit gebeurt door periodieke controle van bestaande en nieuwe activiteiten op het gebied van gegevensverwerkingen zowel binnen als buiten de corporatie. Er wordt onder meer gecontroleerd of de processen plaatsvinden zoals deze zijn afgesproken in contracten en beleid of dat bestaande werkprocessen eventueel moeten worden bijgesteld. Als er bijvoorbeeld afspraken zijn gemaakt over het melden van datalekken, dan moet periodiek worden onderzocht of het beleid nog goed werkt, zeker als de organisatie tussentijds is veranderd. Ten aanzien van nieuwe en gewijzigde gegevensverwerkingen is het nuttig om de risico's van de verwerkingen te onderzoeken aan de hand van een PIA. Ten slotte moet ook actief worden gecommuniceerd over privacy om de bewustwording en het bewustzijn levend te houden binnen de organisatie.

De implementatie van privacy hoeft overigens niet altijd langs deze drie fases te verlopen. Zo kunnen er al lopende activiteiten zijn op bepaalde deelgebieden (bijvoorbeeld informatiebeveiliging of HR), waardoor het niet nodig is om de eerste fase te doorlopen. Het hoe en waarom is dan immers vaak al bekend. Bovendien kunnen bepaalde activiteiten al in een andere fase zijn doorlopen. Het creëren van awareness kan in sommige organisaties bijvoorbeeld juist een voorwaarde zijn om privacy op de agenda te krijgen. In dat geval vindt communicatie over privacy niet (alleen) plaats in de derde fase, maar al in de eerste fase.

LIJST VAN GERAADPLEEGDE EN AANBEVOLEN LITERATUUR

Autoriteit Consument & Markt, *Veelgestelde vragen over de cookiebepaling*, 14 juli 2015. Online te raadplegen via: https://www.acm.nl/nl/download/publicatie/?id=14496

Autoriteit Persoonsgegevens, *Checklist zwarte lijst*. Online te raadplegen via: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/checklist_zwarte_lijst_0.pdf

Autoriteit Persoonsgegevens, *Handleiding protocol zwarte lijst*. Online te raadplegen via: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/handleiding_protocol_zwarte_lijst.pdf

Autoriteit Persoonsgegevens, *Informatie delen in samenwerkingsverbanden*, februari 2012. Online te raadplegen via: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/031_informatie_delen_in_samenwerkingsverbanden_feb_2012.pdf.

Autoriteit Persoonsgegevens, *Wbp-naslag*. Online te raadplegen via: https://autoriteitpersoonsgegevens.nl/nl/over-privacy/wetten/wbp-naslag

Beleidsregels cameratoezicht, Autoriteit Persoonsgegevens van 2 februari 2016, *Stcrt*. 2016, 4971. Online te raadplegen via: https://autoriteitpersoonsgegevens.nl/nl/nieuws/autoriteit-persoonsgegevens-publiceert-beleidsregels-cameratoezicht

Beleidsregels meldplicht datalekken Wbp, Autoriteit Persoonsgegevens van 8 december 2015, *Stcrt*. 2015, 46128. Online te raadplegen via: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/beleidsregels_meldplicht_datalekken.pdf

Boetebeleidsregels Autoriteit Persoonsgegevens van 15 december 2015, *Stcrt*. 2016, 2043. Online te raadplegen via: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebeleidsregels_autoriteit_persoonsgegevens_staatscourant_2016-2043_0.pdf

CBP-richtsnoeren: beveiliging van persoonsgegevens van 1 maart 2013, *Stcrt*. 2013, 5174. Online te raadplegen via: https://autoriteitpersoonsgegevens.nl/nl/nieuws/cbp-publiceert-richtsnoeren-beveiliging-van-persoonsgegevens

P.C. Knol, G.J. Zwenne, *Tekst & Commentaar Telecommunicatie- en privacyrecht*, Deventer: Kluwer 2015

Koninklijke Nederlandsche Maatschappij ter bevordering der Geneeskunst, *Richtlijnen inzake het omgaan met medische gegevens*, 1 januari 2010. Online te raadplegen via: http://www.knmg.nl/web/file?uuid=22fc4006-11c8-4d00-8086-806e4a016a8c&owner=a8a9ce0e-f42b-47a5-960e-be08025b7b04&contentid=71232

H.R. Kranenborg & L.F.M. Verhey, *Wet bescherming persoonsgegevens in Europees perspectief*, Deventer: Kluwer 2011

Nederlands Genootschap van Functionarissen voor de Gegevensbescherming, *Informatieblad – Relatie FG – CBP*. Online te raadplegen via: http://www.ngfg.nl/download.php?id=13

Nederlandse Orde van Register EDP-Auditors, *Privacy Impact Assessment (PIA). Introductie, handreiking en vragenlijst*, november 2015. Online te raadplegen via: http://www.norea.nl/readfile.aspx?ContentID=82987&ObjectID=1265283&Type=1&File=0000042779_PIA%20versie%201.2%20def.pdf

Richtsnoeren identificatie en verificatie van persoonsgegevens (Gebruik van 'kopietje paspoort' in de private sector), College Bescherming Persoonsgegevens van 12 juli 2012, *Stcrt*. 2012, 14741. Online te raadplegen via: https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/rs/rs_kopie-identiteitsbewijs.pdf

COLOFON

Deze publicatie is een uitgave van Aedes vereniging van woningcorporaties in samenwerking met Privacy Company.

Tekst: Simone Fennell en Anna Maj Drenth (Privacy Company)
Vormgeving: Aedes vereniging van woningcorporaties

vereniging van
woningcorporaties

PRIVACY COMPANY

aedes