Handleiding Algemene verordening gegevensbescherming (AVG) voor bouw & infra

Inhoud

1. Inleiding

Vanaf 25 mei is de Algemene verordening gegevensbescherming (AVG) van toepassing. De voorganger van de AVG, de Europese Privacyrichtlijn (in Nederland geïmplementeerd in de Wet bescherming persoonsgegevens) wordt vervangen door de AVG. Voor alle bedrijven en organisaties betekent dat werk aan de winkel om bedrijfsprocessen 'AVG-proof' te maken. Zo zult u in ieder geval tegen het licht moeten houden waar en waarom u persoonsgegevens in uw bedrijf verwerkt. Ook zult u net als iedere andere organisatie:

- een beleid moeten formuleren, documenteren en onderbouwen voor de verwerking van persoonsgegevens volgens de basisbeginselen van de AVG;
- registers moeten bijhouden van de verwerking van persoonsgegevens;
- een procedure voor datalekken moeten vaststellen;
- betrokkenen moeten informeren en vragen om toestemming;
- afspraken moeten maken met opdrachtgevers, leveranciers en onderaannemers over (de medeverantwoordelijkheid voor) gegevensverwerking en privacy.

Afhankelijk van de omvang van de verwerking van persoonsgegevens en de bijbehorende risico's zult u ook:

- een gegevenseffectbeoordeling moeten uitvoeren;
- een functionaris gegevensbescherming (FG) moeten aanstellen.

Deze handleiding is gericht op bouw- en infrabedrijven en geeft op hoofdlijnen informatie over de verplichtingen van de AVG en hoe u daar in de praktijk invulling aan kunt geven. Een gedetailleerde uitwerking van de verschillende onderdelen van de AVG vindt u op www.bouwendnederland.nl/avg of https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving.

2. Het waarom en wat van de AVG

De AVG is er om twee belangen te waarborgen:

- De bescherming van natuurlijke personen in verband met de verwerking van hun gegevens.
- Vrij verkeer van persoonsgegevens binnen de Europese Unie (EU).

Door digitalisering is het steeds makkelijker om informatie te verzamelen, bewaren, combineren en delen. Dat geldt ook voor privacygevoelige zaken, zoals persoonsgegevens. De risico's op misbruik van deze gegevens, bijvoorbeeld in de vorm van identiteitsfraude, nemen daardoor toe. De bedoeling van de AVG is ervoor te zorgen dat bedrijven en organisaties met dergelijke gegevens zorgvuldig omgaan, mede om misbruik te voorkomen.

De AVG regelt de rechtmatige en zorgvuldige omgang van persoonsgegevens binnen de EU. Ze omschrijft welke rechten en plichten gelden voor natuurlijke personen en de organisaties die hun persoonsgegevens verwerken. De AVG geldt voor de gehele EU en soms ook daarbuiten. Daarnaast zijn er nationale uitvoeringswetten voor de onderwerpen waarover de Europese lidstaten in de AVG hebben afgesproken dat zij hier op nationaal niveau regels voor mogen afspreken. In Nederland is dat de Uitvoeringswet AVG. De Uitvoeringswet AVG regelt onder andere:

- de rol, positie en bevoegdheden van de Autoriteit Persoonsgegevens (AP), de Nederlandse nationale toezichthouder;
- uitzonderingen op het verbod voor het gebruik van bijzondere categorieën persoonsgegevens;
- regelingen voor (uitzonderingen) op rechten van betrokkenen;
- regelingen voor specifieke verwerkingssituaties;
- het verbod op de verwerking van een burgerservicenummer (BSN), tenzij dit specifiek is geregeld in een wet.

3. Overzicht belangrijkste onderdelen AVG

De AVG is de Europese opvolger van de Nederlandse Wet bescherming persoonsgegevens. De belangrijkste onderdelen zijn:

- De privacyverklaring wordt transparanter en is uitgelegd in een wetsartikel.
- Alle datalekken moeten gedocumenteerd worden.
- Alle verwerkingen van persoonlijke gegevens moeten gedocumenteerd worden.
- Met leveranciers moeten afspraken over de omgang met persoonsgegevens gemaakt worden.
- Boetes worden hoger.
- Organisaties hebben mogelijk een functionaris gegevensbescherming nodig.
- Als er risico's aan de verwerking van persoonsgegevens kleven, is een gegevensbeschermingseffectbeoordeling of *data protection impact assessment* (DPIA) of *privacy impact assessment* (PIA) nodig. (NB DPIA en PIA is hetzelfde, beide termen komen voor.)
- Organisaties hebben de plicht zo min mogelijk privacygevoelige informatie te verzamelen.
- Software (en -diensten) moeten rekening houden met privacy.
- De beveiliging moet op orde zijn.
- Van de organisatie wordt een privacybeleid verwacht.
- Betrokkenen, de personen om wie het gaat, hebben inzagerecht.
- Bij online diensten hebben betrokkenen het recht hun informatie te downloaden en te exporteren.
- Als uw organisatie interesseprofielen maakt, moet u kunnen uitleggen hoe u dit doet en wat daarmee gebeurt.
- Maakt uw organisatie gebruik van biometrie, dan moet u deze gegevens beter beschermen, omdat dit valt in de categorie 'bijzondere persoonsgegevens'.

4. Grondbeginselen

De AVG gaat uit van zeven beginselen, waaraan elke verwerking van persoonsgegevens moet voldoen. Ze zijn vastgelegd in artikel 5 van de AVG. Deze beginselen zijn:

1. Rechtmatig, behoorlijk en transparant

2. Gebonden aan specifieke verzameldoelen (doelbinding)
3. Toereikend, ter zake dienend en beperkt tot het noodzakelijke (minimale gegevensverwerking)
4. Juistheid
5. Niet langer bewaren dan nodig (opslagbeperking)
6. Goed beveiligd en vertrouwelijk blijven
7. Verantwoordingsplicht

Rechtmatigheid, transparantie en doelbinding

Zomaar allerlei persoonsgegevens verzamelen en opslaan omdat dat 'handig kan zijn', is niet toegestaan. De AVG geeft aan dat er zes redenen kunnen zijn om persoonsgegevens te verwerken, de zogenaamde grondslagen. In de volgende paragraaf leest u hier meer over. Een organisatie moet in haar beleid documenteren en onderbouwen volgens welke van deze zes grondslagen het rechtmatig is om bepaalde persoonsgegevens te verwerken.

U moet alle betrokkenen informeren – transparant zijn – over de verwerking van hun persoonsgegevens. Dit doet u bijvoorbeeld in een privacyverklaring. Hierin staan ook de gebruikte grondslagen benoemd.

Voordat u begint persoonsgegevens te verzamelen, bepaalt u het gebruiksdoel. Vervolgens gebruikt u de persoonsgegevens niet (ook niet later) voor een ander gebruiksdoel. Het doel van de verwerking moet u duidelijk omschrijven in uw privacyverklaring, in voor iedereen begrijpelijke taal. Bijvoorbeeld: een bankrekeningnummer is nodig om het salaris te kunnen overmaken.

Toereikend, ter zake dienend een beperkt tot het noodzakelijke

Zorgt u ervoor dat u in de praktijk alleen persoonsgegevens verwerkt die nodig zijn voor het vooraf vastgestelde doel. Ook maakt u in uw beleid en privacyverklaring duidelijk dat u de persoonsgegevens verwerkt die nodig zijn om het vastgestelde doel te realiseren. Minder hoeft niet, meer mag niet! Dat wordt minimale gegevensverwerking of dataminimalisatie genoemd. Als u het genoemde doel op een andere, minder ingrijpende wijze kunt bereiken, bijvoorbeeld door geen of (veel) minder persoonsgegevens te verwerken, dan moet u daarvoor kiezen.

Juistheid

U moet ervoor zorgen dat de persoonsgegevens die u verwerkt, juist zijn.

Niet langer bewaren dan nodig

U mag gegevens niet langer bewaren dan nodig voor het vastgestelde doel. Soms heeft u op grond van andere wetgeving een langere verplichting om gegevens te bewaren. Dan dient u na te gaan welke gegevens u nodig heeft om aan beide verplichtingen te voldoen. Kunt u bijvoorbeeld voldoen aan een langere verplichte bewaartermijn zonder persoonsgegevens te gebruiken? Dan verwijdert u de persoonsgegevens. Na afloop van de bewaartermijn volgens de AVG moet u de gegevens vernietigen of verwijderen. De wettelijke bewaartermijnen voor bijvoorbeeld een personeelsdossier na het einde van een dienstverband veranderen niet met de komst van de AVG.

Goed beveiligd en vertrouwelijk

U moet ervoor zorgen dat u de persoonsgegevens goed beveiligt en vertrouwelijk behandelt. Dit betekent technische maatregelen, maar ook organisatorische maatregelen. U kunt daarbij denken aan beveiliging van ICT, maar ook aan afspraken over goed afsluitbare dossierkasten en bedrijfspanden. Liggen er geen persoonsgegevens onbeheerd op bureaus? Als medewerkers uit dienst gaan, zie er dan op toe dat u ook hun toegangscodes blokkeert.

Verantwoordingsplicht

U moet kunnen aantonen dat u de beginselen van de AVG naleeft. In de praktijk betekent dit dat u er goed aan doet om maatregelen en afspraken vast te leggen in beleid, protocollen, overeenkomsten en handboeken. Daarnaast zult u een privacy management control framework moeten invoeren om ervoor te zorgen dat de maatregelen en afspraken ook daadwerkelijk worden uitgevoerd en nageleefd.

5. Grondslagen van de AVG

De grondslagen van de AVG zijn de redenen waarom u persoonsgegevens verwerkt of zou mogen of moeten verwerken. Deze grondslagen zijn:

1. De betrokkene heeft toestemming gegeven om zijn persoonsgegevens te verwerken voor een of meer specifieke doeleinden.
2. De verwerking is noodzakelijk om een overeenkomst uit te voeren waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen.
3. De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust.
4. De verwerking is noodzakelijk om de vitale belangen van de betrokkene of een andere natuurlijke persoon te beschermen.
5. De verwerking is noodzakelijk om een taak van algemeen belang te vervullen, of een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen.
6. De verwerking is noodzakelijk om de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of een derde te behartigen, behalve wanneer de belangen of de grondrechten en fundamentele vrijheden van de betrokkene die tot de bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.

Bouw- en infrabedrijven zullen vooral te maken hebben met grondslagen 1 , 2 en 3. In uw beleid geeft u aan op grond waarvan u bepaalde persoonsgegevens verwerkt.

Betrokkene heeft toestemming gegeven

Een concreet voorbeeld van deze grondslag is een medewerker die toestemming geeft om zijn of haar persoonsgegevens door te sturen naar de loonverwerker. Zonder NAW-gegevens en een bankrekeningnummer kunt u immers geen salaris overmaken! Een concreet voorbeeld is het gebruiken van persoonsgegevens voor een bepaald doel, terwijl u de persoonsgegevens toch voor een andere doel wilt gebruiken. Dit gebeurt vaak bij marketingactiviteiten.

De AVG brengt overigens met zich mee dat u bij betrokkenen altijd moet informeren of om toestemming moet vragen om persoonsgegevens te mogen verwerken, ook als er sprake is van een andere grondslag. Alleen speelt bij het vragen van toestemming de informatieverstrekking een grotere rol. Toestemming moet namelijk ‘geïnformeerde, in vrijheid gegeven en specifieke’ toestemming zijn. In het hoofdstuk ‘Rechten van betrokkenen’ is dit verder uitgewerkt.

Noodzakelijk om een overeenkomst uit te voeren

In de bouw en infra zijn er veel ketenpartijen die samenwerken en persoonsgegevens uitwisselen. Dat kan gaan om bewonersgegevens van te renoveren woningen, maar ook om gegevens van medewerkers van onderaannemers. Die gegevens zijn nodig om het afgesproken werk te kunnen

doen en de personeelsadministratie van het werk te kunnen uitvoeren. Dat maakt dat er een grondslag is om die persoonsgegevens te verwerken.

Noodzakelijk om te voldoen aan een wettelijke verplichting

Een concreet voorbeeld van zo'n wettelijke verplichting is het bewaren van een kopie van een geldig identiteitsbewijs van een werknemer in het personeelsdossier. Ook voor de uitvoering van sociale verzekeringswetten en fiscale wetten is de verwerking van een aantal persoonsgegevens verplicht. U informeert de betrokkene dat u de persoonsgegevens verwerkt en hoe u dit doet.

6. Stappenplan AVG

Organisaties moeten actie ondernemen om klaar te zijn voor de AVG. Afhankelijk van de grootte van uw organisatie en de aard en omvang van de verwerking van persoonsgegevens, kunt u diverse maatregelen nemen. In onderstaand stappenplan leest u de tien belangrijkste stappen.

Stap 1: Bewustwording

Zorg ervoor dat de relevante mensen in uw organisatie op de hoogte zijn van de nieuwe privacyregels. Bijvoorbeeld uw hr-manager of administrateur. Zij moeten inschatten welke impact de AVG heeft op uw huidige processen, diensten en goederen en welke aanpassingen nodig zijn om aan de AVG te voldoen. Houd er rekening mee dat de implementatie van de AVG tijd kost en begin er daarom op tijd mee.

Stap 2: Rechten van betrokkenen

Onder de AVG krijgen de mensen van wie u persoonsgegevens verwerkt meer en verbeterde privacyrechten. De AVG gaat om de bescherming van betrokkenen. Daar horen ook rechten van betrokkenen bij. Om te zorgen dat het daadwerkelijk rechten zijn, heeft u ook de verplichting om te zorgen dat de betrokkenen hun privacyrechten goed kunnen uitoefenen. Denk daarbij aan bestaande rechten, zoals het recht op inzage (welke gegevens heeft u van hen?) en het recht op correctie en verwijdering.

Houd ook alvast rekening met nieuwe rechten, zoals het recht op dataportabiliteit. Dit betekent dat u ervoor moet zorgen dat betrokkenen hun gegevens makkelijk kunnen krijgen en vervolgens kunnen doorgeven aan een andere organisatie, als ze dat willen. Om dit te faciliteren maken veel bedrijven omgevingen – portalen – waarin betrokkenen zelf hun gegevens kunnen inzien, wijzigen of downloaden.

Stap 3: Overzicht van verwerkingen

Breng uw gegevensverwerkingen in kaart. Voor welke processen gebruikt uw organisatie persoonsgegevens? Bijvoorbeeld voor de salarisadministratie. Documenteer welke persoonsgegevens u verwerkt en met welk doel u dit doet, waar deze gegevens vandaan komen en met wie u ze deelt.

Onder de AVG heeft u een verantwoordingsplicht, wat inhoudt dat u moet kunnen aantonen dat uw organisatie in overeenstemming met de AVG handelt. Het bijhouden van een register van verwerkingsactiviteiten (verwerkingsregister) is onderdeel van de verantwoordingsplicht. U kunt het verwerkingsregister ook gebruiken bij andere verplichtingen. Als betrokkenen hun privacyrechten uitoefenen, moet u ook de partijen informeren waarmee u de gegevens heeft gedeeld. In het verwerkingsregister ziet u in een oogopslag welke partijen dit zijn.

Stap 4: Data protection impact assessment

Onder de AVG kunt u verplicht zijn een zogeheten data protection impact assessment (DPIA) uit te voeren. Andere termen die hiervoor gebruikt worden zijn gegevensbeschermingseffectbeoordeling of privacy impact assessment (PIA). Met dit instrument brengt u vooraf de privacyrisico's van de verwerking van persoonsgegevens in kaart. Vervolgens kunt u maatregelen nemen om de risico's te verkleinen. U moet een DPIA uitvoeren als:

- uw beoogde gegevensverwerking waarschijnlijk een hoog privacyrisico met zich meebrengt;
- er sprake is van een systematische en uitvoerige beoordeling van persoonlijke aspecten van personen (profilering);
- er op grote schaal bijzondere persoonsgegevens worden verwerkt;
- er op grote schaal en systematisch mensen worden gemonitord in een publiek toegankelijk gebied, bijvoorbeeld met cameratoezicht.

U kunt nu alvast inschatten of u straks DPIA's moet uitvoeren en hoe u dit dan gaat aanpakken. Het kan bijvoorbeeld zijn dat u zo'n analyse moet uitvoeren, omdat uw bedrijf de gegevens van huurders van een woningcorporatie beheert.

Komt uit een DPIA naar voren dat uw beoogde verwerking een hoog risico oplevert? En lukt het u niet om maatregelen te nemen om dit risico te beperken? Dan moet u met de Autoriteit Persoonsgegevens overleggen voordat u met de verwerking start. Dit wordt een voorafgaande raadpleging genoemd. De AP beoordeelt dan of de voorgenomen verwerking in strijd is met de AVG. Is dit het geval, dan ontvangt u een schriftelijk advies van de AP.

Stap 5: Privacy by design *en* privacy by default

Maak uw organisatie nu al vertrouwd met de onder de AVG verplichte uitgangspunten van privacy by design en privacy by default, en ga na hoe u deze beginselen binnen uw organisatie kunt invoeren.

Privacy by design houdt in dat u al bij het ontwerpen van producten en diensten ervoor zorgt dat u persoonsgegevens goed beschermt. Maar bijvoorbeeld ook dat u niet meer gegevens verzamelt dan noodzakelijk is voor het doel van de verwerking. En dat u de gegevens niet langer bewaart dan nodig. Privacy by default houdt in dat u technische en organisatorische maatregelen moet nemen om ervoor te zorgen dat u – standaard – alléén persoonsgegevens verwerkt die noodzakelijk zijn voor het specifieke doel dat u wilt bereiken.

Stap 6: Functionaris gegevensbescherming

Onder de AVG kunnen organisaties verplicht zijn om een functionaris gegevensbescherming (FG) aan te stellen. Dit geldt in ieder geval voor:

- overheden en publieke organisaties;
- organisaties die vanuit hun kernactiviteiten op grote schaal individuen volgen;
- organisaties die op grote schaal bijzondere persoonsgegevens verwerken en dit als kernactiviteit doen.

Bepaal nu alvast of dit voor uw organisatie geldt. Zo ja, wacht dan niet te lang om een FG te werven. Uiteraard mag uw organisatie ook vrijwillig een FG aanstellen.

De meeste bouw- en infrabedrijven vallen niet onder de AVG-verplichting om een FG aan te stellen. Toch is het verstandig om een of meer personen in uw organisatie aan te wijzen die verantwoordelijk is of zijn voor de bescherming van persoonsgegevens en deze ook de nodige bevoegdheden te geven om daar passende maatregelen voor te nemen.

Stap 7: Meldplicht datalekken

De meldplicht voor datalekken blijft onder de AVG grotendeels hetzelfde. Over de meldplicht datalekken vindt u hier meer informatie: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken.

De AVG stelt wel strengere eisen aan uw eigen registratie van de datalekken die zich in uw organisatie hebben voorgedaan. U moet alle datalekken documenteren. Met deze documentatie moet de AP kunnen controleren of u aan de meldplicht heeft voldaan.

Stap 8: Verwerkersovereenkomsten

Heeft u uw gegevensverwerking uitbesteed, bijvoorbeeld aan een salarisverwerker? Ga dan na of de overeengekomen maatregelen in bestaande contracten met uw verwerker(s) nog steeds toereikend zijn. En of deze voldoen aan de eisen die de AVG aan verwerkersovereenkomsten stelt. Zo niet, breng dan tijdig noodzakelijke wijzigingen aan.

Stap 9: Leidende toezichthouder

Heeft uw organisatie vestigingen in meerdere EU-lidstaten? Of hebben uw gegevensverwerkingen in meerdere lidstaten impact? Dan hoeft u onder de AVG nog maar met één privacytoezichthouder zaken te doen. Deze wordt de leidende toezichthouder genoemd. Geldt dit voor uw organisatie, bepaal dan onder welke privacytoezichthouder u valt.

Stap 10: Toestemming

Voor sommige gegevensverwerkingen heeft u toestemming van de betrokkenen nodig. De AVG stelt strengere eisen aan toestemming. Evalueer daarom de manier waarop u toestemming vraagt, krijgt en registreert. Pas deze wijze zo nodig aan.

7. AVG binnen uw organisatie

Persoonsgegevens verwerken is in de AVG een breed begrip: het gaat om het verzamelen, opvragen, opslaan, veranderen, gebruiken, raadplegen, doorsturen en verwijderen ervan. Voorbeelden van persoonsgegevens die bij bouw- en infrabedrijven verwerkt worden, zijn:

- van medewerkers: naam, adres, woonplaats, burgerservicenummer (BSN), geboortedatum, nationaliteit, burgerlijke staat, e-mailadres, telefoonnummers, bankrekeningnummer, kopie van het ID-bewijs, diploma's en certificaten, verblijfs- of werkvergunning, functie, salaris, pensioen, ziek- en hersteldmeldingen, loonbeslagen, gegevens van partners/gezins-/familieleden;
- van medewerkers van onderaannemers: naam, adres, woonplaats, BSN, nationaliteit, verblijfs- of werkvergunning, telefoonnummers;
- van relaties: naam, adres, woonplaats, e-mailadres, telefoonnummers, bankrekening, uittreksel Kamer van Koophandel, g-rekeningovereenkomst, Verklaring betalingsgedrag, loonheffingennummer, mandagenregisters.

Zelfs het inzien van dergelijke gegevens is volgens de AVG al een verwerking van persoonsgegevens. In de praktijk komt het er dus op neer dat het verwerken van deze gegevens als snel onder de AVG valt.

Toch valt niet alle informatie die u over personen verzamelt onder de AVG. Het moet wel gaan om de verwerking voor zakelijke doeleinden en om:

- gegevens die geautomatiseerd worden verwerkt;
- gegevens die opgenomen worden in een bestand.

Voorbeeld: een visitekaartje dat u bewaart in uw agenda, valt hier niet onder. Wel een visitekaartje waarvan u de gegevens verwerkt in een CRM-database (*costumer relationship management*).

Verwerkingsverantwoordelijke vaststellen

Degene die bepaalt welke persoonsgegevens worden verzameld, voor welk doel dit gebeurt, de manier waarop dit plaatsvindt en met welke middelen, is de verwerkingsverantwoordelijke. De verwerkingsverantwoordelijke is altijd de organisatie, niet de persoon die in een organisatie werkt.

De verwerker

De verwerker is degene of organisatie die volgens instructies van een verwerkingsverantwoordelijke bepaalde taken uitvoert. Ook helpt de verwerker de verwerkingsverantwoordelijke bij de uitvoering van plichten, zoals het invullen van rechten van betrokkenen, gegevensbescherming of het melden van datalekken. In de verwerkersovereenkomst leggen de verwerkingsverantwoordelijke en verwerker de afspraken vast over de manier waarop persoonsgegevens worden verwerkt. De afgesproken taken mogen aan een derde partij worden overgedragen (ook weer vastgelegd in een verwerkersovereenkomst), mits de verwerkingsverantwoordelijke daarvoor vooraf schriftelijke toestemming heeft gegeven. Verwerkers hebben ook een registerplicht om bij te houden wat ze aan persoonsgegevens verwerken.

Gegevensbeschermingsbeleid opstellen

Uw organisatie is verplicht een gegevensbeschermingsbeleid op te stellen. Afhankelijk van de omvang van de verwerking en de risico's die eraan hangen, moeten de volgende zaken daarin worden benoemd:

- de technische en organisatorische maatregelen die zijn genomen om te voldoen aan de AVG;
- de vorm die deze maatregelen – processen, werkafspraken, beveiligingsmaatregelen et cetera – hebben;
- de gegevenseffectbeoordeling;
- bij wat voor soort datalekken u een melding doet bij de AP;
- de vastgelegde rollen en verantwoordelijkheden van:
    - de functionaris gegevensbescherming,
    - de verwerkingsverantwoordelijke,
    - de verwerker(s).

Registerplicht

Het register is een opsomming van de verwerkingen van persoonsgegevens die bij uw organisatie worden uitgevoerd. Het register zelf bevat geen persoonsgegevens, alleen een beschrijving van de verwerkingsactiviteiten. In het register neemt u de volgende gegevens op:

- uw naam en contactgegevens, of indien van toepassing die van uw vertegenwoordiger;
- de contactgegevens van uw FG als u die heeft aangesteld;
- de verwerkingsdoeleinden;
- een beschrijving van de categorieën van betrokkenen en de categorieën van persoonsgegevens;
- de categorieën van ontvangers aan wie de persoonsgegevens zijn of worden verstrekt, onder meer ontvangers gevestigd buiten de EER (Europese Economische Ruimte) of internationale organisaties;

- indien mogelijk de beoogde termijnen waarbinnen de verschillende categorieën van gegevens moeten worden gewist;
- indien mogelijk een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

Wanneer de Autoriteit Persoonsgegevens daarom vraagt, moet u haar het register ter beschikking stellen. Ook dient de FG toegang tot het register te krijgen.

Privacy bij ontwerp en standaardinstelling

Privacy en gegevensbescherming moeten verplicht meegenomen worden bij de ontwikkeling van nieuw beleid of nieuwe systemen. Daarbij moet u rekening houden met de stand van de techniek, de uitvoeringskosten en de risico's voor de betrokkenen.

Voorbeelden van ontwerpstrategieën zijn:

- dataminimalisatie: beperk de verwerking van gegevens en verwijder deze zodra dit kan;
- persoonsgegevens scheiden (bijvoorbeeld het formulier vastlegging persoonsgegevens Wet ketenaansprakelijkheid: in stukken is dit niet meer interessant voor kwaadwillenden)
- gegevens abstraheren;
- gegevens beschermen of onherleidbaar maken.

Rechten van betrokkenen

Betrokkenen hebben het recht om te weten wat er met hun persoonsgegevens gebeurt en waarom. Ook moeten zij bewust worden gemaakt van de risico's van de gegevensverwerking, de regels die ervoor gelden, de waarborgen en de manier waarop zij hun rechten over de verwerking van gegevens kunnen uitoefenen.

Wanneer u rechtsreeks bij de betrokkene gegevens verzamelt, moet u diegene tijdens de verzameling informeren over bijvoorbeeld:

- uw identiteit en uw contactgegevens of de contactgegevens van uw vertegenwoordiger;
- de contactgegevens van de FG;
- de doelen waarvoor u persoonsgegevens verwerkt;
- de grondslag waarop u de verwerking baseert (de overeenkomst onderaanneming/inlening op grond waarvan de betrokkene verplicht is de gegevens te verstrekken);
- de eventuele ontvangers of categorieën ontvangers van de gegevens (bijvoorbeeld de hoofdaannemer);
- de passende waarborgen voor bescherming, welke dit zijn en of de betrokkene hiervan een kopie kan krijgen, of waar deze de waarborgen kan raadplegen (bijvoorbeeld een website);
- de bewaartermijn of als dat niet mogelijk is de criteria voor het bepalen ervan;
- de rechten van de betrokkene;
- in het geval van toestemming, het feit dat de betrokkene die toestemming altijd weer kan intrekken;
- het recht van de betrokkene om een klacht in te dienen over uw verwerking bij de AP.

Als u de gegevens niet rechtstreeks van betrokkene heeft gekregen maar via een derde, dan vult u bovenstaande gegevens aan met de informatie over de derde partij.

Betrokkenen hebben volgens de AVG de volgende rechten:

- het recht op inzage en eventueel het recht op afgifte van een kopie van de gegevens die bewaard worden;
- het recht op rectificatie;
- het recht op informatie over de wijziging van de gegevens;
- het recht op verwijdering en het recht om vergeten te worden (geen absoluut recht, er moet een gerechtvaardigd belang zijn);
- het recht op beperking, bijvoorbeeld bij een vermoeden dat de gegevensverwerking onrechtmatig is;
- het recht van verzet;
- het recht op overdraagbaarheid van de gegevens;
- het recht om niet onderworpen te worden aan geautomatiseerde individuele besluitvorming, zoals profilering (bijvoorbeeld de opzegging van een arbeidsovereenkomst, omdat uit de geautomatiseerd verzamelde gegevens blijkt dat de werknemer een risico vormt).

Wanneer betrokkene niet informeren

U hoeft de betrokkene niet te informeren als hij of zij al over de informatie beschikt. Bijvoorbeeld een werknemer van een onderaannemer die al vaker op de bouwplaats is geweest en al eerder is geïnformeerd.

U hoeft betrokkene ook niet te informeren als dit een onevenredige inspanning zou vergen. De informatie moet dan wel openbaar gemaakt zijn en in uw beleid moet zijn opgenomen wat de redenen zijn waarom de inspanning onevenredig is om de betrokkene rechtstreeks te informeren.

Meldplicht datalek

In beginsel moet u ieder datalek aan de AP melden. Alleen de datalekken waarbij het onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen, zijn uitgezonderd van de meldplicht. U moet afwegen of dit in een bepaalde situatie van toepassing is.

Is er sprake van een datalek, dan moet er direct (binnen 72 uur, weekenden tellen mee!) melding gedaan worden bij de Autoriteit Persoonsgegevens. Binnen uw organisatie moet er een procedure of protocol voor datalekken zijn. Het kan zijn dat uit afweging volgt om een datalek niet te melden, maar dat de AP er toch achter komt. In dat geval moet u alsnog aan de hand van de afweging en de procedure of het protocol aannemelijk maken dat er geen reden was om het lek te melden.

Voorbeelden van datalekken:

- Gegevens zijn bij een ‘onbevoegd’ persoon terechtgekomen (bijvoorbeeld door een digitale factuur of er is per ongeluk een bestand verzonden aan de verkeerde persoon).
- De kast met de mandagenstaten en de administratie van Wka-personen, die op een plek staat waar verschillende (onbevoegde) personen (kunnen) komen, heeft niet op slot gestaan (een menselijke fout).
- Een map met persoonsgegevens is verloren gegaan (bijvoorbeeld door auto-inbraak, doordat deze in de trein is blijven liggen of in een normale papierbak gegooid in plaats van naar archiefvernietiging gebracht).
- Een USB-stick of laptop waar gegevens op staan, is verloren, gestolen of niet goed beveiligd (denk aan automatisch opgeslagen wachtwoorden om een systeem in te kunnen).

Afspraken over persoonsgegevens met opdrachtgevers, leveranciers en onderaannemers

In de bouw en infra is vaak sprake van vele partijen die samenwerken op een project te realiseren. Daar hoort de uitwisseling van (grote hoeveelheden) persoonsgegevens bij. Het kan gaan om medewerkers-, maar ook om bewonersgegevens. In de relatie tussen opdrachtgever, aannemer, onderaannemer, uitlener en leveranciers moeten zij schriftelijke afspraken maken over:

- wie verwerkingsverantwoordelijk is;
- wie mogelijk gezamenlijk verwerkingsverantwoordelijken zijn;
- wie verwerker is;
- vorm en inhoud van verwerkersovereenkomsten, met aandacht voor ICT en beveiliging;
- het informeren van betrokkenen;
- privacyafspraken in algemene voorwaarden.

Op http://www.bouwendnederland.nl/modelcontracten/5279450/handreiking-persoonsgegevens vindt u modellen om hieraan invulling te kunnen geven.

8. Bijzondere categorieën persoonsgegevens

Bijzondere categorieën zijn persoonsgegevens die gezien hun aard extra gevoelig zijn, bijvoorbeeld:

- gegevens over ras of etnische afkomst;
- iemands politieke opvattingen;
- iemands religieuze of levensbeschouwelijke overtuigingen;
- het lidmaatschap van een vakbond;
- gegevens over gezondheid;
- gegevens over seksueel gedrag of gerichtheid;
- genetische gegevens;
- biometrische gegevens met het oog op de unieke identificatie van een persoon;
- gegevens over strafrechtelijke veroordelingen en strafbare feiten.

Verwerking is verboden, tenzij onder meer:

- er uitdrukkelijke toestemming van de betrokkene is;
- dit noodzakelijk is vanwege de uitvoering van regels op het gebied van het arbeids- en sociale zekerheidsrecht;
- de betrokkene deze gegevens kennelijk zelf al openbaar heeft gemaakt.

Bouw- en infrabedrijven krijgen naar verwachting vooral te maken met de bijzondere categorie ‘het lidmaatschap van een vakbond’, omdat de cao voor dit lidmaatschap een vergoeding van € 50,00 netto toekent. De medewerker die voor dit bedrag in aanmerking wil komen, maakt zelf bij de werkgever kenbaar dat hij lid is van de vakbond. U mag deze informatie niet gebruiken om in uw personeelsbestand de vakbondsleden te selecteren.

9. AVG en andere wet- en regelgeving

Wet ketenaansprakelijkheid

Bij de Wet ketenaansprakelijkheid gaat het, kort samengevat, erom dat u kunt aantonen dat u eventueel verschuldigde loonheffingen aan een aannemer of onderaannemer heeft betaald. Daarom willen hoofdaannemers of inleners kunnen aantonen welke werknemers hebben gewerkt, op welk

project en wanneer. Om aansprakelijkheid voor loonheffingen te kunnen matigen, houdt u een administratie bij van werknemers van onderaannemers en uitleners met de volgende gegevens:

- naam, adres- en woonplaats;
- geboortedatum;
- BSN;
- nationaliteit;
- soort identiteitsbewijs, het nummer en de geldigheidsduur (geen kopie van het document!);
- specificatie van de uren;
- indien van toepassing, een kopie van de A1-verklaring;
- naam, adres en woonplaats van de uitlener en het inschrijvingsnummer van de uitlener bij de Kamer van Koophandel.

Het is niet toegestaan om kopieën van ID-bewijzen van medewerkers van onderaannemers en uitleners te maken en te verzamelen. Dat mag alleen bij arbeidskrachten van buiten de EER in het kader van de Wet arbeid vreemdelingen.

Per 1 januari 2017 is de Uitvoeringsregeling verplicht gebruik BSN gewijzigd. Hierin is nu specifiek opgenomen dat de uitlener of onderaannemer het burgerservicenummer van de op het werk ingezette werknemers verstrekt aan de inlener of aannemer. Met deze wijziging is voorzien in een juridische basis, die de AVG en de UAVG eisen om het BSN te mogen verzamelen, verstrekken en verwerken. Deze BSN-verstrekking is nodig om een beroep te kunnen doen op de vrijwaring voor of matiging van de inleners- en ketenaansprakelijkheid. De wijziging zorgt er ook voor dat de inlener of aannemer het BSN niet zelf bij de werknemers hoeft op te vragen, maar dit op een efficiëntere manier bij de uitlener of onderaannemer kan doen, waarbij het risico op fouten geringer is.

Huurt u een onderaannemer in, dan:

- mag u geen kopie van het ID-bewijs van de werknemers van een onderaannemer vragen of maken;
- mag u wel van de onderaannemer vragen of hij het BSN op de mandagenstaten wil vermelden (wijziging Uitvoeringsregeling verplicht gebruik BSN per 1 januari 2017), op voorwaarde dat de wijze waarop hij met de mandagenstaten omgaat, voldoet aan de Richtsnoeren beveiliging van persoonsgegevens;
- mag u wel de identiteit controleren van de werknemers van de onderaannemer die bij u op de bouwplaats werken;
- mag u wel de persoonsgegevens van de werknemers van de onderaannemer overschrijven.

Bent u onderaannemer, dan:

- mag u geen kopie van het ID-bewijs of andere persoonsgegevens van uw eigen werknemers verstrekken aan uw opdrachtgever;
- mag u wel het BSN noteren op de mandagenstaten (wijziging Uitvoeringsregeling verplicht gebruik BSN per 1 januari 2017) op voorwaarde dat de wijze waarop u met de mandagenstaten omgaat, voldoet aan de Richtsnoeren beveiliging van persoonsgegevens;
- mag u wel tegen uw werknemers zeggen dat zij zich moeten kunnen identificeren op de bouwplaats waar zij werken en dat de opdrachtgever gegevens mag overnemen van hun ID-bewijs.

Meer weten over de Wet ketenaansprakelijkheid? U vindt een uitgebreide handleiding op http://www.bouwendnederland.nl/download.php?itemID=32448.

Personeelsdossier

Als werkgever bent u verplicht om een personeelsdossier bij te houden om te kunnen voldoen aan fiscale en sociale wetgeving. Het advies is om de persoonsgegevens die u over uw werknemers verzamelt, te inventariseren én de afweging te maken wat de grondslag is om deze gegevens te verzamelen. Zo bent u verplicht om een kopie van een geldig identiteitsbewijs in het personeelsdossier op te nemen. Informatie over bijvoorbeeld iemands vrijetijdsbesteding of de aanwezigheid van kinderen bij het sinterklaasfeest van het bedrijf kunt u beter verwijderen.

In het algemeen bevat een personeelsdossier gegevens en documenten uit de volgende hoofdgroepen:

- persoonlijke gegevens
- contracten & arbeidsvoorwaarden
- functioneren & ontwikkeling
- ziekteverzuim

Persoonlijke gegevens

- NAW-gegevens
- kopie van een geldig identiteitsbewijs
- BSN
- sollicitatiebrief en het cv van de werknemer
- opgave van gegevens voor de loonheffing (voorheen: kopie loonbelastingverklaring)
- kopieën van diploma's
- getuigschriften
- verklaring omtrent gedrag (indien van toepassing)
- werkvergunning of verblijfsvergunning (voor buitenlandse werknemers)

Contracten & arbeidsvoorwaarden

- kopie aanstellingsbrief
- arbeidsovereenkomst
- eventuele aanvullingen of wijzigingen in de arbeidsovereenkomst
- geheimhoudingsverklaring (i.v.t.)
- documentatie over pensioenregeling (i.v.t.)
- onkostenvergoedingen (i.v.t.)
- bonus- en of targetregelingen (i.v.t.)
- documentatie over bedrijfsmiddelen, zoals een leaseauto, laptop, gsm, kleding, persoonlijke beschermingsmiddelen
- eventueel zwangerschaps-, ouderschaps- of zorgverlof, bijzonder verlof (i.v.t.)

Functioneren & ontwikkeling

- functieomschrijving
- salarisschaalindeling
- verslagen van beoordelings- en/of functioneringsgesprekken
- persoonlijk ontwikkelingsplan (POP)
- afspraken over loopbaan: actieplan, POP en targets
- gevolgde cursussen en opleidingen (inclusief kopieën van diploma's en certificaten)

- overzicht van de loopbaan: toegekende promoties et cetera

Ziekteverzuim

- verzuimfrequentie
- eventueel informatie over de functionele beperkingen van de werknemer en de noodzakelijke aanpassingen op de werkplek

U mag géén medische gegevens opnemen in het personeelsdossier, ook niet het re-integratiedossier. Medische gegevens zijn uitsluitend toegankelijk voor de betrokkene en de bedrijfsarts.

Medezeggenschap

De AVG gaat niet in op de rol van de ondernemingsraad (or) of personeelsvertegenwoordiging. Op grond van de Wet op de ondernemingsraden (WOR) moet een werkgever aan de or instemming vragen voor een regeling voor voorzieningen die gericht zijn op, of geschikt zijn voor, de waarneming van of controle op de aanwezigheid van gedrag of prestaties van de in de onderneming werkzame personen.

Dit instemmingsrecht heeft met name betrekking op het aanleggen van een persoonsregistratie en op de door de werkgever opgestelde regelingen over het verzamelen, bewaren, gebruiken en beveiligen van deze persoonsgegevens. Ook een regeling voor bijvoorbeeld cameratoezicht, personeelsvolgsystemen of tijdsregistratiesystemen valt onder het instemmingsrecht van de or.

Gaat u beleid over persoonsgegevens opstellen of aanpassen, dan moet u dat beleid ter instemming voorleggen aan de ondernemingsraad of uw personeelsvertegenwoordiging. Het kan daarom handig zijn om een vertegenwoordiger uit uw medezeggenschapsorgaan bij de voorbereiding te betrekken.

10. Sancties en boetes

Overtreedt een organisatie de bepalingen van de AVG, dan kan de toezichthouder, de Autoriteit Persoonsgegevens, sancties en boetes opleggen. Een sanctie kan bijvoorbeeld zijn een waarschuwing of aanwijzing van de te nemen acties. De AVG noemt twee categorieën boetes:

- Overtreding van bepalingen die gaan over plichten van organisaties kunnen leiden tot een boete maximaal € 10 miljoen of 2 procent van de wereldwijde jaaromzet.
- Overtreding van bepalingen die gaan over principes, rechtsgrondslagen en rechten van betrokkenen kunnen leiden tot een boete van maximaal € 20 miljoen of 4 procent van de wereldwijde jaaromzet.

Een betrokkene kan ook zelf in actie komen als die vindt dat persoonsgegevens in strijd met de wet zijn verwerkt. Deze actie kan bestaan uit het indienen van een klacht bij de AP of vragen om advies of bemiddeling bij een geschil met een verwerkingsverantwoordelijke. Ook kan betrokkene naar de rechter stappen en een vergoeding vragen voor geleden schade als gevolg van overtreding van de AVG.

11. Begrippen

Betrokkene = een natuurlijk persoon op wie de gegevens betrekking hebben.

Bijzondere categorieën persoonsgegevens = gegevens die gezien hun aard extra gevoelig zijn.

Persoonsgegevens = gegevens die betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon.

Verwerker = degene die handelt in opdracht van de verwerkingsverantwoordelijke bij het verwerken van persoonsgegevens, zonder onder diens rechtstreeks gezag te staan.

Verwerking = elke bewerking of elk geheel van bewerkingen van persoonsgegevens, zoals het verzamelen, opvragen, opslaan, veranderen, gebruiken, raadplegen, doorsturen en verwijderen ervan.

Verwerkingsverantwoordelijke = degene die bepaalt hoe en waarom persoonsgegevens worden verwerkt.

12. Afkortingen

AP = Autoriteit Persoonsgegevens

AVG = Algemene verordening gegevensbescherming

BSN = burgerservicenummer

DPIA = Data protection impact assessment (gegevensbeschermingseffectbeoordeling)

EU = Europese unie

FG = Functionaris gegevensbescherming

PIA = Privacy impact assessment

Wbp = Wet bescherming persoonsgegevens