



**Algemene
Verordening
Gegevensbescherming**

Gegevensbeschermingsbeleid Van Asch Infrastructuur

Uitvoeringswet Algemene verordening gegevensbescherming

Inhoud

1. Inleiding	3
Wetgeving en definities.....	3
Uitgangspunten	4
Rollen Van Asch Infrastructuur.....	6
3. Organisatorische en technische maatregelen.....	8
4. Categorieën persoonsgegevens	9
5. Doeleinden persoonsgegevens	10
6. Verwerking persoonsgegevens	12
7. Rechten betrokkenen – AVG- privacy rechten.....	13
Indienen van verzoek	13
8. Hoe lang worden de persoonsgegevens bewaard?	14
9. Functionaris gegevensbescherming	14
10. Register Datalek meldingen	15
11. Afspraken met verwerkers	16
12. Data Protection Impact Assessment (DPIA)	16
13. Privacy by design & default.....	17
14. Beveiligingsmaatregelen	18
15. Leidende toezichthouder	18
16. Informatie verstrekken aan betrokkene	19
Checklist informatie verstrekken aan de betrokkene	19
17. Toestemming.....	20
Bijlage Bijlage 1- Persoonsgegevens.....	22
Bijlage 2- Register van verwerkingsactiviteiten	23

1. Inleiding

In dit beleid laat Van Asch Infrastructuur zien op welke manier zij dagelijks omgaan met persoonsgegevens en de privacy daarvan. Goed en zorgvuldig omgaan met persoonsgegevens is belangrijk voor Van Asch. Het beschermen van de privacy is complex, en wordt steeds complexer door technologische ontwikkelingen, de decentralisaties, grote uitdagingen op het terrein van veiligheid en nieuwe Europese wetgeving. Daarom vinden wij het belangrijk om transparant te zijn over de manier waarop wij met persoonsgegevens omgaan, en de privacy waarborgen.

Om te voldoen aan de verantwoordingsplicht van de Algemene Verordening Gegevensbescherming (AVG) is er onder andere dit gegevensbeschermingsbeleid opgesteld. Om aan te kunnen tonen dat Van Asch Infrastructuur op een juiste wijze omgaat met de privacy van persoonsgegevens en zich dus aan de wet houdt, worden er in dit beleid diverse maatregelen verder toegelicht.

De onderdelen die in dit gegevensbeschermingsbeleid verder worden toegelicht zijn:

- Welke technische en organisatorische maatregelen er genomen worden.
- Hoe deze maatregelen vorm krijgen in de praktijk (processen, procedures etc.).
- Hoe de rollen en verantwoordelijkheden voor de uitvoer ervan belegt is.
- De categorieën van persoonsgegevens.
- De doeleinden van persoonsgegevens.
- De verwerking van persoonsgegevens.
- De rechten van de betrokkene.

Wetgeving en definities

In dit gegevensbeschermingsbeleid worden de volgende begrippen gehanteerd:

Betrokkene:

De persoon op wie de persoonsgegevens betrekking hebben. De betrokkene is degene van wie de gegevens worden verwerkt.

Verwerker:

De persoon of organisatie die de persoonsgegevens verwerkt in opdracht van een andere persoon of organisatie.

Gegevensbeschermingsverantwoordelijke:

Binnen van de Van Asch zijn er twee personen aangewezen die deze rol uitoefenen. Dit zijn Jan-Willem van der Boon en Johan Blankenberg. Dit wordt verder beschreven in hoofdstuk 9.

Persoonsgegevens:

Alle gegevens die gaan over mensen en waaraan je een mens als individu kunt herkennen. Het gaat hierbij niet alleen om vertrouwelijke gegevens, zoals over iemands gezondheid, maar om ieder gegeven dat te herleiden is tot een bepaald persoon (bijvoorbeeld; naam, adres, geboortedatum). Naast gewone persoonsgegevens kent de wet ook bijzondere persoonsgegevens. Dit zijn gegevens die gaan over gevoelige onderwerpen, zoals etnische achtergrond, politieke voorkeuren of het Burgerservicenummer (BSN).

Verantwoordelijke:

Een persoon of instantie die alleen, of samen met een ander, het doel en de middelen voor de verwerking van persoonsgegevens vaststelt.

Verwerking:

Een verwerking is alles wat je met een persoonsgegeven doet, zoals: vastleggen, bewaren, verzamelen, bij elkaar voegen, verstrekken aan een ander, en vernietigen.

Gegevensbeschermingseffectbeoordeling:

Met een gegevensbeschermingseffectbeoordeling worden de effecten en risico's van de nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy. Dit heet ook wel een Privacy Impact Assessment (PIA).

Uitgangspunten

Van Asch Infrastructuur gaat op een veilige manier met persoonsgegevens om en respecteert de privacy van betrokkenen. Van Asch houdt zich hierbij aan de volgende uitgangspunten:

Rechtmatigheid, behoorlijkheid, transparantie

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

Grondslag en doelbinding

Van Asch Infrastructuur zorgt ervoor dat persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen worden verzameld en verwerkt. Persoonsgegevens worden alleen met een rechtvaardige grondslag verwerkt.

Dataminimalisatie

Van Asch Infrastructuur verwerkt alleen de persoonsgegevens die minimaal noodzakelijk zijn voor het vooraf bepaalde doel. Van Asch Infrastructuur streeft naar minimale gegevensverwerking. Waar mogelijk worden minder of geen persoonsgegevens verwerkt.

Bewaartermijn

Persoonsgegevens worden niet langer bewaard dan nodig is. Het bewaren van persoonsgegevens kan nodig zijn om de taken van Van Asch Infrastructuur goed uit te kunnen oefenen of om wettelijke verplichtingen te kunnen naleven.

Integriteit en vertrouwelijkheid

Van Asch Infrastructuur gaat zorgvuldig om met persoonsgegevens en behandelt deze vertrouwelijk. Zo worden persoonsgegevens alleen verwerkt door personen die verantwoordelijk zijn voor gegevensbescherming. Daarbij zorgt Van Asch Infrastructuur voor passende beveiliging van persoonsgegevens.

Delen met derden

In het geval van samenwerking met externe partijen, waarbij sprake is van gegevensverwerking van persoonsgegevens, maakt Van Asch Infrastructuur afspraken over de eisen waar gegevensuitwisseling aan moet voldoen. Deze afspraken voldoen aan de wet. Van Asch Infrastructuur controleert deze afspraken.

Subsidiariteit

Voor het bereiken van het doel waarvoor de persoonsgegevens worden verwerkt, wordt inbreuk op de persoonlijke levenssfeer van de betrokken burger zoveel mogelijk beperkt.

Proportionaliteit

De inbreuk op de belangen van de betrokkene mag niet onevenredig zijn in verhouding tot en met de verwerking te dienen doel.

Rechten van betrokkenen

Van Asch Infrastructuur honoreert alle rechten van betrokkenen.

Aldus vastgesteld door Jan-Willem van den Boon, Directeur

Rollen Van Asch Infrastructuur

De rollen die van Asch aanneemt zijn:

- **Verwerkingsverantwoordelijke** (voorheen de verwerker genoemd):
De persoon of organisatie die het doel en de middelen van de gegevensverwerking vaststelt.
Er zijn een aantal zaken waaraan de verwerkingsverantwoordelijke moet voldoen:
 - Gegevensbeschermingsbeleid opstellen
 - Passende technische en organisatorische maatregelen nemen
 - Register van verwerkingsactiviteiten maken
 - Gegevensbescherming effectbeoordeling
 - Functionaris Gegevensbescherming opstellen, indien van toepassing
 - Melding van een data lek
- **Verwerker** (voorheen de bewerker genoemd):
De persoon of organisatie die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.
- **Betrokkene**: De persoon van wie de persoonsgegevens verwerkt worden.

2. Algemene informatie

Van Asch infrastructuur is een aannemersbedrijf in de Grond- Weg- en Waterbouw (GWW-sector) en hierbij is de CAO voor de Bouwnijverheid van toepassing.

Typering van het bedrijf

- Van Asch Infrastructuur voert projecten uit in de grond-, weg- en waterbouw. Het gaat dan om:
- Saneren en bouwrijp maken van diverse soorten terreinen;
- (Her)inrichten en bestraten van bouwlocaties en bestaande locaties;
- Aanleg van wegverhardingen;
- Aanleg en vervangen van rioleringen, afwateringen en drainage.

Voor de diverse werkzaamheden beschikt van Asch Infrastructuur over het benodigde materiaal en hebben we vakbekwaam personeel in dienst.

Naast bovengenoemde hoofdactiviteiten, richt Van Asch infrastructuur zich op:

- Uitvoering van turnkey projecten;
- Advisering over constructies;
- Ontwerp van bestratingen;
- Door middel van beplanting inrichten van terreinen;
- Het totale onderhoud van openbare locaties.

CAO en overige arbeidsvoorwaarden

Bij Van Asch infrastructuur is de CAO voor de Bouwnijverheid van toepassing, waarin de arbeidsvoorwaarden, regelingen, procedures en afspraken voor het personeel zijn vastgelegd. Deze CAO is uitgesplitst naar :

- Bouwplaats medewerkers – voor het overgrote deel van het personeel;
- UTA medewerkers – voor midden- en hoger kader.

3. Organisatorische en technische maatregelen

In dit hoofdstuk worden de organisatorische en technische maatregelen beschreven die genomen zijn bij Van Asch Infrastructuur. Hieronder worden de maatregelen beschreven en verder toegelicht.

Organisatorische maatregelen:

- Toewijzen van verantwoordelijkheden voor informatiebeveiliging.
Binnen Van Asch zijn er twee verantwoordelijke die de persoonsgegevens beveiligen. Tegelijkertijd zijn dit ook de personen die gaan over de bescherming van de persoonsgegevens.
- Bevorderen van beveiligingsbewustzijn bij bestaande en nieuwe werknemers.
Wanneer er een nieuwe werknemer in dienst komt moet hij/zij tekenen voor toestemming voor gegevensverwerking door Van Asch. Daarmee krijgt hij/zij ook het gegevensbeschermingsbeleid voor betrokkene mee, waarin hij/zij op de hoogte wordt gesteld van het beveiligingsbewustzijn bij Van Asch.
- Minder mensen in de organisatie toegang geven tot persoonsgegevens.
Alle gegevens die eerder openbaar op de server stonden zijn afgeschermd voor de andere gebruikers van de servers. Alleen Jan-Willem en Johan Blankenberg, de personen die gaan over de bescherming van persoonsgegevens hebben nog toegang tot de persoonsgegevens.
- Beoordelen of dezelfde doelen behaald kunnen worden met minder persoonsgegevens.
Deze beoordeling heeft plaats gevonden door Jan-Willem en Johan Blankenberg, hiermee hebben zij kunnen aantonen, dat men met name, minder persoonsgegevens kan verstrekken naar derde, maar wel hetzelfde doel behaald kan worden. Voor de administratie zijn de bestaande gegevens nodig en indien er niet meer gebruikt wordt gemaakt van de gegevens worden deze achterwegen gelaten.

Technische maatregelen:

- Versleuteling van persoonsgegevens. Jan-Willem van der Boon en Johan Blankenberg houden zich bezig met de bescherming van persoonsgegevens.
- Op website is een Cookie-melding toegevoegd.
- De website is voorzien van een https certificaat en hiermee voorzien van het veiligste protocol op het internet.

4. Categorieën persoonsgegevens

Van Asch Infrastructuur beheert twee verschillende categorieën persoonsgegevens, namelijk gewone en bijzondere persoonsgegevens. Hieronder wordt toegelicht welke gegevens Van Asch verzameld verdeeld onder de twee categorieën.

Gewone persoonsgegevens

- Voorletters;
- Achternaam;
- Roepnaam;
- Geslacht;
- Adres;
- Postcode;
- Woonplaats;
- Telefoonnummer;
- Geboortedatum;
- Geboorteplaats;
- E-mail adres;
- Burgerlijke staat;
- Contact bij ongeval;

Bijzondere persoonsgegevens:

- BSN-nummer;
- Kopie identiteitskaart/ paspoort
- Rijbewijs
- VCA diploma
- Behaalde cursussen
- IBAN nummer

De Arbo dienst beschikt over de medische gegevens, hier heeft Van Asch geen toegang tot. In bijlage 1 is het formulier van personeelsgegevens toegevoegd die wordt verwerkt in het personeelsdossier.

5. Doeleinden persoonsgegevens

Op grond van de Verordening mogen persoonsgegevens slechts verwerkt worden voor wel bepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen. De gegevens mogen niet voor andere doelen verwerkt worden. De doeleinden zijn is dit hoofdstuk uitdrukkelijk omschreven, dit houdt in dat de doeleinden voor het verzamelen en verwerken van de persoonsgegevens zijn vastgesteld. Tot slot wordt het doel gerechtvaardigd. Hierbij is het van belang dat de verwerking kan worden gebaseerd op één van de rechtsgrondslagen als genoemd in de Verordening. De zes rechtsgrondslagen worden hieronder kort toegelicht.

Zes rechtsgrondslagen:

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

De grondslagen 2 tot en met 6 zijn 'noodzakelijkheidsgrondslagen': alleen wanneer de verwerkingen noodzakelijk zijn voor de in deze grondslagen genoemde doelen dan is de verwerking gerechtvaardigd.

De doeleinden voor de verwerking van de persoonsgegevens bij Van Asch Infrastructuur zijn:

1. Voor de uitvoering van de administratie waarbij het noodzakelijk is voor het aangaan van een overeenkomst tussen werkgever en werknemer.
2. Het verstrekken van wettelijke verplichte certificaten voor uitvoering van werkzaamheden in de GWW-sector. Denk hierbij aan diverse certificaten als een VCA diploma, het rijbewijs, veilig werken langs de weg etc.

De doeleinden zijn beide gebaseerd op meerdere grondslagen, namelijk:

- Toestemming: de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden, zie hoofdstuk 17;
 - In iedere dossier van een werknemer is een overeenkomst getekend voor de verwerking van de persoonsgegevens. Hiermee geeft de werknemer aan of hij/zij akkoord gaat met de doeleinden van de gegevensverwerking.

- Uitvoeren overeenkomst: de verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen;
 - Voor de totstandkoming van een overeenkomst tussen werknemer en werkgever is Van Asch Infrastructuur genoodzaakt persoonsgegevens te verwerken om een contract te kunnen afsluiten en/of voor de toekomst maatregelen te kunnen nemen. Deze gegevens worden verwerkt in de administratie en het personeelsdossier van de desbetreffende werknemer.

- 7. Wettelijke verplichting: de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;
 - Om te voldoen aan de AVG worden de gegevens verwerkt en geregistreerd. Hiervoor heeft de verwerkingsverantwoordelijke en gegevensbeschermingsverantwoordelijke toegang tot de persoonsgegevens. Daarbij hebben zij de taak om zorgvuldig en de juiste handelingen met de persoonsgegevens uit te voeren.

6. Verwerking persoonsgegevens

De gegevens verwerking wordt in kaart gebracht door een register van verwerkingsactiviteiten. Hierin wordt gedocumenteerd welke persoonsgegevens worden verwerkt, met welk doel dit wordt gedaan, waar de gegevens vandaan komen en met wie deze gegevens worden gedeeld. Het register van verwerkingsactiviteiten wordt beheert en bijgehouden door gegevensbeschermingsverantwoordelijke, Jan- Willem van der Boon en Johan Blankenberg. In bijlage 2 wordt het format van het register weergegeven.

Van Asch Infrastructuur stelt zelf het doel en de middelen voor de verwerking van persoonsgegevens vast. Van Asch infrastructuur is hierbij de verwerkingsverantwoordelijke. Als verwerkingsverantwoordelijke worden de volgende gegevens opgenomen in het register:

- De naam en contactgegevens van:
 - Uw organisatie, of de vertegenwoordiger van uw organisatie;
 - Eventuele andere organisaties met wie u gezamenlijk de doelen en middelen van de verwerking heeft vastgesteld;
 - De Functionaris voor de gegevensbescherming, indien van toepassing;
 - Eventuele andere internationale organisaties waar u persoonsgegevens mee deelt.
- De doelen waarvoor u de persoonsgegevens verwerkt. Bijvoorbeeld voor de werving en selectie van personeel, het bezorgen van producten of direct marketing;
- Een beschrijving van de categorieën van personen van wie u gegevens verwerkt. Bijvoorbeeld uitkeringsgerechtigden, klanten of patiënten;
- Een beschrijving van de categorieën van persoonsgegevens. Zoals het BSN, NAW-gegevens, telefoonnummers, camerabeelden of IP-adressen;
- De datum waarop u de gegevens moet wissen (als dat/deze bekend is);
- De categorieën van ontvangers aan wie u persoonsgegevens verstrekt;
- Een algemene beschrijving van de technische en organisatorische maatregelen die er zijn genomen om persoonsgegevens te beveiligen.

7. Rechten betrokkenen – AVG- privacy rechten

De rechten die de betrokkenen kunnen uitoefenen op Van Asch Infrastructuur worden in dit hoofdstuk verder toegelicht. De rechten die voor de betrokkenen van invloed zijn, luiden als volgt:

- Het recht op inzage, correctie en verwijdering van persoonsgegevens
- Het recht om bij de Autoriteit persoonsgegevens (AP) een klacht in te dienen over de manier waarop met de persoonsgegevens wordt omgegaan. De AP is verplicht om deze klacht te behandelen.
- Het recht op dataportabiliteit. Het recht om persoonsgegevens over te dragen.
- Het recht op vergetelheid. Het recht om 'vergeten' te worden.
- Recht op inzage. Dat is het recht van mensen om de persoonsgegevens die u van hen verwerkt in te zien.
- Recht op rectificatie en aanvulling. Het recht om de persoonsgegevens die Van Asch verwerkt te wijzigen.
- Het recht op beperking van de verwerking: het recht om minder gegevens te laten verwerken.
- Het recht met betrekking tot geautomatiseerde besluitvorming en profilering. Oftewel: het recht op een menselijke blik bij besluiten.
- Het recht om bezwaar te maken tegen de gegevensverwerking.
- Het recht op duidelijke informatie over wat er met de persoonsgegevens wordt gedaan bij Van Asch Infrastructuur.

Indienen van verzoek

Om gebruik te maken van zijn/haar rechten kan de betrokkene een verzoek indienen. Dit verzoek kan zowel schriftelijk als via de e-mail ingediend worden. Van Asch Infrastructuur heeft vier weken de tijd, vanaf de ontvangst van het verzoek, om te beoordelen of het verzoek gerechtvaardigd is. Binnen vier weken zal Van Asch Infrastructuur laten weten wat er met het verzoek gaat gebeuren. Als het verzoek niet wordt opgevolgd is er de mogelijkheid om een klacht in te dienen bij de Autoriteit Persoonsgegevens (AP). Aan de hand van een verzoek kan Van Asch Infrastructuur aanvullende informatie opvragen om zeker te zijn van de identiteit van de betrokkene.

8. Hoe lang worden de persoonsgegevens bewaard?

De persoonsgegevens worden niet langer bewaard dan noodzakelijk is. Hoelang de gegevens bewaard blijven hangt af van het doel waarvoor de persoonsgegevens worden verzameld en verwerkt. Per situatie is dit verschillend, er staat geen vast bewaartermijn voor het bewaren van persoonsgegevens. Per situatie wordt er gekeken naar het doel en of het nog noodzakelijk is om de gegevens te bewaren. Wanneer het doel niet meer noodzakelijk is worden de persoonsgegevens:

- Verwijderd;
- Of bijv. alle identificerende kenmerken worden verwijderd.

Er zijn ook gegevens zonder een wettelijke bewaartermijn, zoals verslagen van functionerings- en beoordelingsgesprekken en administratieve verzuimgegevens. Voor die gegevens geldt over het algemeen een aanbevolen bewaartermijn van twee jaar nadat het dienstverband is beëindigd. Over het algemeen worden de persoonsgegevens bij Van Asch bewaard zolang men in dienst is. Wanneer men uit dienst treedt en er verder geen contact meer plaats vindt, worden de persoonsgegevens verwijderd uit het personeelsdossier. Wanneer er een arbeidsconflict heeft plaats gevonden mogen de gegevens van een (ex)-werknemer langer bewaard worden. De werknemer heeft gedurende vijf jaar het recht om een vordering bij een oud-werkgever in te stellen, bijvoorbeeld vakantiedagen, atv-dagen en vakantierecht. Van Asch vindt het dus zeer belangrijk om zorgvuldig te handelen bij het opruimen van een personeelsdossier.

9. Functionaris gegevensbescherming

Van Asch Infrastructuur heeft geen functionaris gegevensbescherming (FG) aangesteld, met de volgende redenen:

- Van Asch Infrastructuur voert geen overheidstaken uit en is dus geen publieke organisatie, openbaarvervoerbedrijf, energiebedrijf of woningcorporatie etc.
- Van Asch Infrastructuur volgt vanuit zijn kernactiviteiten geen grote groep individuen.
- Van Asch Infrastructuur verwerkt wel bijzondere persoonsgegevens, maar voert dit niet uit op grote schaal. Het aantal persoonsgegevens dat verwerkt wordt is twintig (Autoriteit Persoonsgegevens, 2018) .

Hiermee onderbouwt Van Asch Infrastructuur dat het in de huidige situatie niet noodzakelijk is om een functionaris gegevensbescherming vast te leggen.

Van Asch Infrastructuur heeft ter compensatie twee personen aangewezen die binnen de organisatie gegevensbeschermingsverantwoordelijke zijn voor de persoonsgegevens. Dit zijn:

- Jan-Willem van der Boon;
- Johan Blankenberg.

Zij beheren de persoonsgegevens en zijn de enige bevoegde tot de persoonsgegevens.

10. Register Datalek meldingen

Sinds 1 januari 2016 geldt de meldplicht datalekken. Deze meldplicht houdt in dat er direct een melding gedaan moet worden bij de Autoriteit Persoonsgegevens zodra er een ernstig datalek heeft plaats gevonden. En soms moet het datalek ook gemeld worden aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt). We spreken van een datalek wanneer persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens mogen hebben. De Autoriteit Persoonsgegevens heeft beleidsregels meldplicht datalekken opgesteld. Deze beleidsregels zijn bedoeld om organisaties te helpen bij het bepalen of er sprake is van een datalek dat zij moeten melden bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen.

Van Asch Infrastructuur heeft een register opgesteld waarin de datalekken vermeld moeten worden. Voor nu is dit nog niet van toepassing, omdat er nooit eerder een datalek heeft plaats gevonden. Wanneer er een datalek heeft plaats gevonden moeten de volgende gegevens vermeld worden in het register:

- Een korte omschrijving van het lek.
- Wanneer het datalek heeft plaatsgevonden.
- Wat er met de gegevens is gebeurd.
- Van welke groep(en) personen er gegevens gelekt zijn, en om hoeveel personen het gaat.
- Om welke soorten gegevens het gaat.
- De (mogelijke) gevolgen van de inbreuk.
- De maatregelen die zijn genomen naar aanleiding van het lek.
- Welke actie is ondernomen om schade te voorkomen of zo veel mogelijk te beperken.
- Wat er gedaan is om te zorgen dat het niet nog een keer kan gebeuren.

11. Afspraken met verwerkers

De verwerking van de digitale loonstrook wordt uitbesteed aan People Profs. Zij hebben toegang tot bepaalde persoonsgegevens die betrekking hebben op de loonstrook. Volgens de AVG moeten er afspraken gemaakt worden over de verwerking van deze persoonsgegevens. De afspraken worden schriftelijk vastgesteld. Het document waarin dit wordt vastgesteld is de 'verwerkersovereenkomst'. Deze overeenkomst heeft Van Asch Infrastructuur vastgelegd met alle partijen waarbij de persoonsgegevens worden gedeeld. Van Hal- telecom beheert binnen Van Asch Infrastructuur de telecommunicatie, de server, automatisering en alle overige zaken met betrekking tot telecom. Wanneer Van Asch Infrastructuur te maken heeft met een datalek is hiervoor een verwerkersovereenkomst getekend met Van Hal- telecom om te voldoen aan de eisen van de AVG. Bij 4PS is het boekhoudpakket Navision afgenomen, waarin gegevens van de werknemers worden verwerkt voor onder andere de facturatie en voor het verwerken van de loongegevens. In de verwerkersovereenkomst komen diverse onderwerpen aan bod, zoals, beveiliging, geheimhouding, datalekken en wat er bijvoorbeeld gebeurt met de gegevens na afloop van de overeenkomst. Deze overeenkomst is in het bezit van de verantwoordelijke(n) voor de gegevensbescherming.

12. Data Protection Impact Assessment (DPIA)

In de Nederlandse vertaling van de AVG wordt de term data protection impact assessment (DPIA) gegevensbeschermingseffectbeoordeling genoemd. Met een gegevensbeschermingseffectbeoordeling worden de effecten en risico's van nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy. Van Asch Infrastructuur komt hiermee in aanmerking wanneer zij op een geautomatiseerde manier de persoonsgegevens gaan verwerken, er een grootschalige verwerking en of er een grootschalige monitoring van openbare ruimten plaats gaat vinden.

Als onderdeel van de verantwoordingsplicht is een goede onderbouwing nodig om aan te kunnen geven, geen gebruik van te maken van een DPIA. De huidige situatie van de Autoriteit Persoonsgegevens (AP) geeft aan dat overige organisaties, in tegenstelling tot de rijksoverheid, nu nog niet verplicht zijn een DPIA uit te voeren.

Voor Van Asch Infrastructuur is er nog geen sprake van een DPIA. De omvang van de persoonsgegevens en de uitwisseling van deze gegevens is nog ter mate klein dat dit niet van toepassing is.

Er hoeft geen data protection impact assessment (PIA) uit gevoerd te worden wanneer uw gegevensverwerking:

- Waarschijnlijk geen hoog privacy risico oplevert.
- Sterk lijkt op een andere gegevensverwerking waarvoor al een DPIA is uitgevoerd.
- Wordt geregeld door een andere Europese of nationale wet en er bij de totstandkoming van deze wet al een DPIA is uitgevoerd. Tenzij de privacy toezichthouder oordeelt dat er toch een DPIA nodig is.
- Op een lijst staat van verwerkingen waarvoor een DPIA niet verplicht is. De AVG geeft de privacy toezichthouder de mogelijkheid om zo'n lijst op te stellen, maar dit is niet verplicht (Autoriteit Persoonsgegevens, 2018).

Bovenstaande punten worden bij Van Asch Infrastructuur gehanteerd en daarmee onderbouwt Van Asch tegelijkertijd dat zij niet genoodzaakt zijn om te voldoen aan een DPIA.

13. Privacy by design & default

Om Van Asch Infrastructuur nu al vertrouwd te maken met de AVG verplichte uitgangspunten van privacy by design en privacy by default wordt hieronder toegelicht hoe deze beginselen binnen Van Asch worden uitgevoerd.

Privacy by design

De persoonsgegevens worden beschermd door de verantwoordelijke van de gegevensbescherming, dit zijn Jan-Willem van der Boon en Johan Blankenberg. Tegelijkertijd zijn de gegevens ook digitaal beschermd voor andere gebruikers van het systeem door geen toegang te verlenen. Tot slot worden er niet meer gegevens verzameld dan noodzakelijk voor het doel van de verwerking.

Privacy by default

De technische en organisatorische maatregelen zijn toegelicht in hoofdstuk 3 van dit beleid. Hierin staat beschreven welke maatregelen er genomen zijn om ervoor te zorgen dat als standaard, alléén persoonsgegevens verwerkt worden die noodzakelijk zijn voor het specifieke doel dat Van Asch Infrastructuur wilt bereiken.

14. Beveiligingsmaatregelen

Diverse beveiligingsmaatregelen die genomen zijn om te voldoen aan de verantwoordingsplicht van de AVG zijn:

- Persoonsgegevens zijn alleen toegankelijk voor verwerkers en de gegevensbeschermingsverantwoordelijke.
- Verouderde persoonsgegevens worden verwijderd.
- Alleen noodzakelijke persoonsgegevens worden verwerkt in het personeelsdossier.

15. Leidende toezichthouder

Bij Van Asch Infrastructuur is er geen sprake van vestigingen in meerdere EU-lidstaten. Er is dus ook geen sprake van een leidende toezichthouder.

16. Informatie verstrekken aan betrokkene

Voor het verstrekken van informatie aan de betrokkene is er een checklist opgesteld. Hieronder is de checklist weergegeven. De informatie die uit de checklist naar voren komt is beschreven in een handleiding die verstrekt is aan iedere betrokkene van de persoonsgegevens verwerking.

Checklist informatie verstrekken aan de betrokkene

- Uw identiteit en uw contactgegevens, of de contactgegevens van uw vertegenwoordiger;
- Indien u een functionaris voor de gegevensbescherming hebt aangesteld, de contactgegevens van deze functionaris;
- De doelen waarvoor u persoonsgegevens verwerkt;
- De grondslag waarop u de verwerking baseert;
- Wanneer u de verwerking baseert op de grondslag 'gerechtvaardigd belang': wat uw gerechtvaardigd belang is;
- De eventuele ontvangers of categorieën ontvangers van de gegevens;
- In geval van verstrekking aan derde landen:
 - of er een adequaatheidsbesluit van de Commissie bestaat,
 - of passende waarborgen zijn getroffen, welke dit zijn en of hier een kopie van kan worden verkregen, dan wel waar die waarborgen kunnen worden geraadpleegd;
- De bewaartermijn, of als dat niet mogelijk is de criteria voor het bepalen ervan;
- De rechten van de betrokkene (beschreven in hoofdstuk 7);
- In het geval van toestemming, dat de betrokkene die toestemming altijd weer kan intrekken;
- Dat de betrokkene het recht heeft een klacht in te dienen over uw verwerking bij de Autoriteit

Persoonsgegevens;

- Of het verwerken van persoonsgegevens een wettelijke verplichting is of noodzakelijk is voor de uitvoering of het aangaan van een overeenkomst, of de betrokkene verplicht is die gegevens te verstrekken en wat de gevolgen zijn van het niet verstrekken van die gegevens voor de betrokkene;

De betrokkene bij de verwerking van de persoonsgegevens zijn People Profs, Van Hal-telecom en 4PS. Met alle partijen is een verwerkingsovereenkomst vastgesteld, waarin bovenstaande checklist is verwerkt.

17. Toestemming

De gegevensverwerking is gebaseerd op toestemming van de betrokkene. De AVG stelt strengere eisen aan de toestemming van betrokkene. Van Asch Infrastructuur moet kunnen aantonen dat zij een geldige toestemming van de betrokkene heeft verkregen om zijn of haar persoonsgegevens te verwerken. En dat het voor de betrokkene net zo makkelijk is om hun toestemming in te trekken.

De toestemming moet aan een aantal voorwaarden voldoen om het als een geldige toestemming te laten gelden, namelijk:

Vrij

Ten eerste moet de toestemming vrij gegeven zijn. Dit houdt in dat iemand daadwerkelijk de keuze moet hebben om te weigeren, zonder dat hier negatieve consequenties aan verbonden zijn. Met name wanneer er sprake is van een afhankelijkheidsrelatie, bijvoorbeeld in de arbeidssfeer of in de relatie overheid-burger, zal toestemming niet snel vrij zijn gegeven. Dit betekent dat u in dergelijke situaties de verwerking van persoonsgegevens niet op deze grondslag kan baseren. Wanneer u de uitvoering van een overeenkomst afhankelijk maakt van het geven van toestemming voor een andere verwerking die niet noodzakelijk is voor de uitvoering van de overeenkomst ('bundelen'), dan dient ten strengste rekening te worden gehouden met de vraag of deze toestemming vrijelijk gegeven kan worden. Wanneer bijvoorbeeld een bank aan haar klanten met een betaalrekening vraagt om toestemming voor de verwerking van deze gegevens voor bepaalde direct marketingdoeleinden, en de weigering van deze toestemming leidt tot het niet meer leveren van betaaldiensten, het sluiten van de betaalrekening of hogere kosten voor de betaalrekening, dan wordt de toestemming veronderstelt niet vrij te zijn gegeven.

Specifiek en geïnformeerd

Ten tweede moet toestemming specifiek zijn en geïnformeerd. U moet dus als verwerkingsverantwoordelijke duidelijke informatie verschaffen over de redenen waarom u de persoonsgegevens gaat verwerken (het doel), maar ook over andere zaken die van belang zijn om te zorgen dat de betrokkene voldoende informatie heeft om een goed geïnformeerd besluit te nemen. Denk dan dus ook aan informatie over de manier waarop u de persoonsgegevens verwerkt, met wie u de persoonsgegevens gaat delen, hoe lang u ze gaat bewaren en of ze naar landen buiten de Europese Unie worden doorgegeven.

Ondubbelzinnig

Tenslotte moet toestemming ondubbelzinnig zijn. Er mag geen twijfel bestaan over het feit dat de betrokkene toestemming heeft gegeven. Toestemming kan blijken uit een ondubbelzinnige wilsuiting of uit een ondubbelzinnige, actieve handeling van de betrokkene. Vaak wordt hiervoor de term *opt in* gehanteerd. *Opt out* – het gebruik maken van de optie om je van toestemming te onthouden – is geen toestemming. Wanneer de betrokkene bijvoorbeeld een vinkje zet in een vakje om zijn akkoord aan te geven, dan is er sprake van ondubbelzinnige toestemming (*opt in*). Wanneer echter hetzelfde vakje al aangekruist is en de betrokkene vinkt het niet uit (*opt out*), dan is er geen ondubbelzinnige toestemming tot stand gekomen. Het is namelijk niet duidelijk wat de echte wil van de betrokkene is (deze kan bijvoorbeeld het vakje over het hoofd hebben gezien). Met andere woorden, het afleiden van toestemming uit het feit dat iemand niet handelt of niet protesteert (wat de Engelsen *implied consent* noemen), is niet toegestaan.

De toestemming van de betrokkene zijn verwerkt in het personeelsdossier van die persoon.

Bijlage

Bijlage 1- Persoonsgegevens

Personeelsgegevens

31

Ingangsdatum:	
Werkgever Van Asch Infrastructuur	
Gegevens werknemer	<input type="checkbox"/> Nieuw in dienst per: _____ <input type="checkbox"/> Mutatie ingaande per: _____
Voorletters, achternaam:	
Roepnaam:	<input type="checkbox"/> Man <input type="checkbox"/> Vrouw
Adres	
Postcode, woonplaats	
Telefoonnummer	
Geboortedatum	
Geboorteplaats	
BSN nummer	
Emailadres	
Burgerlijke staat	<input type="checkbox"/> Gehuwd <input type="checkbox"/> Samenwonend <input type="checkbox"/> Ongehuwd <input type="checkbox"/> geregistreerd Datum _____ Datum _____
Naam partner/echtgenoot	
Kinderen	Naam: _____ Geb.datum: _____ J / M Naam: _____ Geb.datum: _____ J / M Naam: _____ Geb.datum: _____ J / M
Legitimatiebewijs	Verplicht kopie inleveren <input type="checkbox"/> paspoort <input type="checkbox"/> identiteitskaart
Rijbewijs	<input type="checkbox"/> A <input type="checkbox"/> B <input type="checkbox"/> C <input type="checkbox"/> D <input type="checkbox"/> E achter B <input type="checkbox"/> E achter C <input type="checkbox"/> E achter D Indien van toepassing graag kopie inleveren
In het bezit van VCA	<input type="checkbox"/> Ja, datum _____ : <input type="checkbox"/> Nee, opgeven voor VCA
Behaalde cursus(s)en	<input type="checkbox"/> _____ datum _____ <input type="checkbox"/> _____ datum _____ <input type="checkbox"/> _____ datum _____
IBAN nummer	_NL_____ Bank _____
Contact bij ongeval	Naam: _____ Telefoon: _____
Overige belangrijke gegevens	

