

# Privacy beleid

## Van Dijk Hoogland BV

**Uitvoeringswet Algemene verordening gegevensbescherming**

**Van Dijk Hoogland | Bunschoterstraat 27a | 3828NR HOOGLAND | 033 480 5199**

# Inhoud

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

## 1. Inleiding

In dit beleid laat Van Dijk Hoogland zien op welke manier zij dagelijks omgaan met persoonsgegevens en de privacy daarvan. Goed en zorgvuldig omgaan met persoonsgegevens is belangrijk voor Van Dijk Hoogland . 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 Dijk Hoogland 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 Dijk Hoogland zijn er drie personen aangewezen die deze rol uitoefenen. Dit zijn Gerald, Danielle en Monique van Dijk. Dit wordt verder beschreven in hoofdstuk 9 van dit gegevensbeschermingsbeleid.

*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 Dijk Hoogland gaat op een veilige manier met persoonsgegevens om en respecteert de privacy van betrokkenen. Van Dijk Hoogland 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 Dijk Hoogland 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 Dijk Hoogland verwerkt alleen de persoonsgegevens die minimaal noodzakelijk zijn voor het vooraf bepaalde doel. Van Dijk Hoogland streeft naar minimale gegevensverwerking. Waar mogelijk worden minder of geen persoonsgegevens worden verwerkt.

*Bewaartermijn*

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

### *Integriteit en vertrouwelijkheid*

Van Dijk Hoogland gaat zorgvuldig om met persoonsgegevens en behandelt deze vertrouwelijk. Zo worden persoonsgegevens alleen verwerkt door personen met een geheimhoudingsplicht en voor het doel waarvoor deze gegevens zijn verzameld. Daarbij zorgt Van Dijk Hoogland 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 Dijk Hoogland afspraken over de eisen waar gegevensuitwisseling aan moet voldoen. Deze afspraken voldoen aan de wet en worden verwerkt in een verwerkersovereenkomst. Van Dijk Hoogland 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 Dijk Hoogland honoreert alle rechten van betrokkenen.

G.H.J. van Dijk, Directeur

## Rollen Van Dijk Hoogland

De rollen die Van Dijk Hoogland 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 nodig)
  - Melding van eventuele inbreuk melden
- **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. Organisatorische en technische maatregelen

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

### **Organisatorische maatregelen:**

- Toewijzen van verantwoordelijkheden voor informatiebeveiliging.  
Binnen Van Dijk Hoogland zijn er drie 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 werknemer.  
Wanneer er een werknemer in dienst komt moet hij/zij tekenen voor toestemming van gegevensverwerking door Van Dijk Hoogland . Daarmee krijgt hij/zij ook het gegevensbeschermingsbeleid voor betrokkene mee, waarin hij/zij op de hoogte wordt gesteld van het beveiligingsbewustzijn bij Van Dijk Hoogland .
- 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 Gerald, Danielle en Monique van Dijk zijn de personen die toegang tot de persoonsgegevens hebben. Indien er door collega's binnen de organisatie persoonsgegevens worden verwerkt gebeurt dit onder toestemming van een van de gegevensbeschermingsverantwoordelijke
- Beoordelen of dezelfde doelen behaald kunnen worden met minder persoonsgegevens.  
Deze beoordeling heeft plaats gevonden door Danielle en Monique van Dijk, hiermee kunnen zij aantonen, dat met name, minder persoonsgegevens verstrekt worden aan derde, hetzelfde doel behaald kan worden. Voor de administratie zijn de bestaande gegevens nodig, wanneer deze gegevens niet meer gebruikt worden, worden de gegevens verwijderd uit het personeelsdossier en het systeem.

### **Technische maatregelen:**

- Versleuteling van persoonsgegevens. Gerald, Danielle en Monique van Dijk 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.

### 3. Categorieën persoonsgegevens

Van Dijk Hoogland beheert twee verschillende categorieën persoonsgegevens, namelijk gewone en bijzondere persoonsgegevens. Hieronder wordt toegelicht welke gegevens Van Dijk Hoogland 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 Boval en Consensus Arbo beschikken over de medische gegevens, hier heeft Van Dijk Hoogland geen toegang tot. In bijlage 1 is het formulier van personeelsgegevens toegevoegd die wordt verwerkt in het personeelsdossier.



## 4. 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 in 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 Dijk Hoogland zijn:

1. Voor de uitvoering van administratieve werkzaamheden, zoals de urenregistratie, salarisadministratie, ziekteverzuim etc. Tevens is het ook noodzakelijk voor het aangaan van een overeenkomst tussen werkgever en werknemer.

2. Het verstrekken van wettelijke verplichte certificaten voor uitvoering van de werkzaamheden. 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 Dijk Hoogland 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.
- 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 en de taak om zorgvuldig en de juiste handelingen met de persoonsgegevens uit te voeren.

## 5. 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 de gegevensbeschermingsverantwoordelijke, Gerald en Danielle van Dijk. In bijlage 2 wordt het format van het register weergegeven.

Van Dijk Hoogland stelt zelf het doel en de middelen voor de verwerking van persoonsgegevens vast. Van Dijk Hoogland 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 (FG) als u die heeft aangesteld;
  - 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;
- Deelt u de gegevens met een land of internationale organisatie buiten de EU? Dan moet u dit aangeven in het register;
- Een algemene beschrijving van de technische en organisatorische maatregelen die u hebt/heeft genomen om persoonsgegevens die u verwerkt te beveiligen.

## 6. Rechten betrokkenen – AVG- privacy rechten

De rechten die de betrokkenen kunnen uitoefenen op Van Dijk Hoogland 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 Dijk Hoogland 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 Dijk Hoogland 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 Dijk Hoogland heeft vier weken de tijd, vanaf de ontvangst van het verzoek, om te beoordelen of het verzoek gerechtvaardigd is. Binnen vier weken zal Van Dijk Hoogland 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 Dijk Hoogland aanvullende informatie opvragen om zeker te zijn van de identiteit van de betrokkene.

## 7. 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.

Over het algemeen worden de persoonsgegevens bij Van Dijk Hoogland 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.

## 8. Functionaris gegevensbescherming

Van Dijk Hoogland heeft geen functionaris gegevensbescherming (FG) aangesteld, met de volgende redenen:

- Van Dijk Hoogland voert geen overheidstaken uit en is dus geen publieke organisatie, openbaarvervoerbedrijf, energiebedrijf of woningcorporatie etc.
- Van Dijk Hoogland volgt vanuit zijn kernactiviteiten geen grote groep individuen.
- Van Dijk Hoogland verwerkt wel bijzondere persoonsgegevens, maar voert dit niet uit op grote schaal. Het aantal persoonsgegevens dat verwerkt wordt is tussen 25 en 30. (Autoriteit Persoonsgegevens, 2018) .

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

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

- Gerald van Dijk;
- Daniëlle van Dijk .

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

## 9. Register Datalek meldingen

Om te voldoen aan de verplichtingen van de AVG is er een procedure opgesteld voor de omgang om datalekken te documenteren. Tegelijkertijd is er ook een registratie van datalekken die zich bij Van Dijk Hoogland r hebben voorgedaan. Voor nu is dit nog niet van toepassing, omdat er nooit eerder een datalek heeft plaats gevonden.

We spreken van een datalek wanneer persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens mogen hebben. Wanneer er een datalek heeft plaatsgevonden meldt de gemeente dit zonder onredelijke vertraging, uiterlijk 72 uur nadat er kennis van de inbreuk is vernomen, aan de Autoriteit Persoonsgegevens (AP). Als dit later dan 72 uur is wordt er een motivering voor de vertraging bij de melding gevoegd. Het kan zijn dat de inbreuk een hoog risico met zich meebrengt voor de rechten en vrijheden van de betrokkenen. In dit geval meldt de gemeente dit aan de betrokkenen in eenvoudige en duidelijke taal. Om toekomstige datalekken te voorkomen worden bestaande datalekken geëvalueerd.

## 10. Afspraken met verwerkers

Van Dijk Hoogland heeft samen met diverse partijen een verwerkingsovereenkomst afgesloten. De afspraken met de externe partijen zijn gemaakt, zijn vastgelegd in de verwerkingsovereenkomst, zodat alle persoonsgegevens goed beschermd blijven en alleen verwerkt worden zoals de wet dat voorschrijft.

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. De overeenkomsten zijn in het bezit van de verantwoordelijke(n) voor de gegevensbescherming.

## 11. Data Protection Impact Assessment (DPIA)

In de Nederlandse vertaling van de AVG wordt de term data protection impact assessment (DPIA) gegevensbeschermingseffectbeoordeling genoemd. Met een gegevens beschermingseffectbeoordeling worden de effecten en risico's van nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy. Van Dijk Hoogland 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 organisatie, in tegenstelling tot de rijksoverheid, nu nog niet verplicht zijn een DPIA uit te voeren.

Voor Van Dijk Hoogland 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 Dijk Hoogland gehanteerd en daarmee onderbouwt Van Dijk Hoogland tegelijkertijd dat zij niet genoodzaakt zijn om te voldoen aan een DPIA.

## 12. Privacy by design & default

Om Van Dijk Hoogland 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 Dijk Hoogland worden uitgevoerd.

### **Privacy by design**

De persoonsgegevens worden beschermd door de verantwoordelijke van de gegevensbescherming, dit zijn Gerald van Dijk en Daniëlle van Dijk. 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 Dijk Hoogland wilt bereiken.

## 13. 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.

## 14. Leidende toezichthouder

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



## 15. 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 betrokkenen 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;

## 16. Toestemming

De gegevensverwerking is gebaseerd op toestemming van de betrokkene. De AVG stelt strengere eisen aan de toestemming van betrokkene. Van Dijk Hoogland 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 het 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.