digitale
gesprekscyclus

Verwerkersovereenkomst

versie 1 april 2025

De ondergetekenden:

De organisatie genaamd _____, met rechtsvorm _____,
statutair gevestigd te _____, aan _____,
hierna te noemen: “**Verwerkingsverantwoordelijke**”,

en

De besloten vennootschap met beperkte aansprakelijkheid De Digitale Gesprekscyclus BV, statutair gevestigd te (1901 ZL) Castricum aan Bosakker 5, hierna te noemen: “**Verwerker**”,

hierna gezamenlijk te noemen “**Partijen**”,

Overwegende dat:

1. Verwerker een dienstverlener is met als doel het vereenvoudigen van het proces rondom functioneren, competenties en beoordelen. Verwerker heeft in dit kader Software, zoals hierna gedefinieerd, ontwikkeld waarmee Verwerkingsverantwoordelijke onder andere functioneringsgesprekken kan (laten) vastleggen van medewerkers, dossieropbouw kan bewerkstelligen, etc.;

2. Verwerker met de Verwerkingsverantwoordelijke een Gebruikersovereenkomst, zoals hierna gedefinieerd, heeft gesloten op basis waarvan Verwerkingsverantwoordelijke het recht heeft om de Software te (laten) gebruiken;

3. Als Verwerkingsverantwoordelijke de Software gebruikt of laat gebruiken, Persoonsgegevens, zoals hierna gedefinieerd, worden verwerkt;

4. Verwerkingsverantwoordelijke voor deze gegevensverwerking kwalificeert als Verwerkingsverantwoordelijke in de zin van artikel 4 lid 7 van de Algemene Verordening Gegevensbescherming (Verordening EU 2016/679) (hierna: “AVG”);

5. Als de Verwerkingsverantwoordelijke de Software gebruikt of laat gebruiken, deze Persoonsgegevens dan door Verwerker in opdracht van de Verwerkingsverantwoordelijke met de Software zullen worden verwerkt;

6. Verwerker voor deze gegevensverwerking kwalificeert als Verwerker in de zin van artikel 4 lid 8 van de AVG;

7. Verwerkingsverantwoordelijke in dit kader aan de Verwerker de opdracht wenst te verlenen om namens Verwerkingsverantwoordelijke Persoonsgegevens te verwerken en Verwerker deze opdracht wenst te aanvaarden;

8. Partijen gelet op het bepaalde in artikel 28 AVG nadere afspraken wensen te maken over de voorwaarden waaronder Verwerker de Persoonsgegevens zal verwerken;

9. Partijen in dit kader in deze Overeenkomst, zoals hierna gedefinieerd, de volgende afspraken schriftelijk wensen vast te leggen.

Verklaren te zijn overeengekomen als volgt:

1. Definities

1.1. De volgende in deze Overeenkomst met een hoofdletter geschreven termen, zullen de navolgende betekenissen hebben:

i. **Doel**: het doel of de doelen van de verwerking van Persoonsgegevens, zoals gespecificeerd in **Bijlage I**;

ii. **Gebruikersovereenkomst**: de gebruikersovereenkomst die tussen Verwerkingsverantwoordelijke en Verwerker is gesloten waardoor Verwerkingsverantwoordelijke het recht van Verwerker heeft verkregen om de Software te gebruiken;

iii. **Persoonsgegevens**: gegevens die kunnen worden herleid naar een natuurlijk persoon, zoals bedoeld in artikel 4 lid 1 van de AVG, zoals nader gespecificeerd in **Bijlage I**;

iv. **Overeenkomst**: de onderhavige Verwerkersovereenkomst, inclusief bijlagen;

v. **Software**: de software van Verwerker genaamd De Digitale Gesprekscyclus, ten behoeve van prestatiemanagement en dossieropbouw.

2. Verlening van opdracht tot verwerking persoonsgegevens

2.1. Verwerkingsverantwoordelijke verleent aan Verwerker de opdracht tot het verwerken van Persoonsgegevens. Verwerker aanvaardt deze opdracht;

2.2. Partijen zullen in **Bijlage I - Privacyverklaring** en **Bijlage II - Informatiebeveiligingsbeleid** vastleggen:

i. op welke wijze Verwerkingsverantwoordelijke de Persoonsgegevens aan Verwerker ter beschikking zal stellen;

ii. welke verwerkingshandelingen Verwerker zal uitvoeren ten aanzien van de Persoonsgegevens;

iii. voor welk Doel de verwerking van Persoonsgegevens plaatsvindt;

iv. welke technische en organisatorische beveiligingsmaatregelen Verwerker zal treffen om de Persoonsgegevens te beveiligen tegen verlies en tegen onrechtmatige verwerking.

2.3. Partijen bevestigen dat Verwerkingsverantwoordelijke volledig en als enige verantwoordelijk is voor het vaststellen van het Doel en de middelen voor de verwerking van Persoonsgegevens. De Verwerker verwerkt de persoonsgegevens uitsluitend ten behoeve van de Verwerkingsverantwoordelijke en slechts op diens instructie.

3. Verplichtingen Verwerker

3.1. Verwerker verplicht zich om:

i. alle instructies van Verwerkingsverantwoordelijke in het kader van de verwerking van de Persoonsgegevens op te volgen;

ii. de Persoonsgegevens nimmer aan een derde te verstrekken, dan wel een derde toegang te verlenen tot de Persoonsgegevens, zonder dat Verwerker hiervoor de uitdrukkelijke schriftelijke toestemming heeft verkregen van Verwerkingsverantwoordelijke, behoudens de situaties zoals gedefinieerd in **Bijlage I - Privacyverklaring en Bijlage II - Informatiebeveiligingsbeleid**;

iii. de Persoonsgegevens uitsluitend te verwerken in het kader van het Doel, en de Persoonsgegevens voor geen enkel ander doel te gebruiken of aan te wenden;

iv. bij de verwerking van de Persoonsgegevens zich te houden aan alle toepasselijke wet- en regelgeving met betrekking tot de bescherming van persoonsgegevens, waaronder in ieder geval begrepen de AVG;

v. op eerste verzoek van Verwerkingsverantwoordelijke aan Verwerkingsverantwoordelijke toegang te geven tot de Persoonsgegevens, dan wel de Persoonsgegevens aan Verwerkingsverantwoordelijke tegen redelijke kosten ter beschikking te stellen op een duurzame gegevensdrager, op de wijze en in het format dat Verwerkings-verantwoordelijke wenst.

3.2. Verwerker hanteert de in haar **Informatiebeveiligingsbeleid (Bijlage II)** vermelde beveiligingsmaatregelen waarmee een passend beveiligingsniveau wordt geboden

dat voldoet aan het in artikel 24 AVG vereiste beschermingsniveau. Verwerker zal uit eigen beweging, en op eigen kosten, de in **Informatiebeveiligingsbeleid (Bijlage II)** vermelde beveiligingsmaatregelen zodanig aanpassen dat deze gedurende de duur van deze Overeenkomst een passend beschermingsniveau blijven bieden;

3.3. Verwerker verplicht zich Verwerkingsverantwoordelijke schriftelijk te informeren volgens de procedure zoals genoemd in **Procedure Datalek (Bijlage III)**, indien een onbevoegde beschikking heeft gekregen over (een deel van) de Persoonsgegevens, dan wel (permanent of tijdelijk) toegang daartoe heeft gehad, zo spoedig als redelijkerwijs mogelijk nadat Verwerker kennis heeft gekregen van de onbevoegde toegang;

3.4. Verwerker zal Verwerkingsverantwoordelijke onverwijld in kennis stellen van een bindend verzoek van een bevoegde instantie tot verstrekking van de Persoonsgegevens, tenzij het Verwerker op grond van enige wettelijke verplichting niet is toegestaan de Verwerkingsverantwoordelijke hiervan in kennis te stellen;

3.5. Verwerker verplicht zich Verwerkingsverantwoordelijke in de gelegenheid te stellen te controleren dat de verwerking van de persoonsgegevens plaatsvindt zoals overeengekomen in deze Overeenkomst.

4. Rechten van betrokkene

4.1. Verwerker zal op eerste verzoek van Verwerkingsverantwoordelijke zo spoedig mogelijk, doch uiterlijk binnen vijf werkdagen nadat het verzoek is gedaan, aan Verwerkingsverantwoordelijke schriftelijk alle informatie verstrekken die Verwerkingsverantwoordelijke nodig mocht hebben om te kunnen voldoen aan de in artikel 15 AVG vervatte mededelingsplicht;

4.2. Verwerker zal op eerste verzoek van Verwerkingsverantwoordelijke opgeslagen Persoonsgegevens verbeteren, aanvullen, verwijderen of afschermen. Verwerker zal aan dit verzoek voldoen binnen zodanige termijn dat Verwerkingsverantwoordelijke niet in overtreding is van het bepaalde in artikel 17 lid 1 AVG, doch in elk geval binnen vijf werkdagen nadat het verzoek door Verwerkingsverantwoordelijke is gedaan.

5. Bijstand

5.1. Verwerker verleent Verwerkingsverantwoordelijke bijstand bij het doen nakomen van de op Verwerkingsverantwoordelijke rustende verplichtingen op grond van de AVG en andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens, zoals met betrekking - maar niet beperkt - tot:

a. het - voor zover redelijkerwijs mogelijk - vervullen van de plicht van Verwerkingsverantwoordelijke om aan verzoeken van de in hoofdstuk 3 van de AVG vastgelegde rechten van de betrokkene binnen de wettelijke

termijnen te voldoen, zoals een verzoek om inzage, verbetering, aanvulling, verwijdering of afscherming van Persoonsgegevens;
b. het uitvoeren van audits zoals bedoeld in Artikel 6. van deze Verwerkersovereenkomst;
c. het uitvoeren van een gegevensbeschermingseffectbeoordeling (DPIA) en een eventuele daaruit voortkomende verplichte voorafgaande raadpleging van de Autoriteit Persoonsgegevens;
d. het voldoen aan verzoeken van de Autoriteit Persoonsgegevens of een andere overheidsinstantie;
e. het voorbereiden, beoordelen en melden van datalekken zoals bedoeld in **Bijlage III - Procedure Datalek** van deze Verwerkersovereenkomst.

5.2. Een klacht of verzoek van een Betrokkene of een verzoek of onderzoek van de Autoriteit Persoonsgegevens met betrekking tot de Verwerking van de Persoonsgegevens, wordt door de Verwerker, voor zover wettelijk is toegestaan, onverwijld doorgestuurd naar Verwerkingsverantwoordelijke, die verantwoordelijk is voor de afhandeling van het verzoek.

5.3. Partijen brengen elkaar voor in redelijkheid verleende bijstand geen kosten in rekening. In het geval dat één van de Partijen kosten in rekening wil brengen, brengt deze partij de andere partij hiervan vooraf op de hoogte.

6. Audits

6.1. Verwerkingsverantwoordelijke heeft het recht om audits uit te laten voeren ter controle van naleving op alle punten uit de Overeenkomst en de AVG.

6.2. Partijen spreken in onderling overleg af dat de audit wordt uitgevoerd door een door één van de Partijen, na goedkeuring door de andere Partij, in te schakelen onafhankelijke gecertificeerde externe deskundige die een derdenverklaring (Third Party Memorandum, TPM) afgeeft.

6.3. De auditor verstrekt het auditrapport alleen aan Partijen.

6.4. Partijen maken onderling afspraken over de omgang met de uitkomsten van de audit.

6.5. Partijen kunnen in onderling overleg afspreken dat, aan de hand van een geldige (inter)nationaal erkende certificering of een gelijkwaardig controle- of bewijsmiddel, een reeds uitgevoerde audit en daaruit afgegeven derdenverklaring gebruikt kunnen worden. Verwerkingsverantwoordelijke wordt in dat geval geïnformeerd over de uitkomsten van de audit.

6.6. Partijen komen overeen dat de kosten van een audit als bedoeld in artikel 6.2 voor rekening komen van de Verwerkingsverantwoordelijke, tenzij uit de audit grote gebreken blijken, die aan Verwerker kunnen worden toegerekend. In dat geval treden Partijen in overleg over de verdeling van de kosten van de audit.

7. Duur, wijziging en beëindiging

7.1. Deze Overeenkomst komt tot stand middels ondertekening door Partijen en zal voortduren voor de duur van de Gebruikersovereenkomst en bij gebrek daaraan voor de duur van de verwerking van persoonsgegevens van Verwerkingsverantwoordelijke door Verwerker.

7.2. Verwerker is gerechtigd deze Overeenkomst met onmiddellijke ingang en zonder rechterlijke tussenkomst te ontbinden, of de ontbinding ervan in rechte te vorderen, zonder gehoudenheid tot betaling van (enige vorm van) schadevergoeding of compensatie, indien Verwerkingsverantwoordelijke na een schriftelijke ingebrekestelling waarin een redelijke termijn is gesteld voor zuivering van de tekortkoming, toerekenbaar tekortschiet in de nakoming van een of meerdere verplichtingen uit deze Overeenkomst, de Gebruikersovereenkomst en/of een andere overeenkomst tussen Partijen;

7.3. Verwerker kan de Overeenkomst per direct ontbinden indien Verwerkingsverantwoordelijke op oneigenlijke wijze gebruik maakt van de Software en/of in strijd handelt met hetgeen bepaald in deze Overeenkomst, volledig ter discretie van Verwerker zonder dat daardoor enige schadeplichtigheid van Verwerker, of recht op restitutie van door Verwerkingsverantwoordelijke vooruitbetaalde vergoedingen ontstaat;

7.4. Deze Overeenkomst kan, zonder enige voorafgaande opzegtermijn, en met onmiddellijke ingang, ontbonden worden door Verwerker, vanaf de dag dat:

i. het faillissement van Verwerkingsverantwoordelijke wordt aangevraagd dan wel Verwerkingsverantwoordelijke zelf zijn faillissement aanvraagt;

ii. Verwerkingsverantwoordelijke in staat van faillissement wordt verklaard;

iii. Verwerkingsverantwoordelijke tot boedelafstand overgaat;

iv. tegen de Verwerkingsverantwoordelijke surseance van betaling wordt verleend of een regeling met zijn crediteuren treft;

v. Verwerkingsverantwoordelijke de vrije beschikking over (een substantieel deel van) zijn vermogen verliest, bijvoorbeeld door beslaglegging;

vi. de liquidatie van Verwerkingsverantwoordelijke wordt aangevangen, dan wel een vordering tot ontbinding van Verwerkingsverantwoordelijke wordt ingesteld of een ontbindingsbesluit ten aanzien van Verwerkingsverantwoordelijke wordt genomen, tenzij er sprake is van een rechtsopvolger;

vii. Verwerkingsverantwoordelijke enige uit kracht van de wet op hem rustende verplichting niet of niet geheel nakomt;

viii. Verwerkingsverantwoordelijke zijn betalingsverplichtingen uit hoofde van een overeenkomst, de Gebruikersovereenkomst en/of deze Overeenkomst niet (geheel) nakomt.

7.5. Ontbinding en opzegging van deze Overeenkomst dient schriftelijk te geschieden;

7.6. Een beroep op het recht deze Overeenkomst te ontbinden laat onverlet het recht van de Verwerker op schadevergoeding;

7.7. Beëindiging, ontbinding of opzegging van deze Overeenkomst, op welke grond of wijze dan ook, laat verbintenissen van Verwerkingsverantwoordelijke onverlet welke naar hun aard bedoeld zijn voort te duren na beëindiging, waaronder in ieder geval begrepen geheimhoudingplichten, vrijwaringsplichten, aansprakelijkheidsbepalingen, en bepalingen omtrent toepasselijk recht en jurisdictie.

7.8. Verwerkingsverantwoordelijke en Verwerker treden met elkaar in overleg over wijzigingen in deze Overeenkomst als een wijziging in wet- of regelgeving daartoe aanleiding geeft.

8. Gevolgen beëindiging

8.1. Bij beëindiging, ontbinding of opzegging van deze Overeenkomst, op welke grond of wijze dan ook, zal Verwerker op eigen kosten en uit eigen beweging:

i. per direct de verwerking van de Persoonsgegevens staken;

ii. alle Persoonsgegevens die elektronisch zijn opgeslagen permanent van de gegevensdrager verwijderen, of voor zover permanente verwijdering van de gegevensdrager niet mogelijk is, de gegevensdrager vernietigen;

iii. aan Verwerkingsverantwoordelijke op aanvraag en tegen redelijke kosten alle Persoonsgegevens ter beschikking stellen, op een door Verwerker gekozen wijze;

iv. aan Verwerkingsverantwoordelijke op aanvraag en tegen redelijke kosten alle documenten waarin de Persoonsgegevens zijn vastgelegd ter beschikking stellen;

v. binnen 30 dagen back-ups van de Persoonsgegevens verwijderen.

8.2. Verwerker zal op verzoek van Verwerkingsverantwoordelijke schriftelijk bevestigen aan Verwerkingsverantwoordelijke dat Verwerker aan alle verplichtingen uit hoofde van dit artikel heeft voldaan.

9. Aansprakelijkheid

9.1. Verwerker aanvaardt wettelijke en contractuele verplichtingen tot schadevergoeding slechts voor zover dat uit dit artikel blijkt;

9.2. Verwerker is slechts aansprakelijk jegens Verwerkingsverantwoordelijke:

i. in het geval van een toerekenbare tekortkoming in de nakoming van deze Overeenkomst, waaronder een toerekenbare tekortkoming in de nakoming de verplichtingen van Verwerker, en dan uitsluitend voor vervangende schadevergoeding, dat wil zeggen vergoeding van de waarde van de achterwege gebleven prestatie, of;

ii. in het geval van een aan Verwerker toerekenbare onrechtmatige daad, waarbij schade of lichamelijk letsel aan personen is toegebracht.

9.3. Iedere aansprakelijkheid van Verwerker voor enige andere vorm van schade is uitgesloten, daaronder begrepen aanvullende schadevergoeding in welke vorm dan ook, alsmede vergoeding van indirecte schade of gevolgschade of schade wegens gederfde omzet of winst, boetes die aan Verwerkingsverantwoordelijke worden opgelegd bijvoorbeeld – maar niet uitsluitend – door de Autoriteit Persoonsgegevens, vertragingsschade, schade wegens verlies van gegevens, schade wegens overschrijding van termijnen als gevolg van gewijzigde omstandigheden, diefstal, verlies of beschadiging van data en zaken en schade wegens door Verwerker gegeven inlichtingen of adviezen waarvan de inhoud niet uitdrukkelijk onderdeel van de verplichtingen van Verwerker vormt;

9.4. De hoogte van enige vergoeding, die Verwerker verschuldigd is het in geval van aansprakelijkheid, is gemaximeerd op het bedrag dat door de aansprakelijkheidsverzekeraar van Verwerker in het betreffende geval wordt uitgekeerd, vermeerderd met zijn eigen risico onder die verzekering. Voor zover de verzekeraar in enig geval niet tot uitkering overgaat en/of indien de beperkingen van aansprakelijkheid zoals gesteld in dit artikel om welke reden dan ook (in rechte) geen stand houden, is de aansprakelijkheid van Verwerker voor de totale schade die voortvloeit uit of in verband staat met de overeengekomen werkzaamheden, waaronder in dit verband zowel alle directe als indirecte schade wordt verstaan, alsmede rente, beperkt tot het bedrag dat voor de werkzaamheden in verband waarmee de schade is ontstaan door Verwerkingsverantwoordelijke aan Verwerker is betaald.

9.5. De aansprakelijkheid van Verwerker wegens toerekenbare tekortkoming in de nakoming van deze Overeenkomst ontstaat slechts indien Verwerkingsverantwoordelijke Verwerker onverwijld en deugdelijk schriftelijk in gebreke stelt, stellende daarbij een redelijke termijn ter zuivering van de tekortkoming, en Verwerker ook na die termijn toerekenbaar in de nakoming van zijn verplichtingen tekort blijft schieten. De ingebrekestelling dient een zo gedetailleerd

mogelijke omschrijving van de tekortkoming te bevatten, zodat Verwerker in staat is adequaat te reageren;

9.6. De uitsluiting en beperking van aansprakelijkheid, zoals bedoeld in de voorgaande leden, geldt niet indien en voor zover de schade het gevolg is van opzet of bewuste roekeloosheid van Verwerker of zijn bedrijfsleiding;

9.7. De Verwerker vrijwaart de Verwerkingsverantwoordelijke voor alle aanspraken van derden die uitsluitend het gevolg zijn van een toerekenbare tekortkoming van de Verwerker in de nakoming van zijn verplichtingen onder de AVG of andere toepasselijke wetgeving inzake gegevensbescherming. Voor al het overige vrijwaart de Verwerkingsverantwoordelijke de Verwerker.

9.8. De Software, updates, onderhoud, support en eventuele andere werkzaamheden van Verwerker worden uitdrukkelijk geleverd op basis van een inspanningsverbintenis.

10. Geheimhouding

10.1. Partijen zullen geen product-, markt- en bedrijfsgegevens over elkaar aan derden kenbaar maken tenzij daar door de andere Partij schriftelijk toestemming voor is gegeven.

11. Overig

11.1. Wijziging van deze Overeenkomst of aanvullingen daarop zijn slechts geldig indien deze schriftelijk zijn overeengekomen;

11.2. Indien een bepaling van deze Overeenkomst nietig, vernietigbaar, of anderszins onafdwingbaar is of wordt, dan blijven de overige bepalingen van deze Overeenkomst volledig van kracht. Partijen zullen in dat geval te goeder trouw in onderhandeling treden om de nietige, vernietigbare, of anderszins onafdwingbare bepaling te vervangen door een uitvoerbare alternatieve bepaling, waarbij Partijen zoveel mogelijk rekening zullen houden met het doel en strekking van de nietige, vernietigde of anderszins niet afdwingbare bepaling;

11.3. Deze Overeenkomst verwoordt de enige afspraken tussen Partijen ter zake van betreffende de verwerking van Persoonsgegevens door Verwerker en vervangt alle voorgaande schriftelijke dan wel mondelinge afspraken en correspondentie.

12. Toepasselijk recht en jurisdictie

12.1. Op deze Overeenkomst, alsmede op de hieruit voortvloeiende of hiermee samenhangende overeenkomsten en overige rechtshandelingen, is uitsluitend het Nederlandse recht van toepassing;

12.2. Alle geschillen, waaronder mede begrepen die welke slechts door één partij als zodanig worden beschouwd, welke voortvloeien uit of verband houden met (de uitvoering van) deze Overeenkomst en/of met de hieruit voortvloeiende of hiermee samenhangende overeenkomsten, alsmede overige rechtshandelingen, welke niet in der minne kunnen worden opgelost, zullen worden beslecht door de bevoegde rechterlijke instantie in Amsterdam.

Aldus ondertekend op _____ te _____,

Verwerkingsverantwoordelijke

_____

Organisatie: _____

Naam: _____

Verwerker

De Digitale Gesprekscyclus BV

Naam: Daniel Hoopman

Bijlage I - Privacyverklaring

De Digitale Gesprekscyclus respecteert uw privacy en al uw gegevens worden vertrouwelijk behandeld. De verwerking van persoonsgegevens geschiedt altijd op een manier die in overeenstemming is met de eisen die de Algemene Verordening Gegevensbescherming (Verordening EU 2016/679, hierna AVG) en eventuele andere wet- en regelgeving daaraan stelt. In deze Privacyverklaring wordt in meer detail uiteengezet hoe De Digitale Gesprekscyclus met dergelijke gegevens omgaat.

Deze privacyverklaring is opgedeeld in een algemeen deel, een deel voor klanten met betrekking tot de applicatie van De Digitale Gesprekscyclus, een deel voor het gebruik van de website van De Digitale Gesprekscyclus en een deel voor de digitale nieuwsbrief.

Algemeen

Voor het leveren van ons product en bijbehorende diensten aan klanten verwerken wij persoonsgegevens. Deze verwerken we in onze eigen software en die van onze partners. Wij verkopen of verstrekken uw gegevens nooit aan derde partijen. We zullen uw gegevens alleen delen:

- Om op uw verzoek diensten of producten leveren;
- In geval van (juridisch) onderzoek bij illegale activiteiten, veronderstelde fraude, mogelijke bedreiging van fysieke veiligheid en welzijn van andere personen, schending van de Algemene Voorwaarden, of als DDGC hierom wordt verzocht door een rechtbank;
- In geval van een overname door of samenvoeging met een ander bedrijf. In dit geval wordt u hiervan tijdig op de hoogte gesteld voordat dit aan de orde is.

Gegevens van De Digitale Gesprekscyclus

De Digitale Gesprekscyclus B.V.
Bosakker 5
1901 ZL Castricum
KvK-nummer: 57628955
Telefoon: +31 (0)75 - 670 2715
E-mail: support@ddgc.nl

Hierna wordt aan De Digitale Gesprekscyclus gerefereerd als “DDGC”.

De software van DDGC

Gebruikers

Van gebruikers in de Software worden Persoonsgegevens verwerkt. De Software bevat verschillende typen gebruikers, die allen op een eigen wijze van de Software gebruik kunnen maken of wiens gegevens om andere redenen in de Software beschikbaar zijn. De verschillende categorieën gebruikers zijn:

1. organisatiebeheerders;
2. leidinggevenden;
3. medewerkers;
4. externen.

Doelen van de gegevensverwerking

Verwerker verwerkt in opdracht van de Verwerkingsverantwoordelijke Persoonsgegevens van gebruikers voor één doel:

1. Functioneren van de software

Verwerker verwerkt Persoonsgegevens zodat de gebruikers kunnen inloggen op de software en derhalve met de software kunnen werken. Dat betekent concreet, afhankelijk van het type gebruiker, dat er functioneringsgesprekken kunnen worden vastgelegd, dat er competentieprofielen kunnen worden ingevuld en dat account- en gebruikersgegevens kunnen worden aangepast.

Van de gebruikers worden de volgende gegevens verwerkt. Gegevens gemarkeerd met een * zijn verplicht, andere gegevens zijn optioneel.

- Aanhef *
- Voornaam *
- Tussenvoegsel
- Achternaam *
- Taalvoorkeur *
- E-mail *
- Gebruikersnaam *
- Organisatiedeel *

- Functie
- Leidinggevende van
- Foto(bestand)
- Bestand kiezen
- Telefoonnummer
- Mobiel nummer
- Datum in dienst
- Personeelsnummer
- Geboortedatum
- Straat of postbus
- Huisnummer
- Postcode
- Stad
- Provincie en land
- Door verwerkingsverantwoordelijke vastgelegde gegevens rondom functioneren, beoordeling, persoonlijke ontwikkeling, competenties, etc.

Externe personen in applicatie

In de Software kunnen medewerkers of leidinggevenden van Verwerkingsverantwoordelijke een e-mail sturen naar externe personen die niet in de Software geregistreerd staan. Van deze personen worden de volgende gegevens verwerkt:

- E-mailadres externe voor uitnodigen 360°-feedback;
- Observaties m.b.t. tot het functioneren van de beoordeelde gebruiker (360°-feedback).

Wijze van ter beschikking stellen en verwerkingshandelingen

De Verwerkingsverantwoordelijke zal de Persoonsgegevens ter beschikking stellen aan Verwerker door de Software te gebruiken. De Software biedt in dit kader de mogelijkheid om via een web-interface (beschikbaar op elk apparaat zoals een computer, laptop of iPad) gegevens in te voeren die vervolgens via de Software door de Verwerker worden verwerkt.

Verwerker kan ook in opdracht een databestand van Verwerkingsverantwoordelijke importeren. Dit databestand zal door Verwerkingsverantwoordelijke worden aangeleverd op een door Verwerker gespecificeerde wijze.

Verwerker kan tevens in opdracht van Verwerkingsverantwoordelijke bepaalde gegevens aanpassen. Dergelijke verzoeken zullen per e-mail of telefonisch door Verwerkingsverantwoordelijke aan Verwerker worden doorgegeven.

De Verwerker zal de Persoonsgegevens opslaan in een database en op haar server. Verwerkingsverantwoordelijke kan zelf Persoonsgegevens verwijderen binnen de Software.

Geen doorgifte van persoonsgegevens

Verwerker zal Persoonsgegevens nooit doorgeven, verkopen en/of anderszins verstrekken aan derden, behalve in de volgende gevallen aan de volgende partijen:

- Aan derden die noodzakelijke (technische) diensten verlenen aan Verwerker ten behoeve van de werking van de Software. Zie Bijlage II - Informatiebeveiligingsbeleid voor een overzicht van Subverwerkers.
- Voor het maken van back-ups. Het hele systeem van Verwerker, en dus ook Persoonsgegevens, wordt dagelijks geback-upt op een server van Amazon in Europa;
- Aan bedrijven die Verwerker (deels) overnemen, waarmee Verwerker fuseert en/of anderszins de rechtsopvolgers van Verwerker zijn;
- Aan overheidsinstanties, indien de wet dat vereist en/of uit hoofde van een verzoek en/of bevoegd gegeven bevel van een overheidsinstantie.

Dit onderdeel beschrijft de gegevensverwerkingen binnen de software van DDGC (bereikbaar via onder andere https://app.ddgc.nl).

Administratie

DDGC verwerkt (persoons)gegevens van u als klant. Als klant van DDGC krijgt u een gebruiksrecht op de software. Om deze gebruikersovereenkomst na te komen en om bepaalde administratieve handelingen te kunnen verrichten (financiële administratie en facturatie), alsmede om u op de hoogte te houden van de laatste ontwikkelingen omtrent DDGC, heeft DDGC een aantal gegevens van u nodig. In dit kader verwerkt DDGC de volgende gegevens:

- Aanhef;
- Voornaam;
- Tussenvoegsel;
- Achternaam;
- E-mailadres.

Logging

Tijdens het gebruik van de software worden door DDGC ook bepaalde gegevens verzameld met o.a. Google Analytics en Sentry. Het gaat hier om gegevens die vereist zijn voor de dienstverlening van DDGC. Deze gegevens kunnen door DDGC gebruikt worden als er bijvoorbeeld klachten zijn over de verbinding. Afhankelijk van de activiteit die u met de software verricht, verwerkt DDGC in dit kader de volgende gegevens:

- IP-adres;
- Loginnaam of klantnummer;
- Tijdstip van handelingen in de software.

Rol DDGC

DDGC verwerkt gegevens van haar klanten en is voor die gegevensverwerkingen **Verwerkingsverantwoordelijke** in de zin van de AVG.

De klanten van DDGC zullen met de software op hun beurt persoonsgegevens gaan verwerken van gebruikers. In deze relatie is De Digitale Gesprekscyclus de Verwerker van de persoonsgegevens in de zin van de AVG. Dat betekent dat DDGC in opdracht en op instructie van zijn klant persoonsgegevens verwerkt. De klanten van DDGC dienen dan ook te worden aangemerkt als Verwerkingsverantwoordelijke voor deze gegevensverwerkingen in de zin van de AVG. Klanten hanteren een eigen privacybeleid waar DDGC niet verantwoordelijk voor is.

Recht op inzage, verbetering of verwijdering

Zoals hiervoor beschreven is DDGC ten opzichte van de gebruikers van de software niet de Verwerkingsverantwoordelijke voor de gegevensverwerkingen in de zin van de AVG. Verzoeken om inzage, correctie of verwijdering kunnen om die reden dan ook niet door DDGC zelfstandig worden afgehandeld. Verzoeken om inzage, correctie of verwijdering dienen te worden ingediend bij de klant van DDGC die gebruik maakt van de diensten en software van DDGC.

De commerciële Website van DDGC

Dit onderdeel beschrijft de gegevensverwerking binnen de website van DDGC, te bereiken via: https://ddgc.nl.

Google Analytics

Op de website van DDGC wordt gebruik gemaakt van Google Analytics om te meten hoe vaak en op welke wijze de website wordt bezocht. Om deze meting te verrichten zal Google bepaalde informatie, zoals uw IP-adres, opslaan op haar servers in de Verenigde Staten. De privacyverklaring van Google kan (onder andere) op http://www.google.com/intl/nl/policies/privacy/ worden geraadpleegd. DDGC heeft Google in dit kader niet toegestaan om de verkregen informatie voor andere doeleinden te gebruiken dan voor de dienstverlening aan DDGC.

Social Media

De inhoud van sommige pagina's binnen de website van DDGC kan worden gedeeld via Facebook, LinkedIn en X (voorheen Twitter). Bij het delen slaan deze platformen cookies op op uw computer. Facebook, LinkedIn en X kunnen in dit geval tevens persoonsgegevens van u verwerken. Om na te gaan wat Facebook en X met deze gegevens kunnen doen, kunnen de respectievelijke

privacyverklaringen van X en Facebook worden geraadpleegd. DDGC heeft hier geen invloed op en draagt hiervoor geen verantwoordelijkheid.

Cookies

Zowel door de website als in de software wordt gebruikgemaakt van technische en functionele cookies. Een cookie is een klein tekstbestand dat door de browser op uw computer, smartphone of tablet wordt geplaatst. DDGC gebruikt cookies om uw instellingen en voorkeuren te onthouden en daarmee uw gebruiksgemak te verhogen.

DDGC maakt ook gebruik van de advertentiedienst van Google (Google Adwords). Google Adwords kan een cookie op uw computer plaatsen. DDGC vraagt u hiervoor om toestemming op het moment dat u de website van DDGC bezoekt. U kunt in uw browser instellen dat u geen cookies wenst op te slaan op uw computer en u kunt eerder opgeslagen cookies ook verwijderen. U leest meer over dit proces op http://www.consumentenbond.nl/internet-privacy/extra/cookies-verwijderen/.

Digitale nieuwsbrief

DDGC stuurt regelmatig een nieuwsbrief per e-mail naar klanten en prospects waarin wordt geïnformeerd over nieuws over DDGC en aanverwante zaken. DDGC voegt u slechts toe aan het nieuwsbriefbestand als u daarvoor expliciet toestemming heeft gegeven of wanneer u klant wordt van DDGC. Het gaat om de volgende gegevens:

- Aanhef;
- Voornaam;
- Achternaam;
- E-mailadres.

Iedere nieuwsbrief bevat een link waarmee u zich kunt afmelden. Voor meer informatie over het privacybeleid van deze software kunt u terecht op:
https://meetmarigold.com/privacy-notices/#services-notice

Relatiebeheersoftware

Ter ondersteuning van onze werkprocessen voor sales en support maakt DDGC gebruik van relatiebeheersoftware om correspondentie met klanten en prospects te bewaren. Op deze wijze kunnen onze accountmanagers en supportmedewerkers u beter van dienst zijn. Het gaat hierbij om de volgende gegevens:

- Aanhef;
- Voornaam;

- Achternaam;
- E-mailadres;
- Telefoonnummer;
- Organisatie;
- Correspondentie.

Voor meer informatie over het privacybeleid van deze software kunt u terecht op: https://37signals.com/policies/privacy.

Bijlage II - Informatiebeveiligingsbeleid (IBB)

De veiligheid van de software die De Digitale Gesprekscyclus BV (hierna: DDGC) aanbiedt, staat hoog in het vaandel. We hebben daarom een Informatiebeveiligingsbeleid (IBB) met procedures en protocollen opgesteld. Op deze manier is zowel intern als voor voor klanten helder hoe gehandeld dient te worden in verschillende situaties. Het IBB is een formeel beleidsdocument dat tweemaal per jaar wordt herzien en aangevuld.

Risico Management Team

Binnen de organisatie van De Digitale Gesprekscyclus is een Risico Management Team verantwoordelijk voor de uitvoer van het Risico Management Programma (RMP) en het beheren van alle documenten zoals genoemd in de Leeswijzer. Het Risico Management Team bestaat uit:

- **Data Protection Officer** (DPO) – Marten Wilmink
  Verantwoordelijk voor het Risico Management Programma en voorzitter RMT;
- **Directeur De Digitale Gesprekscyclus** – Daniel Hoopman
  Verantwoordelijk voor De Digitale Gesprekscyclus BV;
- **Privacy Officer** (indien noodzakelijk) – Extern
  Juridisch adviseur wet- en regelgeving op het gebied van privacy en IT.

Risico Management Programma

De Digitale Gesprekscyclus heeft voor het beheersen van haar Informatiebeveiligingsbeleid een Risico Management Programma (RMP) ingericht dat wordt uitgevoerd door het Risico Management Team (RMT). Dit team bestaat uit de Data Protection Officer en Directeur DDGC en komt iedere zes maanden bijeen voor:

- Analyse van risico's voor privacy en veiligheid binnen bedrijfsprocessen en uitvoering;
- Evaluatie van eerder geïmplementeerde verbetermaatregelen en voorstel van eventuele aanpassingen;
- Opstellen concrete actiepunten en verbetermaatregelen voor nieuwe en bestaande risico's;
- Verslaglegging (verantwoordelijkheid DPO);

De aanpak van risico's binnen het RMP is gebaseerd op de Plan-Do-Check-Act-cyclus. Dit betekent dat continu wordt gekeken naar optimalisatie van processen en beleid op het gebied van veiligheid, ontwikkeling en risico's:

- **Plan** – Analyse beveiligingsrisico's, vaststellen prioriteit en ontwerpplan van aanpak voor optimalisatie.
- **Do** - Uitvoering geplande optimalisatie;
- **Check** - Evaluatie resultaat van de optimalisatie;
- **Act** - Bijstellen aan de hand van de gevonden resultaten bij Check.

Interne documenten

- **Calamiteitenplan** – Intern document met beleid en beschrijving van de procedures bij diverse calamiteiten zoals een storing, diefstal, datalek, nalatigheid of uitval;
- **Risico Instructie** – Instructie voor medewerkers en partners van DDGC met beschrijving van mogelijke gevaren en risico's van het werken met gevoelige gegevens en een beschrijving van de verantwoordelijkheden, functies en taken van de verschillende personen binnen de organisatie;

Human Resources

Alle medewerkers en partners van DDGC worden gescreend alvorens ze in dienst treden bij DDGC op basis van een Verklaring Omtrent het Gedrag (VOG) en een identificatieplicht. Deze screening zal periodiek worden uitgevoerd. Voor alle medewerkers geldt een geheimhoudingsverklaring als onderdeel van de arbeidsovereenkomst. Medewerkers betrachten strikte geheimhouding van informatie van of over klanten of andere gevoelige gegevens tegenover derden.

Nieuwe medewerkers van DDGC en externe partijen die met gevoelige informatie van DDGC werken, tekenen een geheimhoudingsverklaring waarin ze bevestigen dat ze de **Informatiebeveiligingstraining** (IBT), de **Risico Instructie**, het **Calamiteitenplan** en de **Procedure Datalek** die DDGC voorlegt bij indiensttreding, hebben gelezen en begrepen. De IBT bevat een overzicht van de verantwoordelijkheden die medewerkers aangaan bij indiensttreding en de bewustwording van de mogelijke consequenties van nalatigheid of bepaalde beslissingen.

Alle documenten binnen het Informatiebeveiligingsbeleid worden jaarlijks bijgewerkt als onderdeel van het Risico Management Programma. Medewerkers en externen worden vervolgens van de aanpassingen op de hoogte gesteld. Het opfrissen van de informatie uit de IBT, het Calamiteitenplan en de Procedure Datalek is een vast onderdeel tijdens de jaarlijkse beoordelingscyclus van DDGC met haar medewerkers en wordt als dusdanig ook vastgelegd in het gespreksverslag.

Logische toegang

De Data Protection Officer is verantwoordelijk voor het beheer van de logische toegang tot belangrijke gegevens met betrekking tot de applicatie. Hier valt te denken aan toegangscodes, sleutels en wachtwoorden voor servers, software en databases.

De logische toegang voor de verschillende onderdelen van de organisatie, zoals de software, de servers, het CRM, diverse social mediakanalen en de website zijn vastgelegd in wachtwoord software met aparte kluizen voor verschillende niveaus en onderdelen, waarvan toegang wordt verleend aan

individuen op een ‘need-to-know’ basis. De directeur van DDCC is verantwoordelijk voor de fysieke toegang tot panden, het sleutelbeleid en de alarminstallatie.

Tweemaal per jaar of indien noodzakelijk geacht (in geval van bijvoorbeeld vertrek van een teamlid), wordt de logische toegang als onderdeel van het PDCA van alle medewerkers en betrokkenen geëvalueerd en waar nodig bijgesteld. Indien gewenst kan een overzicht worden gegeven van alle personen met logische toegang.

Privacy

Met betrekking tot de privacy van gebruikers en de verwerking van gegevens is een apart **Privacybeleid** opgesteld. Deze is te vinden op de website van DDGC (https://ddgc.nl/algemeen/privacy). Klanten van DDGC zijn wettelijk verplicht om in hun rol als Verwerkingsverantwoordelijke, zoals gedefinieerd in de Algemene Verordening Gegevensbescherming (Verordening EU 2016/679) (hierna: “AVG”), een verwerkersovereenkomst aan te gaan met de Verwerker van persoonsgegevens, in dit geval DDGC. DDGC biedt hiervoor een Verwerkersovereenkomst aan die ondertekend kan worden om aan deze plicht te voldoen. In deze Verwerkersovereenkomst worden de persoonsgegevens beschreven die worden verwerkt in opdracht van de Verwerkingsverantwoordelijke.

Datalek

In geval van een datalek treedt de Procedure Datalek in werking en zal de aangestelde Data Protection Officer (DPO) binnen één werkdag melding maken aan de Verwerkingsverantwoordelijke over de aard, omvang en impact van het betreffende incident. Tevens zal binnen twee dagen melding nadat de verantwoordelijke persoon binnen DDGC er kennis van heeft genomen, het incident bij de Autoriteit Persoonsgegevens gemeld worden. Lees voor meer informatie over dit onderwerp het document **Procedure Datalek**. Dit document is toegevoegd als Bijlage III aan deze Verwerkersovereenkomst.

Subverwerkers

Verwerkingsverantwoordelijke geeft Verwerker door ondertekening van de Verwerkersovereenkomst een algemene schriftelijke toestemming voor het inschakelen van een Subverwerker. Verwerker heeft het recht gebruik te gaan maken van andere Subverwerkers, mits daarvan voorafgaand mededeling wordt gedaan aan Verwerkingsverantwoordelijke, en Verwerkingsverantwoordelijke daartegen bezwaar kan maken binnen een redelijke periode. Verwerker maakt ten tijde van het afsluiten van de Verwerkersovereenkomst gebruik van onderstaande leveranciers als Subverwerkers voor haar dienstverlening.

DDGC maakt gebruik van een Subverwerker buiten de Europese Economische Ruimte (EER) en draagt zodoende persoonlijke gegevens over buiten de EER. DDGC verbindt zich ertoe altijd de Standaard Contractuele Clausules (SCC's) aan te gaan wanneer er een overdracht van gegevens

plaatsvindt buiten de EER, om ervoor te zorgen dat het niveau van gegevensbescherming in overeenstemming is met de vereisten van de Algemene Verordening Gegevensbescherming (AVG).

Naam	Locatie	Beschrijving	Privacy
ActiveCollab	EU	Interne communicatie	GDPR
Amazon Web Services	EU	Hosting software en database	DPA
Campaign Monitor (Marigold)	AU	E-mail service	DPA
CookieFirst	EU	Cookie consent platform	DPA
Freshworks	US	Uptime monitoring	DPA
GitLab	US	Code repository	DPA
Google Ads	US	Advertenties	DPT
Google Analytics	US	Bezoekersgedrag	DPT
Google Workspace	US	Interne/externe communicatie	CDPA
Highrise (37signals)	US	CRM	DPA
Microsoft 365	US	Interne/externe communicatie	DPA
MODxCloud	EU	Web hosting	DPA
Sentry	US	Exception logging	DPA
Slack	US	Interne communicatie	DPA
Twilio	US	2-factor authenticatie	DPA
Vimeo	US	Video hosting	DTA
WeFact	EU	Facturatie	DPA
Zapier	US	Automation	DPA

Ontwikkeling

Bij het ontwikkelen van de software voor DDGC is veiligheid en bescherming van de (persoons)gegevens één van de belangrijkste pijlers. Naast het continu testen van de software door ontwikkelaars en testers, worden ook de best practices aangehouden op het gebied van veilige software. Het bijwerken en updaten van alle gebruikte software, frameworks en modules naar de meest recente versies is hiervan een belangrijk onderdeel.

Bij aanpassingen van de software of serverconfiguratie wordt een impactanalyse uitgevoerd. Concreet worden alle wijzigingen op een acceptatieomgeving die identiek is aan de productieomgeving getest. De software wordt op de acceptatieomgeving softwarematig en handmatig getest om de werking te controleren en de impact van aanpassingen of upgrades op andere onderdelen binnen de software te analyseren. Updates worden volgens het **Releasebeleid** van DDGC uitgevoerd. Onderdeel van dit beleid is de communicatie richting gebruikers voor en na geplande update.

- **TechNative BV** (technative.nl), Amersfoort (NL)
  Hosting management, technische support, beheer
- **CodeSeed** (codeseed.gr), Athene (GR)
  Software architectuur en ontwikkeling, technische support
- **Dinfini** (dinfini.nl), Hengelo (NL)
  Software architectuur en ontwikkeling, technische support

Hosting

De software van Verwerker wordt gehost in moderne datacenters in Frankfurt en Ierland dat wordt geëxploiteerd door Amazon Web Services (AWS). De bestanden van gebruikers worden opgeslagen via de Simple Storage Service (S3) van Amazon. Persoonsgegevens in de database zullen worden opgeslagen op servers in Frankfurt en Ierland en zullen niet worden gekopieerd of verplaatst naar servers in landen waar een minder streng privacy-regime heerst dan in Europa.

Amazon is een bedrijf dat gevestigd is in de Verenigde Staten, echter Amazon garandeert dat persoonsgegevens die in Europa worden opgeslagen nooit naar de Verenigde Staten worden getransporteerd, tenzij zij daartoe wettelijk verplicht is.

Mochten er toch persoonsgegevens naar de Verenigde Staten worden getransporteerd, dan garandeert Amazon dat op die gegevensverwerking in de Verenigde Staten hetzelfde strenge privacy-regime van toepassing is als in Europa. Om deze garantie te kunnen bieden is Verwerker met Amazon een overeenkomst aangegaan (AWS Data Processing Addendum) die Amazon heeft laten goedkeuren door de Europese privacy toezichthouders.

Back-up

Verwerker slaat back-upgegevens op op servers van Amazon. Daartoe gebruikt Verwerker het datacentrum van Amazon in Ierland. Via de volgende link is na te lezen hoe Amazon de bescherming van persoonsgegevens garandeert: https://aws.amazon.com/compliance/data-privacy-faq/

Beveiligingsmaatregelen

Verwerker neemt de bescherming van de Persoonsgegevens zeer serieus en neemt passende maatregelen om misbruik, verlies, onbevoegde toegang, ongewenste openbaarmaking en ongeoorloofde wijziging tegen te gaan. Verwerker implementeert daartoe de volgende maatregelen met betrekking tot de software en infrastructuur:

- **Beveiligingssoftware**: virusscanner en firewall;
- **TLS (voorheen SSL)**: Verwerker verstuurt Persoonsgegevens (en alle andere gegevens) via een beveiligde internetverbinding;
- **DKIM, SPF en DMARC**: zijn internetstandaarden die Verwerker gebruikt om e-mailverkeer van DDGC te authenticeren ter voorkoming van misbruik en spam..

Certificering

Amazon AWS is ISO-27001 gecertificeerde hostingpartij die hiermee voldoet aan de beste praktijken en standaarden met betrekking tot informatiebeveiliging en controle. De Digitale Gesprekscyclus houdt een eigen beveiligingsbeleid aan waarbij tijd wordt besteed aan het up-to-date blijven met de praktijk. DDGC richt zich op het goed op orde hebben van de software en optimalisatie van de software om haar klanten en gebruikers zo goed mogelijk van dienst te kunnen zijn. Met alle beveiligingsmaatregelen en vertrouwde hosting partners voldoet Verwerker aan alle gangbare normen en voor beveiliging.

Bedrijfscontinuïteit

Voor het borgen van de bedrijfscontinuïteit is met een partner een proces ingericht waarin jaarlijks broncode, access en maintenance checks worden uitgevoerd. In het geval van faillissement of ongevallen, zal de applicatie drie maanden volgens de gebruikelijke standaarden blijven werken. Hierin is het waarborgen van data ons grootste belang. Het advies aan klanten is ook om met enige regelmaat zelf exports van gegevens te maken uit de applicatie. Indien klanten een Escrow-certificaat willen ontvangen en dit proces in gang willen zetten, dan is dat tegen vergoeding mogelijk.

Bijlage III - Procedure Datalek

De Digitale Gesprekscyclus respecteert uw privacy en al uw gegevens worden vertrouwelijk behandeld. De verwerking van persoonsgegevens geschiedt altijd op een manier die in overeenstemming is met de eisen die de Algemene Verordening Gegevensbescherming (Verordening EU 2016/679, hierna AVG) en eventuele andere wet- en regelgeving daaraan stelt. In deze Procedure Datalek wordt in meer detail uiteengezet hoe De Digitale Gesprekscyclus in onverhoopt geval met het verlies van dergelijke gegevens omgaat.

Dit document beschrijft de verschillende stappen die binnen DDGC genomen worden bij een datalek, die valt onder de Meldplicht Datalekken. De Meldplicht Datalekken is een wijziging van de Wet Bescherming Persoonsgegevens en is met ingang van 1 januari 2016 in werking getreden. Bij een datalek is er sprake van een inbreuk op de beveiliging van persoonsgegevens (als bedoeld in artikel 33 van de AVG). De persoonsgegevens zijn dan blootgesteld aan verlies of onrechtmatige verwerking. Een datalek moet onverwijld (binnen 2 dagen) nadat de verantwoordelijke persoon binnen DDGC er kennis van heeft genomen, bij de Autoriteit Persoonsgegevens (AP) gemeld worden.

Het datalek moet ook worden gemeld bij de betrokkenen. In het geval van DDGC zijn dit over het algemeen klanten (gebruikers van de software) of medewerkers. Betrokkenen zijn degenen wiens persoonsgegevens zijn betrokken bij een inbreuk. De betrokkene moet onverwijld in kennis worden gesteld van de inbreuk, indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor zijn persoonlijke levenssfeer.

De Verwerker is verplicht om een datalek te melden bij de Verwerkingsverantwoordelijke.

1. **Verwerkingsverantwoordelijke (klant DDGC)** - De Verwerkingsverantwoordelijke heeft zeggenschap over doel en wijze van verwerking. Formeel, juridisch en feitelijk (functioneel) degene die het doel en de middelen voor de verwerking van persoonsgegevens vaststelt. Degene die zeggenschap heeft en verantwoordelijk is over doel en middelen van verwerking en beslist over bewaartermijnen, verstrekking inzageverzoeken etc. De Verwerkingsverantwoordelijke heeft de regierol (regie over het beheer van privacy in de keten), zoals staat beschreven in de Algemene Verordening Gegevensbescherming (Verordening EU 2016/679) (hierna: “AVG);
2. **Verwerker (De Digitale Gesprekscyclus BV)** - De organisatie die de gegevens ten behoeve van de Verwerkingsverantwoordelijke verwerkt zonder aan zijn of haar rechtstreeks gezag te zijn onderworpen. De Verwerker verwerkt persoonsgegevens overeenkomstig de instructies en uiteindelijke verantwoordelijkheid van de Verwerkingsverantwoordelijke. De Verwerker neemt geen beslissingen over het gebruik van de gegevens, de verstrekking aan derden en andere ontvangers, de duur van de opslag van de gegevens, zoals tevens staat beschreven

in de tussen Verwerkingsverantwoordelijke en Verwerker overeengekomen Bewerkersovereenkomst.

Mogelijke oorzaken van een datalek:

- moedwillig handelen (cybercriminaliteit, hacking, identiteitsfraude, malware);
- technisch falen (fouten of bugs in software, verlate updates, storingen);
- menselijk falen (onzorgvuldige omgang gebruikersnaam of wachtwoord, nalatigheid);
- verloren of gestolen hardware (externe harde schijf, USB stick, server-apparatuur of laptop);
- verzenden e-mail naar meerdere gebruikers met openbaring van e-mailadressen;
- calamiteit (brand datacentrum, wateroverlast).

Melding

Alle datalekken van persoonsgegevens moeten intern worden gemeld en worden gedocumenteerd door de Data Protection Officer (DPO). De melding kan door iedere gebruiker en iedere medewerker of derde partij worden gedaan. De melding kan ook door een externe persoon worden gedaan bij een medewerker van DDGC. De melding moet direct en telefonisch worden gedaan bij de DPO en schriftelijk worden vastgelegd. Deze meldt het datalek zo nodig bij de Autoriteit Persoonsgegevens.

De Data Protection Officer legt vast:

- naam van de melder;
- de contactpersoon voor de melding;
- datum en tijd van de melding;
- aard van de inbreuk en risico op verlies of onrechtmatig gebruik gegevens;
- welke persoonsgegevens vallen onder de melding;
- om welk aantal gegevensrecords gaat het;
- welke (groepen) personen zijn betrokken bij de melding;
- welke maatregelen zijn of worden door de melder getroffen;
- welke gevolgen zijn er volgens de melder voor de betrokkenen.

Escalatie bij afwezigheid

Bij afwezigheid van de Data Protection Officer wordt diens rol ingevuld door de directeur DDGC. Als deze ook afwezig is, wordt diens rol ingevuld door de Privacy Officer. Buiten kantoortijden en in het weekend wordt de melding gedaan bij de DPO. Bij het niet kunnen bereiken van de DPO, wordt de melding gedaan bij de directeur DDGC.

Analyse

De Data Protection Officer en de Privacy Officer beoordelen of van de inbreuk ‘redelijkerwijs kan worden aangenomen dat die leidt tot een aanmerkelijk risico op verlies of onrechtmatige verwerking, waaraan nadelige gevolgen voor de privacy van de betrokkenen zijn verbonden’. Is dit niet het geval, dan vindt alleen registratie van de melding plaats door de DPO.

Is dit wel het geval, dan voert de DPO de acties uit zoals beschreven in het Calamiteitenplan van DDGC:

1. Telefonisch informeren directeur DDGC;
2. Tijdens kantooruren onmiddellijk bijeenroepen van het Responseteam Datalek, bestaande uit:
    a. **Data Protection Officer (DPO)** – Marten Wilmink
    Verantwoordelijk voor het Risico Management Programma en voorzitter RMT;
    b. **Directeur De Digitale Gesprekscyclus** – Daniel Hoopman
    Verantwoordelijk voor De Digitale Gesprekscyclus BV;
    c. **Privacy Officer** (indien noodzakelijk) – Extern
    Juridisch adviseur wet- en regelgeving op het gebied van privacy en IT.

De DPO neemt overdag telefonisch contact op met de Privacy Officer. Als het mogelijk is, wordt een eventueel benodigd overleg uitgesteld tot tijdens kantooruren. Als dit niet mogelijk is, wordt zo veel als mogelijk telefonisch en elektronisch overleg gevoerd.

Response Team Datalek

Het Response Team Datalek wordt met hoge prioriteit bijeengeroepen door de DPO. De bijeenkomst wordt voorgezeten door de DPO. Het response team bespreekt en legt vast:

- De gegevens die door de DPO zijn vastgelegd bij het aannemen van de melding;
- De noodzakelijke vervolgacties met betrekking tot het datalek (lek dichten, toegang tot informatie beperken en tegelijkertijd meer informatie vergaren over de indringer);
- De melding die opgesteld moet worden voor de Autoriteit Persoonsgegevens door de DPO. Naast aard inbreuk, welke persoonsgegevens, aantal betrokken personen/records:
    - De mogelijke gevolgen voor de betrokkenen;
    - De maatregelen die DDGC neemt en/of kan nemen om de schade voor betrokkenen te verkleinen;
    - De maatregelen die betrokkenen kunnen nemen om verdere schade te verkleinen, inclusief de wijze van inlichten hierover;
    - Contactgegevens voor betrokkenen.
- De wijze van afhandeling intern, inclusief communicatie naar melder, betreffende afdeling(-en) en manager(s);
- Of er sprake is van eigen aansprakelijkheid, of aansprakelijkheid van derden, zoals uit hoofde van wanprestatie (omdat een geheimhoudingsverplichting is geschonden, of in strijd met een

contractuele verplichting onvoldoende beveiliging is gerealiseerd), of een onrechtmatige daad;
- Of het al dan niet doen van aangifte en vaststellen of sprake is van strafrechtelijke verwijtbaarheid. Dit kan bijvoorbeeld spelen wanneer er sprake is van betrokkenheid vanuit DDGC zelf, een klant, of wanneer er onvoldoende maatregelen zijn getroffen om ongeregeldheden te voorkomen. Indien gewenst vindt overleg plaats met de Privacy Officer;
- Wat er intern wordt gecommuniceerd over het incident;
- Wat er extern wordt gecommuniceerd over het incident en vaststellen of de pers geïnformeerd moet worden;
- Of naast de Autoriteit Persoonsgegevens ook andere stakeholders geïnformeerd moeten worden;
- Welke partij melding doet bij de Autoriteit Persoonsgegevens;
- Of er individuen, klanten, leveranciers geïnformeerd moeten worden;
- Op welke wijze er intern wordt gerapporteerd;
- Of eventuele schade is gedekt door de verzekeringspolis.

Afhandeling

De DPO rapporteert aan de directeur DDGC de uitkomsten van het overleg van het Response Team Datalek. De directeur DDGC accordeert de uit te voeren activiteiten, zoals vastgesteld door het Response Team Datalek, of stelt de uit te voeren activiteiten bij. De door de directeur DDGC vastgestelde activiteiten worden uitgevoerd.

Melding bij de Autoriteit Persoonsgegevens

In overleg met betrokken partijen wordt bepaald wie de melding van het Datalek doet bij de Autoriteit Persoonsgegevens. De betreffende partij meldt vervolgens binnen 2 dagen volgens de aangewezen methode het datalek via het Meldpunt Datalek van de Autoriteit Persoonsgegevens (https://datalekken.autoriteitpersoonsgegevens.nl/).

In ieder geval zal gemeld moeten worden:

- Aard van de inbreuk, waaronder betrokken categorieën, aantal betrokkenen, beschrijving gegevens;
- Beschrijving van de te verwachten gevolgen;
- Getroffen en/of voorgestelde maatregelen;
- Informatie over te nemen maatregelen door de betrokkene om de nadelige gevolgen te beperken;
- Contactgegevens voor betrokkene;

Ontvangstbevestiging Autoriteit Persoonsgegevens

Is er een melding gedaan, dan ontvangt DDGC een ontvangstbevestiging. Bij de meldingen die aanleiding geven tot nadere actie door de Autoriteit Persoonsgegevens, zal de Autoriteit Persoonsgegevens contact opnemen met DDGC om de herkomst van de melding te verifiëren.

Terugkoppeling betrokken

Na de melding bij de Autoriteit Persoonsgegevens en eventuele getroffen maatregelen zal een terugkoppeling plaatsvinden bij de betrokkenen. Hierna zal het incident worden afgesloten en zullen de getroffen maatregelen worden geëvalueerd binnen de PDCA-cyclus van het Risico Management Programma.