

VERWERKERSOVEREENKOMST ALGEMENE VERORDENING GEGEVENSBESCHERMING GENERALE DATA PROTECTION REGULATION (GDPR)

TUSSEN:

Het Sociaal Secretariaat DPS VZW, met maatschappelijke zetel te 9300 Aalst, Arbeidsstraat 112, ingeschreven in de Kruispuntbank van de ondernemingen onder het nummer 0473.487.880 en vertegenwoordigd door de heer Bruno Lahousse en mevrouw Christine Mattheeuws, gedelegeerd bestuurders

hierna genoemd ‘de Verwerker’

EN:

..... met maatschappelijke zetel te
..... ingeschreven in de
Kruispuntbank van de Ondernemingen onder het nummer

en vertegenwoordigd door de....., zaakvoerder,

hierna genoemd “de Verwerkingsverantwoordelijke” (afgekort “de Verantwoordelijke”)

VOORAFGAAND:

Huidige overeenkomst wordt afgesloten in het kader van de verwerking van de persoonsgegevens (GDPR-wetgeving).

Door het afsluiten van huidige overeenkomst stellen partijen zich in orde met de Algemene Verordening Gegevensbescherming.

Teneinde alle discussies te vermijden, achten partijen het aangewezen om de begrippen die betrekking hebben op de Algemene Verordening Gegevensbescherming voorafgaandelijk duidelijk te omschrijven.


Begrippen :

- Onder “**persoonsgegevens**” wordt verstaan alle informatie over een natuurlijk persoon “de betrokkene” waardoor deze direct of indirect kan geïdentificeerd worden. Persoonsgegevens zijn gegevens zoals naam, foto, adres, bankrekeningnummer, vingerafdruk, medische data, rijksregisternummer, locatiegegevens, telefoonnummers, e-mailadressen, online identificators, ... Maar ook alle (andere) gegevens met betrekking tot de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van een natuurlijke persoon worden als persoonsgegevens beschouwd. Persoonsgegevens zijn alle gegevens die betrekking hebben op een individu, ongeacht of het gaat om zijn privé-, beroeps- of openbare leven.
- De “**verwerking**” is een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés. Het betreft dus o.a. het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

- De “**Verwerkingsverantwoordelijke**” of afgekort de “**Verantwoordelijke**” is een natuurlijke persoon, een rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, die alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. De Verwerkingsverantwoordelijke is diegene die de toezichthouder kan aanspreken in verband met de verwerking van persoonsgegevens, en diegenen tot wie de betrokkenen zich kunnen wenden om hun rechten uit te oefenen. In kader van huidige overeenkomst is dit de werkgever.
- De “**Verwerker**” is een natuurlijke persoon, een rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die ten behoeve van de Verwerkingsverantwoordelijke de persoonsgegevens verwerkt. In kader van huidige overeenkomst is dit het Sociaal Secretariaat DPS vzw.
- Een “**subverwerker**” is een natuurlijke persoon, een rechtspersoon of een dienst waar de Verwerker beroep op doet om de dienstverlening te waarborgen. Dit kan gaan over het hosten van een digitaal platform, het aanmaken van betalingsbestanden, het afprinten van bestanden, het versturen van postzendingen of het afleveren van pakketten ...
- De “**betrokkene**” is de geïdentificeerde of identificeerbare natuurlijk persoon op wie de verwerkte persoonsgegevens betrekking hebben. In kader van huidige overeenkomst zijn dit de werknemers van de Verantwoordelijke.
- De “**verwerkersovereenkomst**” is de overeenkomst tussen de Verwerker en de Verantwoordelijke waarin afspraken gemaakt worden over de respectievelijke verplichtingen ten aanzien van de AVG.
- De “**overeenkomst**” bestaat uit de verwerkersovereenkomst en 3 bijlagen, zijnde het overzicht met verwerkingen van persoonsgegevens en verwerkingsdoelen, het overzicht met beveiligingsmaatregelen en het proces rondom het melden van datalekken en de te verstrekken informatie.
- Een “**datalek**” is een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.
- De “**Functionaris voor Gegevensbescherming (of Data Protection Officer)**” is een persoon die toeziet op de omgang met persoonsgegevens en controleert of de wettelijke voorwaarden voldaan zijn. De DPO is de heer Didier Lecluyse. Hij is telefonisch te bereiken op het nummer 050/800.161 of via email Didier.lecluyse@groupdaenens.be.
- Een “**gegevensbeschermingseffectbeoordeling**” betreft het uitvoeren van een beoordeling, voorafgaand aan het uitvoeren van de verwerking, van het effect van de beoogde verwerkingsactiviteiten op de bescherming van de persoonsgegevens.
- De “**Toezichthoudende Autoriteit**” is een onafhankelijke overheidsinstantie verantwoordelijk voor het toezicht op de naleving van de wet in verband met de verwerking van persoonsgegevens. In België is dit de Gegevensbeschermingsautoriteit.

DPS vzw

Erkend sociaal secretariaat nr. 980 (M.B. 22.05.2002, B.S. 05.06.2002)
Kantoren te Aalst, Antwerpen, Gent, Lichtervelde en Waregem

 2 

WORDT OVEREENGEKOMEN HETGEEN VOLGT:

1. Totstandkoming, duur en beëindiging van de overeenkomst

- 1.1. De overeenkomst bestaat uit de verwerkersovereenkomst en 3 bijlagen, zijnde het overzicht met verwerkingen van persoonsgegevens en de verwerkingsdoelen, het overzicht met beveiligingsmaatregelen en de beschrijving van het proces rondom het melden van datalekken en de te verstrekken informatie.
- 1.2. Zowel de verwerkersovereenkomst als de bijlagen maken onlosmakelijk deel uit van de overeenkomst.
- 1.3. De overeenkomst wordt afgesloten voor onbepaalde duur en treedt in werking op de datum van ondertekening door beide partijen.

2. Verwerken persoonsgegevens

- 2.1. De Verwerker verwerkt in het kader van een dienstverleningsovereenkomst de persoonsgegevens ontvangen van de Verantwoordelijke. De Verwerker verwerkt de persoonsgegevens in opdracht van de Verantwoordelijke maar heeft geen zeggenschap over de persoonsgegevens. De Verwerker volgt de afspraken die hierover gemaakt werden met de Verantwoordelijke op.
- 2.2. In Bijlage 1 wordt opgenomen welke persoonsgegevens de Verwerker precies zal verwerken en voor welke verwerkingsdoeleinden.
- 2.3. De Verwerker zal enkel de persoonsgegevens verwerken die strikt noodzakelijk zijn voor de dienstverleningsovereenkomst en het bereiken van het doel van de verwerking. De Verwerker houdt zich aan de wet en verwerkt de gegevens op een behoorlijke, zorgvuldige en transparante wijze.
- 2.4. De Verwerker zal geen kopies maken van de persoonsgegevens tenzij met goedkeuring van de Verantwoordelijke. De Verwerker dient geen goedkeuring te krijgen van de Verantwoordelijke indien het kopiëren van de persoonsgegevens gebeurt met het oog op een back-up of indien dit noodzakelijk is voor de uitvoering van de overeenkomst.
- 2.5. De Verwerker verbindt er zich uitdrukkelijk toe om zijn personeelsleden op te leggen de AVG wetgeving na te leven en voorziet hiervoor de nodige opleidingen.
- 2.6. De Verantwoordelijke is ervan op de hoogte dat de Verwerker in het kader van het vervullen van zijn dienstverlening een beroep doet of kan doen op subverwerkers. De Verantwoordelijke erkent dat deze inschakeling van subverwerkers door de Verwerker noodzakelijk is voor het nakomen van zijn contractuele verplichtingen en geeft er dan ook zijn toestemming voor.


De Verantwoordelijke verleent algemene toestemming aan de Verwerker om andere subverwerkers in te schakelen en/of bestaande subverwerkers te vervangen. Indien de Verwerker beroep zal doen op een nieuwe subverwerker zal hij de Verantwoordelijke in de mate van het mogelijke hierover op voorhand inlichten. De Verantwoordelijke heeft het recht omwille van gemotiveerde en gegronde redenen hiertegen bezwaar aan te tekenen.

Wanneer de Verwerker een subverwerker inschakelt, zal de Verwerker erop toezien dat deze minimaal voldoet aan de eisen die zijn opgenomen in deze verwerkersovereenkomst.

De Verwerker blijft aansprakelijk wanneer de subverwerker zijn verplichtingen t.a.v. de beveiliging van gegevens zoals voorzien in huidige overeenkomst niet naleeft.
- 2.7. De Verantwoordelijke zal elk officieel verzoek en elke inspectie van de Gegevensbeschermingsautoriteit melden aan de Verwerker.

DPS vzw

Erkend sociaal secretariaat nr. 980 (M.B. 22.05.2002, B.S. 05.06.2002)
Kantoren te Aalst, Antwerpen, Gent, Lichtervelde en Waregem

 3 

2.8. De Verwerker beantwoordt geen rechtstreekse verzoeken van betrokkenen maar zal de betrokkenen steeds doorverwijzen naar de Verantwoordelijke.

De Verantwoordelijke zal instaan voor het garanderen van alle rechten van betrokkenen.

Deze rechten kunnen o.a. bestaan uit een verzoek om inzage, verbetering, aanvulling, verwijdering of afscherming van de persoonsgegevens. De betrokkene kan ook bezwaar maken tegen de verwerking van de persoonsgegevens en een verzoek indienen tot overdraagbaarheid van de eigen persoonsgegevens.

De Verwerker zal rekening houdend met de aard van de verwerking, de Verantwoordelijke bijstaan bij het vervullen van diens plicht om verzoeken tot uitoefenen van de rechten van betrokkenen te beantwoorden. Eveneens zal de Verwerker de Verantwoordelijke bijstand verlenen bij het doen nakomen van de verplichtingen i.v.m. de beveiliging van de verwerking en de melding van inbreuken aan de Toezichhoudende Autoriteit.

2.9. Wanneer de Verantwoordelijke de Verwerker verzoekt om informatie te geven voor het uitvoeren van een Gegevensbeschermingseffectbeoordeling, dan zal Verwerker de informatie verstrekken.

3. Beveiligen van Persoonsgegevens

3.1. Verwerker zorgt ervoor dat de persoonsgegevens voldoende beveiligd zijn. Om verlies, vernietiging, vervalsing, niet toegelaten verspreiding of toegang en elke andere vorm van onrechtmatige verwerking te voorkomen neemt Verwerker passende technische en organisatorische maatregelen.

3.2. Deze maatregelen zijn afgestemd op het risico van de verwerking. Een overzicht van deze maatregelen en het beleid daarover werd opgenomen in Bijlage 2.

3.3. De Verantwoordelijke heeft het recht te controleren of het verwerken van de persoonsgegevens aan de wet en de afspraken uit deze Verwerkersovereenkomst voldoet. De Verwerker zal audits, waaronder inspecties door de Verantwoordelijke of een door de Verantwoordelijke gemachtigd controleur mogelijk maken en eraan bijdragen

3.4. De kosten voor de uitvoering van deze audit zullen enkel voor rekening van de Verwerker komen wanneer de Verantwoordelijke kan aantonen dat Verwerker zich manifest niet aan de verplichtingen in deze verwerkersovereenkomst heeft gehouden.

3.5. De Verantwoordelijke staat zelf in voor het nemen van alle passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen.

3.6. Wanneer één van beide partijen vindt dat een wijziging in de te nemen beveiligingsmaatregelen noodzakelijk is, treden beide partijen in overleg over de wijziging daarvan. De kosten voor het wijzigen van de beveiligingsmaatregelen komen voor de rekening van degene die de kosten maakt.

4. Exporteren Persoonsgegevens:

4.1. Verwerker mag geen persoonsgegevens laten verwerken door andere personen of organisaties buiten de Europese Economische Ruimte (EER), zonder daarvoor voorafgaande schriftelijke toestemming te hebben verkregen van de Verantwoordelijke.

5. Geheimhouding:

DPS vzw

Erkend sociaal secretariaat nr. 980 (M.B. 22.05.2002, B.S. 05.06.2002)

Kantoren te Aalst, Antwerpen, Gent, Lichtervelde en Waregem

 4 

5.1. Verwerker zal de verstrekte persoonsgegevens geheim houden, tenzij dit op basis van een wettelijke verplichting niet mogelijk is.

5.2. Verwerker doet het nodige opdat ook haar personeel en ingeschakelde hulppersonen of subverwerkers zich aan deze geheimhouding houden.

6. Datalekken:

6.1. In geval van een ontdekking van een mogelijk datalek zal de Verwerker de Verantwoordelijke hierover informeren binnen 24 uur en de informatie verstrekken die is aangegeven in Bijlage 3, zodat de Verantwoordelijke indien nodig een melding bij de Toezichthoudende Autoriteit kan doen.

6.2. Na de melding van een datalek aan de Verantwoordelijke, zal de Verwerker de Verantwoordelijke op de hoogte houden van nieuwe ontwikkelingen rondom het datalek en de maatregelen die Verwerker heeft getroffen om de omvang van het datalek te beperken en te beëindigen en een soortgelijk incident in de toekomst te kunnen voorkomen.

6.3. Het is niet toegestaan dat Verwerker een melding van een datalek doet aan de Toezichthoudende Autoriteit. Evenmin mag Verwerker de betrokkenen informeren over het datalek. Dit is de taak van de Verantwoordelijke.

6.4. Eventuele kosten die gemaakt worden om het datalek op te lossen en in de toekomst te kunnen voorkomen, zijn voor rekening van degene die de kosten maakt.

7. Aansprakelijkheid:

7.1. De Verwerker wordt geacht een inspanningsverbintenis te hebben aangegaan. De Verwerker is behoudens bedrog, een zware of opzettelijke fout, niet aansprakelijk voor schade te wijten aan het niet naleven van de verplichtingen uit deze verwerkersovereenkomst. Indien de Verantwoordelijke van zijn eventueel recht op schadevergoeding gebruik wil maken, dient hij dit binnen de 6 maanden na het voordoen van de vermeende fout aan de Verwerker via aangetekend schrijven mee te delen. Indien mogelijk zal de Verwerker de fout op eigen kosten herstellen. De Verantwoordelijke zal in dat geval geen aanspraak kunnen maken op de schadevergoeding.

7.2. De aansprakelijkheid is in elk geval beperkt tot de jaarlijkse waarde van de overeenkomst voor de uitvoering van de diensten.

8. Teruggave Persoonsgegevens en bewaartermijn:

8.1. De Verwerker zal de persoonsgegevens bewaren gedurende de overeenkomst en vanaf het einde van de overeenkomst gedurende een termijn gelijk aan de wettelijke bewaringstermijn of de verjaringstermijn waarbinnen een rechtsvordering kan worden ingesteld. Een wettelijke bewaartermijn is er bijvoorbeeld wanneer Verwerker de persoonsgegevens moet bewaren om sociaalrechtelijke of fiscale redenen.

8.2. Na deze termijnen zal de Verwerker de persoonsgegevens in de mate van het mogelijke terugbezorgen aan de Verantwoordelijke indien deze hierom vraagt. Eventuele achtergebleven persoonsgegevens zullen op een zorgvuldige en veilige manier vernietigd worden.

8.3. Indien de Verantwoordelijke niet gevraagd heeft om de persoonsgegevens terug te krijgen, zullen de persoonsgegevens na het verstrijken van voornoemde termijnen gewist worden behoudens indien het bewaren van de gegevens wettelijk verplicht is.

DPS vzw

Erkend sociaal secretariaat nr. 980 (M.B. 22.05.2002, B.S. 05.06.2002)
Kantoren te Aalst, Antwerpen, Gent, Lichtervelde en Waregem

 5 

9. Slotbepalingen

9.1. Deze verwerkersovereenkomst is onderdeel van de overeenkomst. Alle rechten en verplichtingen uit de overeenkomst zijn daarom ook van toepassing op de verwerkersovereenkomst.

9.2. Bij eventuele tegenstrijdigheden tussen de bepalingen in de verwerkers-overeenkomst en de overeenkomst m.b.t. persoonsgegevens gelden de bepalingen uit deze verwerkersovereenkomst.

9.3. Afwijkingen van deze verwerkersovereenkomst zijn slechts geldig wanneer beide partijen dit samen schriftelijk afspreken.

9.4. De nietigheid van een bepaling van huidige overeenkomst tast de geldigheid van de overige bepalingen niet aan.

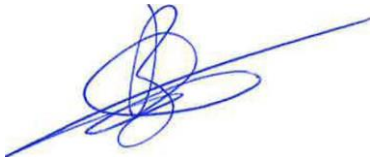
9.5. Op deze verwerkersovereenkomst en de werkzaamheden van de verwerker is het Belgisch recht van toepassing.

9.6. Bij gebreke aan een minnelijke regeling, zullen alle geschillen m.b.t. huidige overeenkomst worden voorgelegd aan de rechtbanken bevoegd binnen het rechtsgebied waar de maatschappelijke zetel van de verwerker gevestigd is.

9.7. Beide partijen erkennen een origineel exemplaar van de huidige verwerkersovereenkomst te hebben ontvangen, behoorlijk ondertekend door alle partijen.

Opgemaakt te Waregem op 15/11/2022

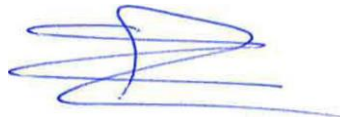
Namens de Verwerker



Bruno Lahousse

Gedelegeerd bestuurder

Namens de Verwerker



Christine Mattheeuws

Gedelegeerd bestuurder

Namens de Verantwoordelijke

Voor "Gelezen en goedgekeurd"

.....

(handtekening*)

Naam

functie

**De Verantwoordelijke laat zijn handtekening voorafgaan door de handgeschreven vermelding 'Gelezen en goedgekeurd' en parafeert eveneens elk van de voorgaande bladzijden*

Bijlage 1:

Overzicht met verwerkingen van persoonsgegevens en verwerkingsdoelen

Het onderstaande schema zal ingevuld moeten worden elke keer dat een Verwerkersovereenkomst wordt gesloten.

Het geeft een volledig overzicht van de persoonsgegevens die verwerkt zullen worden.

Dit maakt het makkelijker om aan te kunnen tonen waar, door wie en voor welk doel de persoonsgegevens worden verwerkt.

Persoonsgegevens:

Identificatiegegevens

Contactgegevens

Familiale gegevens

Opleidings-en beroepsgegevens

Financiële gegevens

Aard en doel van de verwerkingen:

Registraties, berekeningen en aangiftes in het kader van de loonadministratie en loonberekening en alle hiermee gepaard gaande begeleidende maatregelen.

Bijlage 2:

Overzicht met beveiligingsmaatregelen

Hieronder worden enkele van de beveiligingsnormen vermeld die de Verwerker op het moment van het afsluiten van huidige overeenkomst, voorziet. Deze lijst is niet limitatief. Deze maatregelen kunnen bovendien, afhankelijk van de noden, uitgebreid en aangepast worden. Eventueel kan de Verantwoordelijke aan de Verwerker bijkomende beveiligingsmaatregelen opleggen.

Technische beveiligingsmaatregelen:

- Up-to-date virusscan
- Unieke inlogcode en wachtwoord (regelmatig aanpassen)
- Geen onbeveiligde externe harde schijven
- Geen onbeveiligde back ups maken

Organisatorische beveiligingsmaatregelen:

- Clean desk policy
- Laptop niet onbemand achterlaten
- Eigen privacy policy
- Privacy screens medewerkers
- Oude documenten op juiste manier vernietigen
- Zorgvuldig gebruik van USB-stick

DPS vzw

Erkend sociaal secretariaat nr. 980 (M.B. 22.05.2002, B.S. 05.06.2002)
Kantoren te Aalst, Antwerpen, Gent, Lichtervelde en Waregem

 8 

Bijlage 3:

Proces rondom het melden van datalekken en de te verstrekken informatie

Een datalek moet gemeld worden als het waarschijnlijk is dat de betrokkene hierdoor enige vorm van schade zal/kan leiden. Hieronder een aantal niet limitatief opgesomde voorbeelden van beveiligingsincidenten die moeten worden gemeld bij de toezichthoudende autoriteit : de website met logingegevens is gehackt of is toegankelijk voor derden ; verlies van een laptop of USB-stick met persoonsgegevens, loonstroken/individuele rekeningen zijn naar verkeerde personen verstuurd ; brieven of e-mails worden naar een verkeerd adres verstuurd ; een aanval van een hacker op het ICT systeem ; een verloren of gestolen telefoon waar persoonsgegevens op aanwezig zijn...

Bij twijfel of het datalek gemeld moet worden, kunnen de volgende vragen als leidraad gebruikt worden : Is er een technisch of fysiek beveiligingsprobleem? Gaat het probleem over de beveiliging van Persoonsgegevens? Gaat het om gevoelige gegevens zoals gezondheidsgegevens, locatiegegevens, rijksregisternummers? Gaat het om gegevens van kwetsbare groepen zoals kinderen? Zijn er grote hoeveelheden persoonsgegevens onbedoeld toegankelijk geworden voor derden?

Bij het melden van een datalek, dienen de gegevens zo volledig mogelijk omschreven te worden. Men kan zich hiervoor best baseren op de vragen die door de Verantwoordelijke aan de Toezichthoudende Autoriteit zullen moeten worden beantwoord:

Geef een samenvatting van het beveiligingslek / beveiligingsincident / datalek: wat is er gebeurd? Vermeld hier ook de naam van het betrokken systeem. Welke typen persoonsgegevens zijn betrokken bij het beveiligingsincident? Van hoeveel personen zijn de persoonsgegevens betrokken bij het beveiligingsincident? Maak een inschatting van het minimum en maximum aantal personen. Omschrijving groep personen om wiens gegevens het gaat (bijzondere aandacht voor gevoelige gegevens en/of gegevens van kwetsbare groepen personen, zoals kinderen). Zijn de contactgegevens van de betrokken personen bekend? Moeten zij geïnformeerd worden over het datalek? Wat is de oorzaak van het beveiligingsincident? Hoe is het beveiligingsincident kunnen ontstaan? Op welke datum of in welke periode heeft het beveiligingsincident plaats kunnen vinden?

DPS vzw

Erkend sociaal secretariaat nr. 980 (M.B. 22.05.2002, B.S. 05.06.2002)
Kantoren te Aalst, Antwerpen, Gent, Lichtervelde en Waregem

 9 