WONINGCORPORATIE ZAYAZ

OVEREENKOMST GEZAMENLIJKE VERANTWOORDELIJKHEID

Contractpartijen:

Medeverantwoordelijke te weten Stichting Zayaz, statutair gevestigd te 's-Hertogenbosch, vertegenwoordigd door

hierna te noemen: "**Medeverantwoordelijke 1**",
en
Medeverantwoordelijke te weten

,

statutair gevestigd te

,

ingeschreven in het Handelsregister van de Kamer van Koophandel onder dossiernummer

,

vertegenwoordigd door

hierna te noemen: "**Medeverantwoordelijke 2**",
gezamenlijk aan te duiden als: "**Partijen**",

Overwegende dat:

Partijen hebben een Overeenkomst met betrekking tot

gesloten.

Om deze overeenkomst te kunnen uitvoeren, worden Persoonsgegevens verwerkt.

Partijen hechten grote waarde aan het beschermen van deze Persoonsgegevens. Om die reden leggen Partijen in deze Overeenkomst gezamenlijke verantwoordelijkheid en de daarbij behorende bijlagen, te weten:

1. Overzicht met verwerkingen van Persoonsgegevens en verwerkingsdoelen
2. Proces rondom het melden van Datalekken en de te verstrekken informatie

en de wederzijdse verantwoordelijkheden vast.

Postbus 488 ▪ 5201 AL ▪ 's-Hertogenbosch

1. Definities

De hierna en hiervoor gebruikte begrippen volgen uit de Algemene Verordening Gegevensbescherming en hebben de volgende betekenis:

Betrokkene: geïdentificeerde of identificeerbaar natuurlijk persoon op wie de verwerkte persoonsgegevens-betrekking hebben;

Gezamenlijke verantwoordelijkheid: wanneer twee of meer verantwoordelijken gezamenlijk de doel-einden en middelen van de verwerking bepalen, zijn zij gezamenlijk verantwoordelijk;

Inbreuk in verband met persoonsgegevens: een inbreuk op de beveiliging die per ongeluk of op onrecht-matige 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 ("**Datalek**");

Overeenkomst: de hoofdovereenkomst waar deze Overeenkomst gezamelijke verantwoordelijkheid uit voortvloeit;

Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrok-kene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdenti-ficeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;

Toezichthoudende autoriteit: een onafhankelijke overheidsinstantie verantwoordelijk voor het toezicht op de naleving van de wet in verband met de verwerking van Persoonsgegevens. In Nederland is dit de Autori-teit Persoonsgegevens;

Verantwoordelijke: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lid statelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsver-antwoordelijke is of volgens welke criteria deze wordt aangewezen;

Verwerking: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, ver-strekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

2. Totstandkoming, duur en beëindiging van deze Overeenkomst gezamenlijke verantwoordelijkheid

2.1 Deze Overeenkomst gezamenlijke verantwoordelijkheid treedt in werking op het moment dat Persoonsgegevens worden gedeeld of uitgewisseld.

2.2 Deze Overeenkomst gezamenlijke verantwoordelijkheid is onderdeel van de Overeenkomst en zal gelden voor zolang de Overeenkomst duurt.

2.3 Indien de Overeenkomst eindigt, eindigt deze Overeenkomst gezamenlijke verantwoordelijkheid automatisch; de Overeenkomst gezamenlijke verantwoordelijkheid kan niet apart worden opgezegd.

2.4 Na beëindiging van deze Overeenkomst gezamenlijke verantwoordelijkheid zullen de lopende verplichtingen voor Verwerker zoals het melden van Datalekken, waarbij de Persoonsgegevens van Partijen betrokken zijn en de plicht tot geheimhouding blijven voortduren.

3. Verwerken Persoonsgegevens

3.1 Partijen verwerken Persoonsgegevens alleen op de wijze zoals Partijen dit bij deze Overeenkomst gezamenlijke verantwoordelijkheid overeenkomen en zullen Persoonsgegevens niet op een andere manier verwerken, tenzij Partijen dit gezamenlijk overeenkomen.

3.2 In Bijlage 1 wordt opgenomen welke Persoonsgegevens Partijen precies zullen verwerken, voor welke verwerkingsdoeleinden en wie voor welk deel verantwoordelijk is.

3.3 Partijen houden zich bij het verwerken van persoonsgegevens aan de wet en de gegevens worden verwerkt op een behoorlijke, zorgvuldige en transparante wijze.

3.4 Partijen mogen zonder voorafgaande schriftelijke toestemming van - elkaar geen andere personen of organisaties inschakelen bij het verwerken van de Persoonsgegevens.

3.5 Wanneer Partijen met toestemming van elkaar andere organisaties inschakelen, moeten zij minimaal voldoen aan de eisen die zijn opgenomen in deze Overeenkomst gezamenlijke verantwoordelijkheid.

3.6 Wanneer Partijen een verzoek van een Betrokkene ontvangen ten aanzien van het uitoefenen van zijn of haar rechten, zullen Partijen daar binnen de wettelijke termijn aan meewerken. Deze rechten bestaan uit een verzoek om inzage, verbetering, aanvulling, verwijdering of afscherming, bezwaar maken tegen de verwerking van de persoonsgegevens en een verzoek tot overdraagbaarheid van de eigen Persoonsgegevens.

Postbus 488 ▪ 5201 AL ▪ 's-Hertogenbosch

4. Exporteren Persoonsgegevens

4.1 Partijen mogen geen Persoonsgegevens laten verwerken door andere personen of organisaties buiten de Europese Economische Ruimte (EER), zonder daarvoor voorafgaande schriftelijke toestemming te hebben verkregen van Medeverantwoordelijke.

5. Geheimhouding

5.1 Partijen zullen de verstrekte Persoonsgegevens geheim houden, tenzij dit op basis van een wettelijke verplichting niet kan.

5.2 Partijen zorgen ervoor dat het personeel en ingeschakelde hulppersonen zich aan deze geheimhouding houden.

6. Datalekken

6.1 In geval van een ontdekking van een mogelijk Datalek zullen partijen elkaar hierover informeren binnen 24 uur overeenkomstig de procedure zoals die is opgenomen in Bijlage 2.

6.2 Partijen zullen elkaar op de hoogte houden van nieuwe ontwikkelingen rondom het Datalek, ook zullen Partijen de getroffen maatregelen om het Datalek te beperken en te beëindigen en een soortgelijk incident in de toekomst te kunnen voorkomen, overleggen aan elkaar.

6.3 Partijen doen elk voor dat deel waar zij verantwoordelijk voor zijn de melding van een Datalek bij de Toezichthouder. Hetzelfde geldt voor de melding aan de Betrokkenen.

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

7. Aansprakelijkheid

7.1 Als een van de partijen de verplichtingen uit deze Overeenkomst gezamenlijke verantwoordelijkheid niet nakomt, kunnen zij voor hun deel van de verwerking aansprakelijk gesteld worden.

7.2 De ene Medeverantwoordelijke is aansprakelijk voor alle directe en indirecte schade geleden door de andere Medeverantwoordelijke als gevolg van het niet nakomen van de wet en de bepalingen uit deze overeenkomst, voor zover dit is ontstaan door werkzaamheden van de ene Medeverantwoordelijke. Voor onderzoek bij een Datalek mag de andere Medeverantwoordelijke een expert inschakelen, dit valt onder de indirecte schade.

7.3 Als de Toezichthoudende autoriteit een bestuurlijke boete oplegt aan de ene medeverantwoordelijke, terwijl de schade het gevolg is van onrechtmatig of nalatig handelen van de andere medeverantwoordelijke, dan is de andere medeverantwoordelijke hiervoor aansprakelijk.

7.4 De ene Medeverantwoordelijke is niet aansprakelijk voor aanspraken van Betrokkenen of andere personen en organisaties waar de andere Medeverantwoordelijke de samenwerking mee is aangegaan, als dit het gevolg is van het onrechtmatig of nalatig handelen van die Medeverantwoordelijke.

8. Teruggave Persoonsgegevens en bewaartermijn

8.1 Na het beëindigen van deze Overeenkomst gezamenlijke verantwoordelijkheid geven Partijen de Persoonsgegevens aan elkaar terug indien van toepassing.

8.2 Eventuele overgebleven Persoonsgegevens zullen Partijen vernietigen na verstrijken van de wettelijke bewaartermijn.

9. Slotbepalingen

9.1 Deze Overeenkomst gezamenlijke verantwoordelijkheid is onderdeel van de Overeenkomst. Alle rechten en verplichtingen uit de Overeenkomst zijn daarom ook van toepassing op de Overeenkomst gezamenlijke verantwoordelijkheid.

9.2 Bij eventuele tegenstrijdigheden tussen de bepalingen in de Overeenkomst gezamenlijke verantwoordelijkheid en de Overeenkomst, gelden de bepalingen uit deze Overeenkomst gezamenlijke verantwoordelijkheid ten aanzien van de verwerking van Persoonsgegevens.

9.3 Afwijkingen van deze Overeenkomst gezamenlijke verantwoordelijkheid zijn slechts geldig wanneer Partijen dit samen schriftelijk afspreken.

9.4 Op deze overeenkomst en werkzaamheden is het Nederlandse recht van toepassing.

Postbus 488 ▪ 5201 AL ▪ 's-Hertogenbosch

Aldus door Partijen overeengekomen en ondertekend:

MEDEVERANTWOORDELIJKE 1:

Ondertekend voor en namens:
Stichting Zayaz

Naam:

Functie:

Datum en plaats:

Handtekening:

MEDEVERANTWOORDELIJKE 2:

Ondertekend voor en namens:

Naam:

Functie:

Datum en plaats:

Handtekening:

WONINGCORPORATIE NAYAN

BIJLAGE 1: OVERZICHT VERWERKINGEN PERSOONSGEGEVENS EN VERWERKINGSDOELEN

In dit overzicht staan de persoonsgegevens die verwerkt worden. Dit maakt het makkelijker om aan te tonen waar, door wie en met welk doel de persoonsgegevens worden verwerkt.

Beschrijving verwerkingen door Partijen:

Medeverantwoordelijke 1:

Medeverantwoordelijke 2:

De persoonsgegevens worden gebruikt om:

Medeverantwoordelijke 1:

Medeverantwoordelijke 2:

Adresgegevens van (eventuele) Subverwerkers:

Medeverantwoordelijke 2:

Verwerkte persoonsgegevens (kruis aan wat van toepassing is):

- ☐ Naam, adres en woonplaatsgegevens
- ☐ Telefoonnummers, e-mailadressen
- ☐ Toegangs/ of identificatie gegevens
- ☐ Financiële gegevens
- ☐ Burgerservicenummer (BSN)
- ☐ Kopieën ID / legitimatiebewijzen
- ☐ Geslacht, geboortedatum en/of leeftijd
- ☐ Bijzondere persoonsgegevens (zie bijlage 2)

Locatie verwerkingen (waar worden de gegevens opgeslagen):

Medeverantwoordelijke 1:

Medeverantwoordelijke 2:

BIJLAGE 2: PROCES RONDOM MELDEN DATALEKKEN

Wat is een beveiligingsincident en wanneer moet dit gemeld worden?
Een datalek is een beveiligingsincident waarbij Persoonsgegevens, die de ene verantwoordelijke namens de andere verantwoordelijke beheert, mogelijk verloren zijn gegaan of onbedoeld toegankelijk waren voor derden. Elke Medeverantwoordelijke dient voor het deel waar hij/zij verantwoordelijk voor is een melding te maken bij de Toezichthoudende autoriteit wanneer er sprake is van een beveiligingsincident. Het gaat om gegevens die te koppelen zijn aan deze personen, zoals, maar niet beperkt tot, namen, adressen, telefoonnummers, e-mailadressen, log in gegevens, cookies, IP adressen of identificerende gegevens van computers of telefoons.

Hieronder staan een aantal voorbeelden van beveiligingsincidenten die moeten worden gemeld bij de Toezichthouder (Autoriteit Persoonsgegevens):

- Brieven of e-mails worden naar een verkeerd adres gestuurd.
- Verlies of diefstal van een laptop, telefoon of USB-stick met persoonsgegevens.
- Adresbestanden zijn onbedoeld toegankelijk voor derden.
- De website met logingegevens is gehackt of is toegankelijk voor derden.
- Een aanval van een hacker op het ICT systeem.

Wat te doen bij twijfel?
Neem ook bij twijfel altijd even contact op met Zayaz via iteam@zayaz.nl of telefoonnummer 073-648 27 00!
Weet u niet zeker of er sprake is van een beveiligingsincident? Stel dan in ieder geval de volgende vragen als hulpmiddel:

- Is er een technisch of fysiek beveiligingsprobleem?
- Gaat het probleem over de beveiliging van Persoonsgegevens? Ook IP-adressen, telefoonnummers of identificerende gegevens, bijvoorbeeld van hardware, kunnen hieronder vallen.
- Gaat het om bijzondere gegevens zoals ras, gezondheidsgegevens, informatie over iemands financiële situatie, zoals salaris of gegevens waar (identiteits)fraude mee kan worden gepleegd, zoals een Burgerservicenummer.
- Zijn er grote hoeveelheden persoonsgegevens onbedoeld toegankelijk geworden voor derden?
- Gaat het om gegevens van kwetsbare groepen?
- Worden de persoonsgegevens beheerd door een leverancier?

Postbus 488 ▪ 5201 AL ▪ 's-Hertogenbosch

Waar meldt u een beveiligingsincident?
Als u een beveiligingsincident ontdekt, neem dan direct contact op met:

Medeverantwoordelijke 1:
Medewerker I-team Zayaz
Telefoon: 073- 6482700
E-mail: iteam@zayaz.nl

Medeverantwoordelijke 2:

Telefoon:

E-mail:

Geef in de e-mail antwoord op de onderstaande vragen:

1. **Wie is de melder van het beveiligingsincident?**
   Geef de naam van de melder.
2. **Wie is de contactpersoon van het beveiligingsincident?**
   Geef de naam, telefoonnummer en het e-mailadres van de contactpersoon.
3. **Op welke datum of in welke periode vond het beveiligingsincident plaats?**
   Geef dit alstublieft zo specifiek mogelijk aan.
4. **Geef een samenvatting van het beveiligingslek / beveiligingsincident / datalek: wat is er gebeurd en waar is dit gebeurd?**
   Vermeld hier ook de naam van het betrokken systeem.
5. **Welke typen persoonsgegevens zijn betrokken bij het beveiligingsincident?**
   Zoals, maar niet beperkt tot, naam, adres, e-mailadres, IP-nummer, Burgerservicenummer, pasfoto en ieder ander tot een persoon te herleiden gegeven.
6. **Omschrijving groep personen om wiens gegevens het gaat.**
   Geef aan of het gaat om medewerkersgegevens, gegevens van internetgebruikers. Bijzondere aandacht verdienen gegevens van een kwetsbare groepen personen, zoals kinderen.
7. **Van hoeveel personen zijn de persoonsgegevens betrokken bij het beveiligingsincident?**
   Geef alstublieft een minimum en maximum aantal personen.
8. **Zijn de contactgegevens van de betrokken personen bekend?**
   Het kan zijn dat betrokkenen geïnformeerd moeten worden over het datalek, kunnen we deze personen in dat geval bereiken?
9. **Wat is de oorzaak (root cause) van het beveiligingsincident?**
   Heeft u een idee hoe het beveiligingsincident heeft kunnen ontstaan?

Deze vragen komen overeen met de informatie die aan de Toezichthouder moet worden verstrekt. Beantwoord de vragen alstublieft schriftelijk, en zo volledig mogelijk.

VERSIE 1
mei 2018

Paraaf
Medeverantwoordelijke 1:

Paraaf
Medeverantwoordelijke 2:

Postbus 488 ▪ 5201 AL ▪ 's-Hertogenbosch