Concept-Verwerkersovereenkomst Omgevingsdienst Haaglanden

CONCEPT

Overeenkomst

Omgevingsdienst Haaglanden gevestigd aan het Zuid-Hollandplein 1 , 2596 AW te Den Haag en geregistreerd bij de Kamer van Koophandel onder nummer 56093926, verder te noemen Verwerkingsverantwoordelijke, te dezen rechtsgeldig vertegenwoordigd door <…>,

en
bedrijf
gevestigd te
(adres en plaatsnaam)

geregistreerd bij de Kamer van Koophandel onder nummer

verder te noemen Verwerker, te dezen rechtsgeldig vertegenwoordigd door *(persoonsnaam en functie)*.

in aanmerking nemende dat

- Verwerkingsverantwoordelijke de beschikking heeft over persoonsgegevens en bij de verwerking hiervan Verwerker wenst in te schakelen;
- Verwerkingsverantwoordelijke en Verwerker ten behoeve van het voorgaande een overeenkomst hebben gesloten op (*datum)*

  (hierna: ''de Overeenkomst'') inzake (*onderwerp hoofdovereenkomst)*
- Verwerkingsverantwoordelijke de doeleinden en middelen aanwijst voor de verwerking, waarvoor de in de onderhavige overeenkomst genoemde voorwaarden gelden;
- Verwerker tevens bereid is verplichtingen omtrent beveiliging en andere aspecten van de Algemene Verordening Gegevensbescherming (hierna ook: AVG) dan wel (de corresponderende bepalingen uit) de uitvoeringswet Algemene verordening gegevensbescherming (UAVG) na te komen;
- Partijen hun rechten en plichten schriftelijk wensen vast te leggen middels deze verwerkersovereenkomst (hierna: "Verwerkersovereenkomst").

komen overeen:

Artikel 1 Definities

1.1 *Bijlagen*: aanhangsels bij deze overeenkomst, die na door beide partijen te zijn geparafeerd, deel uitmaken van deze overeenkomst.

1.2 *Verwerking*: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bewerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, evenals het afschermen, uitwissen of vernietigen van gegevens, zoals bedoeld in artikel 4 AVG

1.3 *Bestand*: elk gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen, zoals bedoeld in artikel 4 AVG.

1.4 *Verwerkingsverantwoordelijke*: de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt, zoals bedoeld in artikel 4 AVG.

1.5 *Verwerker*: degene die ten behoeve van Verwerkingsverantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen, zoals bedoeld in artikel 4 AVG.

1.6 *Betrokkene*: degene op wie een persoonsgegeven betrekking heeft.

1.7 *Derde*: ieder, niet zijnde de betrokkene, Verwerkingsverantwoordelijke, de Verwerker, of enig persoon die onder rechtstreeks gezag van Verwerkingsverantwoordelijke of Verwerker gemachtigd is om persoonsgegevens te verwerken, zoals bedoeld in artikel 4 AVG.

1.8 *Ontvanger*: degene aan wie de persoonsgegevens worden verstrekt, zoals bedoeld in artikel 4 AVG.

1.9 *De Autoriteit Persoonsgegevens of AP*: de autoriteit als bedoeld in artikel 6 UAVG.

1.10 *Functionaris*: de functionaris voor de gegevensbescherming als bedoeld in artikel 37 tot en met 39 van de Verordening.

1.11 *Voorafgaand onderzoek*: een onderzoek als bedoeld in artikel 36 van de Verordening.

1.12 *Verstrekken van persoonsgegevens*:- het bekend maken of ter beschikking stellen van persoonsgegevens.

1.13 Algemene verordening gegevensbescherming (afgekort: AVG): Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016.

Artikel 2 Ingangsdatum en duur

2.1 Deze overeenkomst gaat in op het moment van ondertekening en duurt voort zolang Verwerker de door Verwerkingsverantwoordelijke ter beschikking gestelde persoonsgegevens niet vernietigd heeft; ongeacht of de hoofdovereenkomst is beëindigd

Artikel 3 Onderwerp van deze overeenkomst

3.1 De Verwerker verwerkt persoonsgegevens in opdracht van Verwerkingsverantwoordelijke in het kader van de uitvoering van de volgende contractnummers:

CONCEPT

Het betreft de volgende soorten persoonsgegevens *(aankruisen)*:

○	categorie 1	indirecte persoonsgegevens wel herleidbaar (IP adres, personeelsnummer)
○	categorie 2	persoonsgegevens NAW+ (locatiegegevens)
○	categorie 3	gevoelige persoonsgegevens: NAW+ en betaalgegevens, BSN, ID (paspoort, rijbewijs)
○	categorie 4	strafrechtelijk

Het betreft de volgende categorieën betrokkenen *(bijvoorbeeld personeel, contractanten, aanvragers, burgers, bedrijven, website bezoekers)*:

3.2 Verwerker verbindt zich om in het kader van die werkzaamheden de door Verwerkingsverantwoordelijke ter beschikking gestelde persoonsgegevens zorgvuldig te verwerken.

Artikel 4 Naleving wet- en regelgeving

4.1 Verwerker verwerkt gegevens uitsluitend ten behoeve van Verwerkingsverantwoordelijke en in overeenstemming met diens instructies.

4.2 Verwerker heeft geen zeggenschap over de ter beschikking gestelde persoonsgegevens. Zo neemt hij geen beslissingen over ontvangst en gebruik van de gegevens, de verstrekking aan derden en de duur van de opslag van gegevens. De zeggenschap over de persoonsgegevens verstrekt onder deze overeenkomst komt nimmer bij de Verwerker te berusten.

4.3 Verwerker zal bij de verwerking van persoonsgegevens in het kader van de in artikel genoemde werkzaamheden, handelen in overeenstemming met de toepasselijke wet- en regelgeving betreffende de bescherming van persoonsgegevens. Verwerker verwerkt persoonsgegevens slechts in opdracht van Verwerkingsverantwoordelijke en zal alle redelijke instructies van Verwerkingsverantwoordelijke dienaangaande opvolgen, behoudens afwijkende wettelijke verplichtingen.

4.4 Verwerker zal te allen tijde op eerste verzoek van Verwerkingsverantwoordelijke onmiddellijk alle van Verwerkingsverantwoordelijke afkomstige persoonsgegevens met betrekking tot de Overeenkomst ter hand stellen, in een nader overeen te komen format.

4.5 Verwerker zal alle van Verwerkingsverantwoordelijke afkomstige persoonsgegevens met betrekking tot de Overeenkomst op een nader te bepalen wijze vernietigen en laten vernietigen op het moment van beëindigen van de Overeenkomst, dan wel op uitdrukkelijk verzoek van Verwerkingsverantwoordelijke de gegevens vernietigen op een nader te bepalen wijze en tijdstip.

4.6 Verwerker biedt Verwerkingsverantwoordelijke de noodzakelijke ondersteuning om binnen de wettelijke termijnen te voldoen aan de verplichtingen op grond van de AVG en de daarop rustende wettelijke bepalingen, meer in het bijzonder de rechten van betrokkenen, zoals, maar niet beperkt tot een verzoek om inzage, verbetering, aanvulling, verwijdering of afscherming van persoonsgegevens en het uitvoeren van een gehonoreerd verzet.

CONCEPT

4.7 Verwerker zal Verwerkingsverantwoordelijke de noodzakelijke medewerking verlenen wanneer er in het kader van de verwerking een Gegevensbeschermingseffectbeoordeling (Data Protection Impact Assessment), of een voorafgaande raadpleging van de toezichthouder, noodzakelijk mocht zijn.

Artikel 5 Geheimhoudingsplicht

5.1 Personen in dienst van, dan wel werkzaam ten behoeve van Verwerker, evenals Verwerker zelf, zijn verplicht tot geheimhouding met betrekking tot de persoonsgegevens waarvan zij kennis kunnen nemen of hebben genomen, behoudens voor zover een bij, of krachtens de wet gegeven voorschrift tot verstrekking verplicht of hun taak daartoe noodzaakt. De medewerkers van Verwerker tekenen hiertoe een geheimhoudingsverklaring. Deze geheimhoudingsverklaring wordt op eerste verzoek aan Verwerkingsverantwoordelijke ter inzage gegeven.

5.2 Indien Verwerker op grond van een wettelijke verplichting gegevens dient te verstrekken, zal Verwerker de grondslag van het verzoek en de identiteit van de verzoeker verifiëren en zal Verwerker Verwerkingsverantwoordelijke onmiddellijk na kennisname van het verzoek, voorafgaand aan de verstrekking, ter zake informeren en in de gelegenheid stellen tegen dat verzoek rechtsmiddelen in te stellen, tenzij wettelijke bepalingen dit verbieden.

Artikel 6 Beveiligingsmaatregelen

6.1 Verwerker neemt passende technische en organisatorische maatregelen om de persoonsgegevens die worden verwerkt ten dienste van Verwerkingsverantwoordelijke te beveiligen en beveiligd te houden tegen verlies of tegen enige vorm van onrechtmatige verwerking. Verwerker zal zich hiertoe houden aan de normen en standaards van Verwerkingsverantwoordelijke, zoals beschreven in bijlage 1. Hierin staan verplichte maatregelen welke voorafgaand aan afname dienst minimaal moeten zijn geïmplementeerd.

6.2 Bij afwijking van deze maatregelen is goedkeuring van Verwerkingsverantwoordelijke vereist. De wijze waarop Verwerker deze passende technische en organisatorische maatregelen aantoont, is een van de volgende opties:

Normenstelsel
□ De informatiebeveiliging vindt plaats volgens algemeen erkende normen, namelijk:
……..
(vermeld normenstelsel, zoals bijvoorbeeld NEN7510, NEN/ISO 27001, PCI/DSS).
□ De informatiebeveiliging vindt plaats volgens een algemeen erkende overheidsnorm zoals de BIG (of de BIR, BIO) of vergelijkbaar, namelijk:
……..
□ Anders, nl. ……..

De toereikendheid van de informatiebeveiliging blijkt uit de volgende certificering en verklaring van toepasselijkheid:
□ Periodieke externe controles zoals audits, pentesten of TPM's (bijv. ISAE3xxx SOC type II). ;
□ Een Assurance rapport van een auditor die is aangesloten bij NOREA;
□ Eigen controles of eigen mededelingen over de beveiligingsmaatregelen zoals hieronder beschreven:

……

CONCEPT

Artikel 7 Audit

7.1 Verwerkingsverantwoordelijke heeft het recht om audits uit te laten voeren door een onafhankelijke deskundige derde die aan geheimhouding is gebonden ter controle van naleving van alle punten uit deze verwerkersovereenkomst, en alles wat daar direct verband mee houdt.

7.2 Deze audit mag eens per jaar plaatsvinden, of vaker als er een concreet vermoeden van misbruik van persoonsgegevens of niet nakomen van deze verwerkersovereenkomst bestaat.

7.3 Verwerker zal aan de audit meewerken en alle voor de audit redelijkerwijs relevante informatie, inclusief ondersteunende gegevens zoals systeemlogs, en medewerkers zo tijdig mogelijk ter beschikking stellen.

7.4 De bevindingen naar aanleiding van de uitgevoerde audit zullen door Partijen in onderling overleg worden beoordeeld. Naar aanleiding daarvan zullen indien noodzakelijk wijzigingen worden doorgevoerd door één van de Partijen of door beide Partijen gezamenlijk.

7.5 De kosten van de audit worden door Verwerker gedragen indien er door Verwerker niet conform de verwerkersovereenkomst blijkt te zijn gewerkt, en/of er fouten worden gevonden die toegerekend moeten worden aan Verwerker. In ieder ander geval zullen de kosten van de audit worden gedragen door Verwerkingsverantwoordelijke.

Artikel 8 Meldplicht

8.1. Verwerkingsverantwoordelijke is verantwoordelijk voor het melden van een datalek (een inbreuk op de beveiliging van persoonsgegevens die leidt tot een aanzienlijke kans op ernstige nadelige gevolgen, dan wel ernstige nadelige gevolgen heeft, voor de bescherming van persoonsgegevens, zoals bedoeld in art. 33 AVG), aan de toezichthouder en eventueel aan betrokkenen. Om Verwerkingsverantwoordelijke in staat te stellen aan deze wettelijke plicht te voldoen, stelt Verwerker Verwerkingsverantwoordelijke onverwijld, maar in ieder geval binnen 24 uur na ontdekking, op de hoogte van ieder (potentieel) datalek.

8.2. De meldplicht behelst in ieder geval het melden van het feit dat er (mogelijk) een datalek is geweest. Daarnaast behelst de meldplicht:

- wat de (vermeende) oorzaak is van het datalek;
- (bij benadering) om hoeveel (bestanden van) persoonsgegevens het gaat, en van hoeveel betrokkenen;
- wat het (vooralsnog bekende en/of te verwachten) gevolg is;
- wat de (voorgestelde) oplossing is;
- contactgegevens voor de opvolging van de melding;
- wie geïnformeerd is (zoals betrokkene zelf, Verwerkingsverantwoordelijke, toezichthouder).

8.3. Mocht de bovenstaande informatie ten tijde van het ontdekken van het (mogelijke) datalek door Verwerker nog niet volledig bekend zijn, dan zal Verwerker alle reeds bekende informatie doorgeven aan Verwerkingsverantwoordelijke. Verwerker zal de ontbrekende informatie onverwijld achterhalen, en zal de melding aan Verwerkingsverantwoordelijke aanvullen zodra zij meer informatie heeft over het (mogelijke) datalek.

8.4 Verwerker heeft een gedetailleerd logboek van de Inbreuken en de maatregelen die op Inbreuken zijn genomen. Verwerkingsverantwoordelijke mag dat inzien, wanneer deze daarom vraagt.

8.5 Verwerkingsverantwoordelijke beslist of de Inbreuk moet worden gemeld bij de toezichthoudende autoriteit en/of Betrokkene.

CONCEPT

Artikel 9 Inschakeling derden

9.1 Verwerker is slechts gerechtigd de uitvoering van de werkzaamheden geheel of ten dele uit te besteden aan onderaannemers (subverwerkers) na voorafgaande schriftelijke toestemming van Verwerkingsverantwoordelijke. Verwerker zal Verwerkingsverantwoordelijke tijdig op de hoogte stellen van iedere voorgenomen nieuwe of te wijzigen subverwerker, en Verwerkingsverantwoordelijke in de gelegenheid stellen hiertegen schriftelijk bezwaar te maken. Wanneer Verwerkingsverantwoordelijke bezwaar maakt, zullen partijen hierover in overleg treden om tot een oplossing te komen.

9.2 Verwerker zorgt er in ieder geval voor dat subverwerkers schriftelijk ten minste dezelfde plichten op zich nemen als tussen Verwerkingsverantwoordelijke en Verwerker zijn overeengekomen. Verwerkingsverantwoordelijke heeft het recht de mogelijk hierbij betrokken overeenkomsten, zoals subverwerkers overeenkomsten, in te zien en daarvan afschrift of kopie te nemen.

9.3 Verwerker staat in voor een correcte naleving van de plichten uit deze verwerkersovereenkomst door deze subverwerkers en is bij fouten van deze subverwerkers zelf aansprakelijk voor alle schade alsof zij zelf de fout(en) heeft begaan

Artikel 10 Wijziging overeenkomst

10.1 Wijziging van deze overeenkomst geschiedt schriftelijk middels een door beide partijen geaccordeerd voorstel.

10.2 Zodra de samenwerking is beëindigd, vernietigt Verwerker de persoonsgegevens die hij in welke vorm dan ook van Verwerkingsverantwoordelijke heeft ontvangen, en toont dit aan middels een schriftelijke verklaring, tenzij partijen iets anders overeenkomen. Deze vernietiging moet, binnen nader overeen te komen termijn, uitgevoerd worden en hiervan wordt een verslag gemaakt dat bij de schriftelijke verklaring wordt gevoegd.

10.3 De geheimhouding geldt ook nog na beëindiging van deze Verwerkersovereenkomst.

Artikel 11 Aansprakelijkheid

11.1 Indien Verwerker tekortschiet in de nakoming van de verplichting uit deze overeenkomst kan Verwerkingsverantwoordelijke hem in gebreke stellen. Verwerker is echter onmiddellijk in gebreke als de nakoming van desbetreffende verplichting anders dan door overmacht binnen de overeengekomen termijn, reeds blijvend onmogelijk is. Ingebrekestelling geschiedt schriftelijk, waarbij aan de Verwerker een redelijke termijn wordt gegund om alsnog zijn verplichtingen na te komen. Deze termijn is een fatale termijn. Indien nakoming binnen deze termijn uitblijft, is Verwerker in verzuim.

11.2 Verwerker is aansprakelijk voor alle schade of nadeel voortvloeiende uit het niet-nakomen van, of in strijd handelen met de bij of krachtens de AVG en de op grond daarvan gegeven wettelijke voorschriften en/of het niet-nakomen van, of in strijd handelen met het in deze overeenkomst bepaalde.
Onverminderd de aanspraken op grond van wettelijke regels: Verwerker is aansprakelijk voor schade of nadeel voor zover ontstaan door zijn werkzaamheid. Verwerker is tevens aansprakelijk voor alle schade of nadeel voortvloeiende uit de door zijn werkzaamheid ontstane inbreuken op de persoonlijke levenssfeer van betrokkenen.

Artikel 12 Toepasselijk recht

12.1 Op deze overeenkomst en op alle geschillen die daaruit mogen voortvloeien of daarmee mogen samenhangen, is Nederlands recht van toepassing.

12.2 De bevoegde rechter is de rechter te Den Haag.

CONCEPT

Aldus in tweevoud ondertekend

namens Verwerkingsverantwoordelijke: datum:

namens Verwerker: datum:

CONCEPT

Bijlage 1: Maatregelen Informatiebeveiliging

Domein	Technische / organisatorische maatregel
Beveiligingsbeleid en Organisatie van informatiebeveiliging	**Eigenaarschap voor beveiliging en gegevensbescherming.** Verwerker heeft een Security Officer aangewezen die verantwoordelijk is voor het coördineren en controleren van de beveiligingsregels en -procedures. **Beveiligingsverantwoordelijkheden.** De beveiligingsverantwoordelijkheden van medewerkers zijn formeel gedocumenteerd en gepubliceerd in een beveiligingsbeleid. **Risicobeheer.** Verwerker voert periodiek risicoanalyses uit van de genomen beveiligingsmaatregelen.
Veilig personeelsbeleid	**Vertrouwelijkheidsverplichtingen.** Medewerkers van Verwerker zijn onderworpen aan vertrouwelijkheidsverplichtingen en deze verplichtingen worden formeel opgenomen in arbeidsovereenkomsten. **Beveiligingstraining.** De leverancier stelt haar medewerkers op de hoogte van de relevante beveiligingsprocedures voor het beschermen van klantendata en hun rol daarbij. **Beëindiging.** Toegangsrechten worden bij beëindiging van de samenwerking tijdig ingetrokken, in overeenstemming met formele beveiligingsadministratieprocedures.
Beheer van bedrijfsmiddelen	**Inventaris van bedrijfsmiddelen.** De leverancier houdt een inventaris bij van alle IT materiaal en media in gebruik. Toegang tot de inventarissen is beperkt tot hiervoor geautoriseerde medewerkers. **Behandeling van bedrijfsmiddelen** - Data op draagbare apparaten is versleuteld. - Verwerker beschikt over procedures voor het veilig vernietigen van media en afgedrukt materiaal die vertrouwelijke data bevatten.
Cryptografie	Versleuteling van vertrouwelijke data gebeurt volgens formele processen en crypto grafische standaarden. TLS-encryptie mechanismes zijn geïmplementeerd volgens de hoogste standaarden en gebruiken enkel sterke algoritmes met minimaal 128-bit encryptie.
Fysieke beveiliging en beveiliging van de omgeving	**Fysieke toegang tot faciliteiten.** - Verwerker beperkt de toegang tot faciliteiten waar vertrouwelijke informatie wordt verwerkt tot geïdentificeerde, geautoriseerde personen. - Fysieke toegang tot datacentra wordt uitsluitend toegekend volgens een formele autorisatieprocedure, en toegangsrechten worden periodiek beoordeeld. **Bescherming tegen verstoringen.** Verwerker gebruikt verschillende systemen die voldoen aan industrienormen om zijn datacentra te beschermen tegen gegevensverlies als gevolg van stroomuitval en brand.

CONCEPT

Domein	Technische / organisatorische maatregel
Toegangscontrole	**Toegangsbeleid** Verwerker hanteert een toegangscontrolebeleid op basis van 'need-to-know'- en 'least privileges'-beginselen. **Toegangsautorisatie** - Verwerker implementeert en handhaaft een autorisatiebeheersysteem dat de toegang controleert tot systemen die klantengegevens bevatten. - Elk individu die toegang heeft tot systemen die klantengegevens bevatten, heeft een aparte, unieke ID / gebruikersnaam. - Verwerker beperkt de toegang tot klantengegevens tot die personen die dergelijke toegang nodig hebben om hun functie uit te voeren. **Authenticatie** - Verwerker maakt gebruik van standaardpraktijken die voldoen aan industrienormen om gebruikers te identificeren en te authentiseren die zich proberen toegang te verschaffen tot de netwerk- of informatiesystemen van Verwerker, waaronder sterke authenticatie. - Indien authenticatiemechanismen gebaseerd zijn op wachtwoorden, dan vereist Verwerker dat de wachtwoorden ten minste acht tekens lang en voldoende complex zijn. - Gedeactiveerde of verlopen ID's / gebruikersnamen worden niet toegekend aan andere personen. - Accounts worden vergrendeld bij herhaalde pogingen om met behulp van een ongeldig wachtwoord toegang te krijgen tot het informatiesysteem. - Verwerker handhaaft praktijken om de vertrouwelijkheid en integriteit van wachtwoorden te garanderen wanneer ze worden toegekend en verstrekt, en tijdens de opslag. **Netwerktoegang.** Verwerker implementeert de nodige controlemaatregelen (bv. firewalls, security appliances, netwerk segmentatie) die een redelijke mate van zekerheid bieden dat toegang tot zijn netwerk op gepast wijze wordt beschermd.
Beveiliging van de bedrijfsactiviteiten (operationele beveiliging)	**Gegevensherstel** - Verwerker maakt op periodieke basis, maar in geen geval minder vaak dan één keer per week (tenzij tijdens die periode geen gegevens bijgewerkt werden), back-ups van klantengegevens voor hersteldoeleinden. - Verwerker bewaart kopieën van klantengegevens en gegevensherstelprocedures op een andere plaats dan waar de primaire computerapparatuur die de klantengegevens verwerkt, zich bevindt. **Kwaadaardige Software.** Verwerker voert anti-malwarecontroles uit om te helpen voorkomen dat kwaadaardige software ongeautoriseerde toegang tot klanten-gegevens krijgt. **Beveiligingsupdates.** Beveiligingsupdates worden opgevolgd en geïnstalleerd volgens een gedocumenteerd patch managementproces. **Logboekregistratie**. Verwerker registreert de toegang tot en het gebruik van zijn informatiesystemen die klantendata bevatten, met inbegrip van de gebruikers ID, de tijd en de desbetreffende activiteit.

CONCEPT

Domein	Technische / organisatorische maatregel
Communicatie beveiliging	**Netwerksegregatie.** Verwerker heeft een netwerksegmentatiebeleid en controles ingevoerd om te vermijden dat personen toegang krijgen tot communicatie en systemen waarvoor ze geen autorisatie hebben. **Transfer buiten eigen netwerk** Verwerker versleutelt klantengegevens die worden verzonden via publieke, niet-vertrouwde netwerken. **Informatieoverdracht.** Overdracht van klantengegevens aan derde partijen geschiedt enkel na het sluiten van een formele schriftelijke overeenkomst.
Verwerving, ontwikkeling en onderhoud van informatiesystemen	**Beveiligingsvereisten**. De vereisten voor de bescherming van gegevens en systemen worden geanalyseerd en gespecificeerd. **Controle over wijzigingen.** Verwerker heeft een formeel wijzigingsbeheerproces geïmplementeerd om ervoor te zorgen dat wijzigingen in operationele systemen en toepassingen plaatsvinden op een gecontroleerde wijze.
Leveranciersrelaties	**Keuze van leveranciers.** Verwerker handhaaft een selectieproces waarbij het de beveiliging en privacy praktijken van een leverancier met betrekking tot gegevensverwerking evalueert. **Contractuele verplichtingen.** Leveranciers met toegang tot klantengegevens zijn onderworpen aan verplichtingen inzake gegevensbescherming en deze worden formeel opgenomen in leverancierscontracten
Beheer van informatiebeveiligings-incidenten	**Incident response.** Verwerker houdt een register van beveiligingsinbreuken bij met een beschrijving van de inbreuk, het tijdstip, de gevolgen van de inbreuk, de naam van de melder en van degene aan wie de inbreuk werd gemeld. **Notificatie van incidenten.** In geval van een informatiebeveiligingsincident dat impact heeft op de vertrouwelijkheid of integriteit van klantengegevens, zal Verwerker, zonder onredelijke vertraging, de klant hiervan informeren (zoals beschreven in de overeenkomst).
Bedrijfscontinuïteit	**Noodherstel.** Verwerker handhaaft een noodherstelplan voor de datacentra waar zich informatiesystemen van Verwerker bevinden die klantengegevens verwerken. **Redundantie.** De redundante opslag en procedures voor gegevensherstel van Verwerker zijn ontworpen met als doel klantengegevens te herstellen in hun laatst geback-upte staat voor het tijdstip waarop ze verloren gegaan zijn of vernietigd werden.
Naleving	**Beveiligingsevaluaties.** De naleving van informatiebeveiligingscontroles wordt op periodieke basis onafhankelijk geëvalueerd en aan het management gerapporteerd.

CONCEPT