Verwerkersovereenkomst persoonsgegevens

Partijen

1. Verantwoordelijke, te weten .....

   statutair gevestigd te .....

   vertegenwoordigd door .....

   hierna te noemen: Opdrachtgever;

2. Verwerker, te weten Psantis B.V., statutair gevestigd te Heerhugowaard en vertegenwoordigd door J. Kern, hierna te noemen: Primosite[1] ;

Overwegende dat

1. Per 25 mei 2018 de Algemene Verordening Gegevensbescherming (AVG) voor alle lidstaten van de Europese Unie geldt;
2. Partijen eerder een overeenkomst zijn aangegaan waarop de AVG van toepassing is en waarop de Algemene Voorwaarden van Primosite van vóór 25 mei 2018 van toepassing zijn;
3. Opdrachtgever niet de gewijzigde Algemene Voorwaarden van Primosite accepteert die gelden vanaf 25 mei 2018;
4. Volgens de definities in de AVG Opdrachtgever de 'verwerkingsverantwoordelijke' is en Primosite de 'verwerker';

Komen als volgt overeen

Primosite zal persoonsgegevens als bedoeld in de AVG alleen verwerken voor en in opdracht van Opdrachtgever om uitvoering te geven aan de overeenkomst. Primosite heeft geen zeggenschap over de persoonsgegevens die door de Opdrachtgever beschikbaar worden gesteld. Zonder noodzaak, gezien de aard van de door de Opdrachtgever verstrekte opdracht, expliciete toestemming van de Opdrachtgever of wettelijke verplichting zal Primosite de gegevens niet aan derden verstrekken of voor andere doeleinden verwerken, dan voor de overeengekomen doeleinden. Opdrachtgever garandeert dat de persoonsgegevens verwerkt mogen worden op basis van een in de AVG genoemde grondslag.

[1] Primosite® is een geregistreerd merk en een handelsnaam van Psantis B.V.

Voor het gebruik van de door programmatuur van Primosite waarvoor Opdrachtgever een gebruiksrechtlecentie heeft, verstrekt Primosite aan Opdrachtgever toegangs- of identificatiecodes. Opdrachtgever behandelt de toegangs- en identificatiecodes vertrouwelijk en met zorg. Primosite is nimmer aansprakelijk voor schade of kosten die het gevolg zijn van gebruik of misbruik dat van toegangs- of identificatiecodes wordt gemaakt.

Primosite neemt passende technische en organisatorische maatregelen om de persoonsgegevens van de Opdrachtgever te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. Deze maatregelen worden aangemerkt als een passend beveiligingsniveau in de zin van de AVG. De Opdrachtgever is gerechtigd om in overleg met Primosite tijdens de looptijd van de overeenkomst door een onafhankelijke deskundige de naleving hiervan te controleren, bijvoorbeeld door middel van het uitvoeren van een audit. Primosite zal op grond van wet- en regelgeving, alle informatie beschikbaar stellen aan toezichthoudende organisaties indien hiervoor een verzoek wordt ingediend. Tevens verplicht Primosite de subbewerker, zoals hieronder benoemd, eveneens te voldoen aan een dergelijk verzoek van deze toezichthouders. De Opdrachtgever zal alle kosten in verband met deze controle dragen.

De Autoriteit Persoonsgegevens zal eerst aan de verwerkersverantwoordelijke een bindende aanwijzing geven voordat de Autoriteit Persoonsgegevens een bestuurlijke boete op kan leggen. De verwerkersverantwoordelijke zal Primosite direct op de hoogte stellen van deze bindende aanwijzing. Primosite zal er alles aan doen wat in redelijkheid van haar verwacht kan worden om de naleving mogelijk te maken. De kosten hiervoor komen, voor zover zij niet zijn toe te schrijven aan opzet of ernstige verwijtbare nalatigheid aan de kant van Primosite, voor rekening van Opdrachtgever. Als Primosite niet doet wat in redelijkheid van haar gevraagd kan worden waardoor er een boete volgt, of als de Autoriteit Persoonsgegevens direct een boete oplegt omdat sprake is van opzet of ernstige verwijtbare nalatigheid aan de kant van Primosite, dan geldt de toepasselijke aansprakelijkheidsbeperking als omschreven in deze algemene voorwaarden niet.

De datacenters waar de servers van Primosite zijn gehuisvest, bevinden zich uitsluitend in Nederland en vallen onder Europese wet- en regelgeving en voldoen aan de strenge Europese wetgeving met betrekking tot logische en fysieke toegangsbeveiliging en continuïteit. De datacenters zijn ISO 27001 gecertificeerd. Primosite heeft gekozen voor datacenters van Solcon en deze is hiermee subverwerker van de Opdrachtgeverdata.

Primosite is aansprakelijk voor schade in het kader van persoonsgegevens door handelen of nalaten van haar subverwerker(s) waarbij de aansprakelijkheidsbeperking uit de algemene voorwaarden geldt. De toepasselijke aansprakelijkheidsbeperking geldt niet indien er bij de subverwerker sprake is van grove nalatigheid of opzettelijk wangedrag. Primosite is niet aansprakelijk in geval van overmacht (zoals gedefinieerd in de algemene voorwaarden) aan de kant van de subverwerker.

Primosite zal geen nieuwe subverwerkers gegevens laten verwerken zonder de Opdrachtgever daarover tijdig te informeren. De Opdrachtgever kan, indien hij dat nodig acht, bezwaar maken bij Primosite tegen de subverwerker en in het uiterste geval heeft de Opdrachtgever de mogelijkheid om de overeenkomst te beëindigen.

Medewerkers en subverwerkers van Primosite hebben volledige toegang tot de Opdrachtgevergegevens voor technisch en functioneel onderhoud aan de Programmatuur, het maken van back-ups en voor het verlenen van support.

De AVG vereist dat eventuele datalekken gemeld worden aan de Autoriteit Persoonsgegevens door de verwerkingsverantwoordelijke van de data. Primosite zal daarom zelf geen meldingen doen bij de Autoriteit Persoonsgegevens. Uiteraard zal Primosite als verwerker de Opdrachtgever juist, tijdig en volledig informeren over relevante incidenten, zodat de Opdrachtgever als verwerkingsverantwoordelijke aan zijn wettelijke verplichtingen kan voldoen. De Beleidsregels meldplicht datalekken van de Autoriteit Persoonsgegevens geven hierover meer informatie.

Voor het bepalen van een datalek, gebruikt Primosite de AVG en de Beleidsregels meldplicht datalekken als leidraad. Onder een datalek vallen alle beveiligingsincidenten waardoor de bescherming van persoonsgegevens op enig moment is doorbroken of waardoor de persoonsgegevens blootgesteld zijn aan verlies of onrechtmatige verwerking. Het kan bijvoorbeeld gaan om het verlies van een USB-stick of computer, inbraak door een hacker, verzending van een e-mail waarin de e-mailadressen zichtbaar zijn voor alle geadresseerden, een malwarebesmetting of een calamiteit zoals brand in een datacenter.

Indien de Opdrachtgever een (voorlopige) melding verricht bij de Autoriteit Persoonsgegevens en/of de betrokkene(n) over een datalek bij Primosite, terwijl zonder meer voor de Opdrachtgever duidelijk is dat bij Primosite geen sprake is van een datalek dan is de Opdrachtgever aansprakelijk voor alle door Primosite geleden schade en kosten. De Opdrachtgever is daarnaast verplicht een dergelijke melding direct in te trekken.

Indien blijkt dat bij Primosite sprake is van een datalek, dat door de Opdrachtgever gemeld moet worden aan de Autoriteit Persoonsgegevens en/of de betrokkene(n), dan zal Primosite de reguliere contactpersoon van Opdrachtgever hierover zo spoedig mogelijk informeren nadat Primosite bekend is geworden met het datalek. Om dit te realiseren zorgt Primosite ervoor dat al haar medewerkers in staat zijn en blijven om een datalek te constateren en verwacht Primosite van haar opdrachtnemers dat zij Primosite in staat stelt om hier aan te kunnen voldoen. Voor de duidelijkheid: als er een datalek is bij een leverancier van Primosite, dan meldt Primosite dit uiteraard ook. Primosite is het contactpunt voor de Opdrachtgever. De Opdrachtgever hoeft geen contact op te nemen met de leveranciers van Primosite.

In het geval van een datalek probeert Primosite aan Opdrachtgever direct alle informatie te verstrekken die Opdrachtgever nodig heeft om een volledige melding bij de Autoriteit Persoonsgegevens en/of de betrokkene(n) te verrichten. Indien deze informatie nog niet bekend is, bijvoorbeeld omdat het datalek door Primosite wordt onderzocht, dan zal Primosite de Opdrachtgever de informatie verstrekken die de Opdrachtgever nodig heeft om in ieder geval eerst een voorlopige melding bij de Autoriteit Persoonsgegevens en/of de betrokkene(n) te kunnen verrichten. Hierbij volgt Primosite de informatielijst uit de eerder genoemde beleidsregels. Dit bevat in ieder geval de aard van de inbreuk, een beschrijving van de geconstateerde en de vermoedelijke gevolgen van de inbreuk en de getroffen en te treffen maatregelen om de negatieve gevolgen van het datalek te beperken en te verhelpen.

De AVG geeft aan dat een datalek 'onverwijld' moet worden gemeld. Dit is volgens de Autoriteit Persoonsgegevens zonder onnodige vertraging en zo mogelijk niet later dan 72 uur na ontdekking. Primosite informeert de Opdrachtgever daarom zo snel mogelijk, uiterlijk binnen 48 uur na het ontdekken van een datalek, zodat de Opdrachtgever tijdig de melding kan doen bij de Autoriteit Persoonsgegevens. Primosite zal de Opdrachtgever op de hoogte houden over de voortgang en de maatregelen die getroffen worden. Primosite maakt hierover afspraken met de reguliere contactpersoon bij de initiële melding. In ieder geval houdt Primosite de Opdrachtgever op de hoogte in geval van een wijziging van de situatie, het bekend worden van nadere informatie en over de maatregelen die getroffen worden.

Aldus overeengekomen en ondertekend:

Verantwoordelijke:

Ondertekend voor en namens Opdrachtgever:

Naam: .....

Functie: .....

Plaats: .....

Datum: .....

Handtekening: .....

Bewerker:

Ondertekend voor en namens: Primosite

Naam: J. Kern

Functie: Directeur

Plaats: Heerhugowaard

Datum: .....

Handtekening: .....