Verwerkersovereenkomst

Verwerkingsverantwoordelijke	⇨	Filmhuis Lumen
Verwerker	⇨	Cramgo BV / ActiveTickets
Datum	⇨	26-4-2018
Voor akkoord Verwerkings-verantwoordelijke	⇨	«voor_akkoord»
Datum / Plaats	⇨	
Ondertekening	⇨	
Voor akkoord Verwerker	⇨	José Manuel Martinez Martinez
Datum / Plaats	⇨	26-4-2018, Utrecht
Ondertekening	⇨	

Inhoud

1. Doelstelling

1.1 Wij, Cramgo B.V. t.h.o.d.n. ActiveTickets, gaan (gingen) met u, onze klant en tevens Verwerkingsverantwoordelijke, een Overeenkomst aan met betrekking tot het beschikbaar stellen van (kaartverkoop-)software van ActiveTickets en daaraan verbonden producten en diensten. Hierbij is inbegrepen het beheren van de online databases en servers waarop ActiveTickets draait, waarvoor met u een hosting abonnement is afgesloten.

1.2 Wij en u verwerken voor de uitvoering van deze Overeenkomst Persoonsgegevens.
1.3 In deze Verwerkersovereenkomst maken we afspraken over de gegevensverwerking en de technische en organisatorische maatregelen die we treffen om bij de uitvoering van de Overeenkomst te handelen conform de Algemene Verordening Gegevensbescherming (verder: AVG).

2. Definities

Voor de betekenis van de hierna gebruikte begrippen verwijzen wij naar de AVG.

3. Totstandkoming, duur en beëindiging van deze overeenkomst

3.1 Deze Verwerkersovereenkomst gaat in tegelijk met onze Overeenkomst met u of, indien deze Overeenkomst al langer bestond, op de datum van ondertekening door beide partijen.
3.2 Deze Verwerkersovereenkomst is onderdeel van de Overeenkomst en geldt zolang de Overeenkomst duurt. Als de Overeenkomst eindigt, eindigt deze Verwerkersovereenkomst automatisch.
3.3 Na beëindiging van deze Verwerkersovereenkomst zullen de langer lopende verplichtingen voor u en ons, waarbij de Persoonsgegevens van Verwerkingsverantwoordelijke betrokken zijn, zoals het melden van Datalekken en de plicht tot geheimhouding, voortduren.

4. Algemene beschrijving van de verwerking

4.1 Wij verwerken de Persoonsgegevens in opdracht van u.
4.2 U moet eventuele risicovolle verwerking van Persoonsgegevens tot 25 mei 2018 bij de Autoriteit Persoonsgegevens melden.
4.3 U bepaalt de aard en de samenstelling van de Persoonsgegevens die worden verwerkt en met welk doel.
4.4 U stelt ons op de hoogte wanneer de samenstelling van de verzamelde gegevens wijzigt en ook of en per wanneer zogenaamde Bijzondere Persoonsgegevens worden verwerkt in onze software.
4.5 Wij verwerken Persoonsgegevens op geen andere manier, dan vastgelegd in deze overeenkomst, tenzij u hier vooraf schriftelijk toestemming voor geeft.
4.6 Bijlage 1 vermeldt welke persoonsgegevens wij verwerken en met welk gerechtvaardigd doel.
4.7 Wij houden ons aan de wet en verwerken gegevens op een zorgvuldige en transparante wijze.
4.8 We zullen – naast de in deze overeenkomst / bijlagen genoemde Sub-Verwerkers – geen andere personen of organisaties inschakelen voor het verwerken van de Persoonsgegevens zonder voorafgaande mededeling (noodgevallen uitgezonderd).
4.9 Wanneer we derde partijen inschakelen, zullen deze partijen minimaal voldoen aan de eisen in deze Verwerkersovereenkomst.

5. Instructies verwerking

5.1 Wij faciliteren in uw opdracht de registratie van Persoonsgegevens van uw bezoekers via de software, door middel van importeerfuncties en formulieren voor bezoekersregistratie in de box office, webshop en backoffice.
5.2 Persoonsgegevens van bezoekersaccounts worden opgeslagen in online databases en/of (via replicaties) in (een) lokale database(s) in uw eigen beheer, indien van toepassing voor uw situatie. We maken de gegevens in de online database op overeengekomen wijze toegankelijk voor u.
5.3 Voor bezoekersgegevens die zijn ingevoerd aan de kassa via het Snelle Registratieformulier geldt dat geen beheersbaar bezoekersaccount wordt aangemaakt. Deze Persoonsgegevens worden enkel voor korte tijd bewaard in de database ten behoeve van de afwikkeling van een enkele transactie en voor Servicedoeleinden. Deze gegevens worden volledig verwijderd, direct na het verstrijken van de datum van de voorstelling of dienst waarop de transactie betrekking heeft.
5.4 We registreren en verwerken verkooptransacties tussen u en uw bezoekers in de software van ActiveTickets. In de software worden tickets gegenereerd en naar bezoekers digitaal verzonden of via de kassa beschikbaar gemaakt voor prints in verschillende gangbare formats. Betalingen vinden plaats buiten onze software op het gekoppelde betaalplatform van uw keuze. ActiveTickets koppelt alleen met betaalplatforms die PCI-compliant zijn. De uitwisseling van noodzakelijke Persoonsgegevens met het betaalplatform vindt alleen versleuteld plaats.
5.5 In uw opdracht ontsluiten we Persoonsgegevens van bezoekers op overeengekomen wijze naar de in Bijlage 1 vermelde Ontvangers via koppelingen en API's.
5.6 Voor Servicedoeleinden en voor het oplossen van onverhoopte verstoringen in het systeem verwerken wij ook Persoonsgegevens van bezoekers in het mailsysteem van onze Supportafdeling. Voor zover hierbij bankrekeninggegevens of andere gevoelige persoonsgegevens aan ons beschikbaar worden gesteld door u of vanuit de provider van het betaalplatform, blijven deze Persoonsgegevens maximaal twee maanden bewaard in ons systeem, tenzij het voor het oplossen van een storing noodzakelijk is om deze langer te bewaren.
5.7 In verband met onze dienstverlening aan u verwerken we in ons mailsysteem, ons CRM-systeem en ActiveTickets Persoonsgegevens van personen die namens u contacten onderhouden met onze medewerkers. Voor administratieve doeleinden blijven deze maximaal 7 jaar bewaard na het eindigen van de Overeenkomst tussen u en ons. De Persoonsgegevens worden niet aan derden verstrekt tenzij u hier toestemming voor heeft gegeven of dit in het kader van wetgeving noodzakelijk is.

6. Beveiliging van Persoonsgegevens

6.1 Rekening houdend met de stand van de techniek, de uitvoeringskosten, en met de aard, omvang, context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, treffen wij en u alle passende organisatorische en technische maatregelen conform de wetgeving om de verwerkte Persoonsgegevens voldoende te beveiligen.
6.2 Onze beveiligingsmaatregelen zijn gericht op het voorkomen van verlies en onrechtmatige verwerking en op het waarborgen van de juiste toegang, beschikbaarheid, integriteit en vertrouwelijkheid van de gegevens. Een overzicht van de belangrijkste maatregelen is opgenomen in Bijlage 2.
6.3 Op uw verzoek en binnen een acceptabele termijn zullen we nadere informatie verstrekken over het actuele informatiebeveiligingsbeleid, op voorwaarde dat u informatie en documentatie hieromtrent vertrouwelijk behandelt en deze niet zonder onze toestemming aan derden beschikbaar stelt, tenzij dit vanuit de wet noodzakelijk is (bijvoorbeeld in verband met een Datalek).
6.4 Beide partijen zorgen ervoor dat communicatie van Persoonsgegevens via netwerken of andere media versleuteld plaatsvindt met technologie die volgens actuele standaarden voldoende bescherming biedt.
6.5 Beide partijen zorgen voor een passend beveiligingsniveau van de lokale systemen waarop ActiveTickets draait (voorzien van de juiste updates e.d.).
6.6 Beide partijen beperken toegangs- en gebruikersrechten van medewerkers zodanig via ingestelde rollen en rechten, dat een medewerker alleen beschikt over de noodzakelijke rechten voor de uitoefening van zijn/haar taken. Beide partijen instrueren alle medewerkers die toegang tot Persoonsgegevens hebben over de geldende procedures en wetgeving in de zorg voor en bescherming van deze gegevens.
6.7 Beide partijen hanteren een wachtwoordbeleid dat is gericht op het voorkomen van misbruik en ongeoorloofde en onbedoelde toegang tot databases met Persoonsgegevens. U moet zorgvuldig omgaan met door ons aan u verstrekte gebruikersnamen en wachtwoorden van gebruikersaccounts en deze niet zonder onze toestemming aan derden beschikbaar stellen.

7. Sub-Verwerkers

7.1 Om een optimale beschikbaarheid, bereikbaarheid en veerkracht van de online servers en databases te kunnen garanderen, worden de databases beheerd door externe Data Hostingpartijen die voldoende geografische spreiding kunnen waarborgen met het oog op Disaster Recovery.
7.2 Wij werken alleen samen met hostingpartijen die beschikken over de juiste certificeringen om een passend beveiligingsniveau te kunnen garanderen. Dit betreft thans (april 2018): Microsoft Azure voor de hosting van de actieve databases en Amazon Web Services voor back-ups.
7.3 Alle mailverkeer vanuit ActiveTickets, inclusief ticketverzending, verloopt via het mailplatform van derde Sub-Verwerker SendGrid om – ook tijdens piekbelasting – een betrouwbare en stabiele afleverperformance te kunnen waarborgen. SendGrid beschikt over de juiste certificeringen om een passend beveiligingsniveau te kunnen garanderen conform de AVG.
7.4 Uiterlijk met ingang van 25 mei 2018 zijn de noodzakelijke overeenkomsten tussen ActiveTickets en de genoemde Sub-Verwerkers van toepassing die voldoen aan de vereisten van de AVG.
7.5 Met de ondertekening van deze overeenkomst geeft u toestemming voor de genoemde verwerking van Persoonsgegevens door de hierboven vermelde Sub-Verwerkers op de in artikel 8 genoemde locaties.
7.6 Wanneer er - in het belang van u als klant of in het belang van de bescherming van de privacy van Betrokkenen - dringende redenen zijn om de servers en databases onder te brengen bij andere hostingpartijen of de mailverzending ergens anders uit te besteden, dan mogen wij dit doen en zullen we u hierover zo spoedig mogelijk informeren, onverminderd uw recht hiertegen bezwaar te maken.

8. Locatie van data

8.1 De actieve databases met Persoonsgegevens worden door Microsoft Azure fysiek bewaard op verschillende locaties binnen de EU volgens de algemene eisen uit de wetgeving.
8.2 Encrypted back-ups worden door Amazon Web Services opgeslagen buiten de EU (Japan). Amazon biedt voldoende technische en contractuele waarborgen voor een beveiligingsniveau conform de richtlijnen in de AVG.
8.3 SendGrid slaat de data op in geografisch gespreide datacenters op wisselende locaties, zowel binnen als buiten de EU en maakt daarbij alleen gebruik van voldoende gecertificeerde hosting partijen. SendGrid geeft voldoende contractuele waarborgen voor een passend beveiligingsniveau conform de wetgeving.
8.4 We zullen behalve bij dringende omstandigheden geen Persoonsgegevens van u laten verwerken buiten de Europese Economische Ruimte (EER) door anderen dan bovengenoemde Sub-Verwerkers, zonder uw schriftelijke toestemming.

9. Geheimhouding

9.1 U en wij houden de Persoonsgegevens geheim en dragen ervoor zorg dat deze niet ter beschikking komen van derden, tenzij dit op basis van een wettelijke verplichting niet mogelijk is.
9.2 U en wij houden personeel en ingeschakelde hulppersonen aan de geheimhoudingsplicht, door deze in de desbetreffende (arbeids-)contracten op te nemen.

10. Toestemming Betrokkene

10.1 Uiterlijk met ingang van 25 mei 2018 verwerken u en wij alleen nog Persoonsgegevens in de software van bezoekers die hiervoor uitdrukkelijk toestemming hebben gegeven op een wijze die voldoet aan de vereisten volgens de AVG. We faciliteren de noodzakelijke toestemmingshandelingen in de software voor de verschillende manieren van bezoekersregistratie. Relevante gegevens met betrekking tot de gegeven toestemming worden vastgelegd op bezoekersniveau en aan u beschikbaar gesteld, zodat u kunt voldoen aan dit onderdeel van de documentatieplicht. U bent zelf verantwoordelijk voor de handelingen van minderjarigen en wilsonbekwamen.
10.2 Als de bezoekersregistratie plaatsvindt buiten onze software – waarbij via uw eigen website verzamelde bezoekersgegevens automatisch worden ingelezen in ons systeem – moet u (of uw webbouwer) ervoor zorg dragen dat op de juiste wijze toestemming is verkregen van de Betrokkene voor de gegevensverwerking.
10.3 De software biedt de mogelijkheid voor Betrokkenen om via een actieve handeling toestemming te geven voor het ontvangen van nieuwsbrieven, en zich af te melden (recht van bezwaar). Relevante gegevens met betrekking tot deze toestemming worden geregistreerd en beschikbaar gesteld.

11. Privacy rechten

11.1 Als eigenaar van uw eigen bezoekersdatabase bent u in de eerste plaats zelf verantwoordelijk voor het behandelen van verzoeken van een Betrokkene uit uw database die zijn of haar privacy rechten wil uitoefenen, onverminderd onze verplichtingen aangaande het op een gebruiksvriendelijke wijze faciliteren hiervan via de software. Deze privacy rechten bestaan uit een verzoek om inzage, verbetering, aanvulling, verwijdering of afscherming, bezwaar maken tegen de verwerking van Persoonsgegevens en een verzoek tot overdraagbaarheid van de eigen Persoonsgegevens.
11.2 Wij zullen hierbij zoveel mogelijk technisch ondersteunen via opties in het Bezoekersbeheer en het beschikbaar stellen van de noodzakelijke rapporten. We dragen zorg voor een adequate en tijdige anonimisering van data in geval van verwijderingsverzoeken. Voor zover van toepassing voor de wet zullen we ons inspannen om aan de in artikel 11.1 genoemde verplichtingen te voldoen.
11.3 Wij treffen de in verband met de wet noodzakelijke maatregelen om een vlotte toegang van bezoekers tot hun Persoonsgegevens te kunnen garanderen via daarvoor bestemde accountbeheerpagina's die beveiligd zijn met een persoonlijk wachtwoord. Dit wachtwoord is alleen versleuteld in de database opgeslagen.
11.4 Betrokkenen kunnen via de software een transparant overzicht van vastgelegde Persoonsgegevens en transactiegegevens verkrijgen in een gestructureerde, machine leesbare vorm (recht op inzage; overdraagbaarheid van gegevens); de vastgelegde gegevens bewerken (recht op correctie); hun wachtwoord wijzigen; hun bestelgeschiedenis anonimiseren en hun account verwijderen (recht op vergetelheid).
11.5 Bij het verwijderen van een bezoekersaccount worden alle gekoppelde transacties direct geanonimiseerd in de actieve database. Na verwijdering uit de actieve database blijven de Persoonsgegevens maximaal 4 weken bewaard in de back-up database bij Amazon. Daarna worden deze automatisch en volledig verwijderd.
11.6 Beperkte Persoonsgegevens van bezoekers die zich als gevolg van een ticketverzending of mailing kunnen bevinden in databases van SendGrid worden niet automatisch verwijderd bij het verwijderen van Persoonsgegevens uit databases die bij ons in beheer zijn. SendGrid zal zich zoveel mogelijk inspannen om Persoonsgegevens van een Betrokkene te verwijderen op een redelijke termijn als een Betrokkene hiertoe een verzoek indient volgens de afspraken met ActiveTickets. Als geen specifiek verzoek wordt ingediend voor verwijdering van data bij SendGrid, dan blijven deze maximaal een jaar bewaard in databases van SendGrid.
11.7 U zorgt voor correcte verwijzingen naar de juiste accountbeheerpagina's bij de integratie van de webshop in de eigen website om de toegankelijkheid van de Persoonsgegevens voor de Betrokkene voldoende te waarborgen. Als geen gebruik wordt gemaakt van de bestaande functionaliteit voor het online beheren van een bezoekersaccount, richt u dit zelf binnen de webshop in conform de wetgeving.
11.8 U neemt passende maatregelen om tijdig te kunnen voldoen aan de informatieplicht door middel van een heldere privacyverklaring voor bezoekers in eenvoudige bewoordingen die via een hyperlink gekoppeld kan worden aan onze online toestemming-functionaliteit.
11.9 Inactieve accounts verwijderen: wij zullen u via de software ondersteunen bij het identificeren van inactieve bezoekersaccounts om deze periodiek op een eenvoudige wijze te kunnen verwijderen op grond van een door uw organisatie te bepalen bewaartermijn.

12. Datalekken

12.1 Na het ontdekken van een Datalek zullen wij dit zo spoedig mogelijk, doch uiterlijk binnen 36 uur melden aan de door u aangewezen contactpersoon (contactgegevens in Bijlage 3), zodat deze hiervan zo nodig melding kan doen bij de toezichthoudende autoriteit. Als u een Datalek ontdekt moet u dit onmiddellijk bij ons melden zodat wij passende maatregelen kunnen treffen.
12.2 We zullen bij het melden van een Datalek de informatie verstrekken die is aangegeven in Bijlage 3.
12.3 Na het melden van een Datalek zullen we u op de hoogte houden van nieuwe ontwikkelingen en maatregelen om de omvang van het Datalek te beperken en te beëindigen en een soortgelijk incident in de toekomst te voorkomen.
12.4 Wij doen zelf geen melding van een Datalek aan de Toezichthouder, noch informeren wij Betrokkenen hierover. Dit is uw taak.
12.5 Eventuele kosten om het Datalek op te lossen en in de toekomst te kunnen voorkomen, komen voor rekening van de partij die verantwoordelijk is voor het ontstaan ervan.

13. Andere verplichtingen

13.1 We helpen u waar nodig bij het nakomen van uw verplichtingen in relatie tot de AVG, zoals bij het melden van Datalekken, het uitvoeren van een DPIA en bij voorafgaande raadpleging.
13.2 Documentatieplicht: U moet relevante wijzigingen wat betreft contactpersonen voor het melden van een Datalek of aanpassingen in de aard van de verzamelde gegevens tijdig aan ons doorgeven.
13.3 Wij stellen u desgevraagd alle informatie ter beschikking die noodzakelijk is om aan te tonen dat wij aan alle aan ons in het kader van de Verwerking van Persoonsgegevens gestelde eisen hebben voldaan.

14. Bewaartermijn en verwijdering van Persoonsgegevens

14.1 Na het beëindigen van de Verwerkersovereenkomst zullen wij de in het kader van de Overeenkomst verzamelde Persoonsgegevens exporteren en aan u overdragen op de overeengekomen datum, tenzij u aangeeft geen interesse meer te hebben in de Persoonsgegevens. De kosten voor het maken van de export zullen aan u worden doorberekend. Direct na het exporteren gaat de actieve database offline. De back-up van de database blijft na het offline gaan maximaal vier weken bestaan.
14.2 Wij zullen back-ups van Persoonsgegevens of kopieën daarvan op een zorgvuldige manier vernietigen na het verstrijken van de wettelijke bewaartermijn en/of op uw verzoek.
14.3 U moet ons na het beëindigen van de Overeenkomst toegang geven tot eventuele lokale servers bestemd voor replicaties om kopieën te kunnen verwijderen.
14.4 Wij zullen u per omgaande informeren, wanneer de verwijdering of vernietiging van uw Persoonsgegevens is uitgevoerd.
14.5 Indien er bij het eindigen van de Overeenkomst via een export een overdracht plaatsvindt van Persoonsgegevens naar een ander ticketing- of planningssysteem, dan bent u verplicht zelf de Betrokkenen te informeren over de verwerking van de Persoonsgegevens door de nieuwe partij en hiervoor op de juiste wijze toestemming te vragen.

15. Aansprakelijkheid

15.1 Wij zijn enkel aansprakelijk voor schade en nadeel geleden door het niet-nakomen van de wet en de bepalingen uit deze Verwerkersovereenkomst, voor zover dit is ontstaan door onze werkzaamheden.
15.2 Wij zijn enkel aansprakelijk voor een aan u door Toezichthouder opgelegde boete als de geleden schade een gevolg is van onrechtmatig of nalatig handelen door ons.
15.3. Onze aansprakelijkheid wordt verder beperkt door de Overeenkomst met u en onze algemene voorwaarden.

16. Audits

16.1 Wij werken mee aan audits door een geaccrediteerde externe deskundige in uw opdracht of die van een derde partij, mits u een redelijke termijn in acht neemt om ons over deze intentie te informeren en redelijke maatregelen neemt om ervoor te zorgen dat de audit qua planning en uitvoering zo min mogelijk verstorend is voor de dagelijkse operationele processen binnen de organisatie ActiveTickets. We stellen hierbij alle relevante informatie beschikbaar om te controleren of ActiveTickets en u zich houden aan de verplichtingen zoals vastgelegd in deze overeenkomst. Voordat een dergelijke audit aanvangt, stellen de partijen in onderlinge overeenstemming de omvang, het tijdstip en de duur van de audit vast.
16.2 Wanneer u of wij vinden dat een wijziging in de beveiligingsmaatregelen noodzakelijk is om aan de wet- en regelgeving te (blijven) voldoen, treden wij in overleg over de wijziging daarvan.

17. Slotbepalingen

17.1 Deze Verwerkersovereenkomst is onderdeel van de Overeenkomst en is niet apart opzegbaar. Alle rechten en verplichtingen uit de Overeenkomst en bijbehorende algemene voorwaarden zijn daarom ook van toepassing op de Verwerkersovereenkomst.
17.2 Bij eventuele tegenstrijdigheden tussen de bepalingen in de Verwerkersovereenkomst en de Overeenkomst, gelden de bepalingen uit deze Verwerkersovereenkomst, tenzij hier of in de overeenkomst anders bepaald.
17.3 Afwijkingen van deze Verwerkersovereenkomst zijn slechts geldig wanneer wij dit samen schriftelijk afspreken.

Bijlage 1 - Overzicht Verwerking Persoonsgegevens

WELKE PERSOONSGEGEVENS WORDEN VERWERKT?

1. Persoonsgegevens van uw klanten/bezoekers

In en door middel van de software van ActiveTickets worden Persoonsgegevens van uw bezoekers verzameld, vastgelegd, opgeslagen, geraadpleegd, verstrekt, gewijzigd, gebruikt voor het mogelijk maken van verkooptransacties en/of het versturen van mailberichten, en gewist of vernietigd.

- De Persoonsgegevens worden voor u toegankelijk gemaakt voor inzage en bewerking via gebruikersaccounts beveiligd met een persoonlijk wachtwoord.
- U kent zelf in het systeem de door u gewenste rechten en bevoegdheden toe aan de gebruikers die namens u toegang hebben tot de gegevens.
- ActiveTickets verwerkt de gegevens voor geen ander doel dan het tot stand brengen van verkooptransacties en het verlenen van service aan u aangaande de afhandeling van deze transacties.

Normale Persoonsgegevens
De volgende standaard Persoonsgegevens van bezoekers (kunnen door u) worden verwerkt in ActiveTickets via bezoekersregistratieformulieren en via de backoffice:

- e-mailadres, voornaam, achternaam, adresgegevens, geslacht, telefoon- of faxnummer(s), geboortedatum, organisatie, functie, taalachtergrond, opleiding, interesses en nieuwsbriefvoorkeuren, IP-adres.

Bijzondere en/of gevoelige Persoonsgegevens
De volgende gegevens kunnen worden verwerkt in ActiveTickets maar vallen niet onder de standaard verwerking. Geef hieronder aan of/welke van onderstaande gegevens in het kader van de Overeenkomst worden verwerkt en met welk gerechtvaardigd doel:

Persoonsgegeven	Doel	Ja/nee
Foto		
Bankrekeninggegevens		
Nationaal identificatienummer		

Vrije invoervelden
Vrije invoervelden in ActiveTickets kunnen worden gebruikt voor aanvullende Persoonsgegevens, zoals interesses. Deze velden mogen echter niet door u worden aangewend voor het registreren van gevoelige gegevens waaronder inbegrepen: gegevens over ras of etniciteit, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, het lidmaatschap van een vakbond, genetische gegevens, gegevens over gezondheid of over iemands seksueel gedrag of seksuele gerichtheid.

Cookies
ActiveTickets gebruikt voor de werking van de winkelwagen alleen functionele sessie-cookies; deze worden per sessie aangemaakt en zijn alleen tijdens een sessie geldig. ActiveTickets gebruikt geen andere cookies (bijvoorbeeld trackingcookies).

Verwerking van Persoonsgegevens van bezoekers voor Supportdoeleinden
De supportafdeling van ActiveTickets verwerkt Persoons- en transactiegegevens van individuele bezoekers buiten de kaartverkoopsoftware in mailsystemen bedoeld voor onze dienstverlening aan u. Dit gebeurt wanneer uzelf of uw betaalplatformprovider deze gegevens verstrekt aan ons om

eventuele storingen te kunnen verhelpen en om te kunnen testen of een probleemoplossing succesvol is.

Kopieën van bevestigingsmails van individuele bestellers die Persoonsgegevens bevatten, ontvangen wij alleen in opdracht van u en indien dit voor het verhelpen van een storing of het testen van de werking van de functionaliteit van ticketverzending noodzakelijk is. Wij gebruiken deze Persoonsgegevens voor geen ander doel dan hier omschreven en niet langer dan daarvoor noodzakelijk.

Ontsluiting van Persoonsgegevens naar derden
Naast de in bijlage 4 genoemde Sub-Verwerkers voor de hosting van de databases en servers en voor ticketverzending, ontsluit ActiveTickets in het kader van deze Overeenkomst in uw opdracht Persoonsgegevens van bezoekers aan de volgende derde partijen via Webservices (bijvoorbeeld een CRM-partij of planningssysteem):

Naam derde partij	Web services	Doel

2. Persoonsgegevens van contactpersonen binnen uw organisatie

ActiveTickets registreert naast bezoekersgegevens ook Persoonsgegevens van personen die namens u contact onderhouden met ons ten behoeve van onze dienstverlening aan u en voor het versturen van mailingen over het gebruik van de software en andere voor uw organisatie relevante nieuwsberichten. U hebt altijd het recht personen uit onze bestanden te laten verwijderen of personen voor de nieuwsbrieven af te melden.

De volgende Persoonsgegevens van uw contactpersonen worden vastgelegd in onze informatiesystemen (CRM systeem, mailsysteem, ActiveTickets): naam, mailadres organisatie of privé mailadressen (op uw verzoek of op verzoek van Betrokkene), functie, telefoon- en adresgegevens organisatie, nieuwsbriefvoorkeuren.

HOE LANG BLIJVEN DE PERSOONSGEGEVENS BEWAARD?

Bewaartermijnen persoonsgegevens bezoekers:

Normale bezoekersregistratie (online/kassa) en geïmporteerde bezoekersaccounts	Zo lang als voor de uitvoering van deze overeenkomst noodzakelijk is. U bepaalt zelf de bewaartermijn van inactieve accounts (de maximale bewaartermijn is 2 jaar).
Snelle bezoekersregistratie (kassa)	Vanaf het moment van de transactie tot en met de datum van de opvoering/het evenement waarop de transactie betrekking heeft (daarna

	worden de Persoonsgegevens verwijderd)
Bezoekersgegevens in Supportsystemen van ActiveTickets	Gevoelige persoonsgegevens: maximaal 2 maanden. Normale persoonsgegevens: voor de duur van de Overeenkomst tot maximaal 7 jaar na het eindigen ervan.

Persoonsgegevens van uw contactpersonen blijven minimaal bewaard voor de duur van de Overeenkomst en maximaal zeven jaar na het eindigen ervan.

VERWIJDERING VAN PERSOONSGEGEVENS

Een bezoeker kan via accountbeheerpagina's zijn bestelgegevens anonimiseren of zijn account zelf geheel verwijderen of hiertoe rechtstreeks een verzoek indienen bij de betreffende organisatie uit wiens naam de Persoonsgegevens zijn verzameld en vastgelegd, waarna het account via de back-office van ActiveTickets verwijderd kan worden.

Gevolgen
Na het verwijderen van een account blijft de bestelgeschiedenis voor administratieve doeleinden bewaard in de database, maar deze is niet meer te herleiden naar een identificeerbaar persoon (geanonimiseerd). De Persoonsgegevens zelf worden direct verwijderd uit de actieve database. De Persoonsgegevens blijven maximaal 4 weken bewaard in de back-up van de database.

Bijlage 2 - Informatiebeveiliging

In deze Bijlage worden de belangrijkste, algemene technische en organisatorische maatregelen beschreven die gericht zijn op het voorkomen van ongeautoriseerde toegang en gebruik, en ongewenst verlies of aantasting van persoonsgegevens.

De maatregelen richten zich op het waarborgen van de betrouwbaarheid van systemen, technische en organisatorische processen en data ten aanzien van de volgende onderdelen: **beschikbaarheid – integriteit – vertrouwelijkheid – controleerbaarheid – beheersbaarheid**.

1. AANSLUITING BIJ STANDAARDEN VOOR INFORMATIEBEVEILIGING

ActiveTickets streeft ernaar het informatiebeveiligingsbeleid in te richten en actueel te houden conform de standaarden van de Code voor Informatiebeveiliging (ISO 27001/27002), en de standaardnorm van de *ICT-Beveiligingsrichtlijnen voor Webapplicaties* van het NCSC. ActiveTickets heeft een certificeringstraject in voorbereiding (2018).

2. DATA-OPSLAG

De databases met persoonsgegevens zijn ondergebracht bij Cloud-hostingpartijen die beschikken over de juiste ISO-certificeringen en de noodzakelijke contractuele garanties hebben afgegeven voor een passend beveiligingsniveau (fysieke servers, technisch en organisatorisch). 1. **Microsoft Azure (actieve databases)**: compliant met verschillende internationale standaarden voor informatiebeveiliging, waaronder de ISO 27001 en de ISO 27018 Cloud privacy standaard. Jaarlijks vinden audits plaats. Azure toont haar beveiligingsniveau aan met actuele certificaten (2018). 2. **Amazon Web Services (back-ups)**: compliant met verschillende internationale standaarden voor informatiebeveiliging, waaronder ISO 27001, ISO 27017 en ISO 27018 Cloud privacy standaard. Jaarlijks vinden audits plaats. AWS toont haar beveiligingsniveau aan met actuele certificaten (2018).
Risicospreiding: Er is gekozen voor geografisch gespreide datacenters in verschillende landen binnen en buiten de EU, en het hardware- en schijfmanagement is uitbesteed aan Microsoft Azure. Dit om risico's op eventuele downtime van systemen zoveel mogelijk te beperken, en ook in andere opzichten voldoende waarborgen te kunnen bieden waar het gaat om de veerkracht, beschikbaarheid en continuïteit van systemen en toegangsvoorziening tot servers en data(bases).
Opslag in derde land: Voor de back-ups in Japan (volgens de EU wetgeving een derde land) geldt dat AWS beschikt over een door de EC goedgekeurd, ongewijzigd modelcontract zonder aanvullingen als bedoeld in artikel 26, vierde lid, van richtlijn nr. 95/46/EG van het Europees Parlement en de Raad van de Europese Unie. Op basis hiervan wordt de dataopslag in Japan geacht te voldoen aan de beveiligingseisen conform AVG en is geen aparte vergunning nodig voor deze opslag.
Encryptie/versleuteling: Alle persoonsgegevens in de back-up databases zijn encrypted opgeslagen. Encrypted sleutels die toegang kunnen verschaffen tot deze persoonsgegevens zijn beveiligd opgeslagen bij ActiveTickets en alleen toegankelijk voor de directie van ActiveTickets.
Encryptie/versleuteling: Alle wachtwoorden van gebruikers en bezoekers in databases zijn alleen versleuteld opgeslagen door middel van een hashing-techniek op basis van een daarvoor geschikt algoritme behorend tot de RSA Laboratories Public-Key Cryptography Standards (PKCS).
Recht op vergetelheid: In geval van een verzoek van gegevenswissing door een Betrokkene worden persoonsgegevens automatisch verwijderd uit de databases van ActiveTickets. Bijbehorende transactiegegevens blijven opgeslagen, maar worden in database geanonimiseerd (zijn niet meer herleidbaar tot individuele Betrokkene).

3. TOEGANG TOT PERSOONSGEGEVENS

Toegangsvoorziening: Toegangscontrole op basis van een autorisatiestructuur is ingericht en ingeschakeld voor alle applicaties van ActiveTickets en daaraan gekoppelde klantdatabases (zowel op memberniveau als op gebruikersniveau).
Authenticatiemiddelen: Applicaties van ActiveTickets zijn alleen toegankelijk via gebruikersaccounts beveiligd met een wachtwoord. Er worden eisen gesteld aan de lengte (minimaal 8 tekens) en de samenstelling (minimaal 1 letter en cijfer of ander teken) van wachtwoorden die toegang geven tot applicaties van ActiveTickets en gekoppelde klantdatabases. Hierbij wordt aangesloten bij de gangbare richtlijnen voor veilige wachtwoorden.
Beveiliging inlogprocedures: Wachtwoorden worden niet getoond bij het invoeren.
Autorisaties/rechten: Authenticatie vindt plaats op basis van – aan de gebruiker toegekende – rollen en rechten met betrekking tot inzage en het kunnen bewerken van data. Gebruikers worden, zodra zij zijn geauthentiseerd, uitsluitend geautoriseerd voor de toegangsniveaus die bij hun functies horen. Bij ActiveTickets zijn de toegangsniveaus op hoofdlijnen onderverdeeld in een Operationele Admin en een Developer Admin.
Applicatiesessies: Gebruikerssessies na succesvolle aanmelding hebben altijd een beperkte duur (waarna automatisch wordt uitgelogd bij geen activiteit) en gebruikers kunnen zelf een sessie beëindigen. De single sign-on in webshop 3.0 heeft een tijdslimiet.

4. COMMUNICATIE & VERZENDING VAN PERSOONSGEGEVENS

Encryptie / versleuteling: Verzending van persoonsgegevens via de webshop van ActiveTickets vindt alleen versleuteld plaats via https (SSL). Minimale gegevensuitwisseling ten behoeve van de verwerking van de transacties vindt encrypted plaats tussen AT en betaalplatforms.
Encryptie / versleuteling: Het uploaden van bestanden via CRM Export naar FTP servers van onze klanten vindt plaats via een beveiligde verbinding. Uitzonderingen hierop zijn alleen expliciet in opdracht van en onder verantwoordelijkheid van de Ontvanger.
Encryptie / versleuteling: CRM dumps die digitaal worden verstuurd vanuit ActiveTickets worden versleuteld (door middel van gangbare tools) en voorzien van een wachtwoord.
Privacy bevorderend: Uitwisseling van persoonsgegevens via Web services is IP-restricted en kan versleuteld plaatsvinden.
Privacy bevorderend: ActiveTickets heeft een beleid voor het veilig verstrekken van gebruikersnamen en wachtwoorden aan gebruikers en/of contactpersonen, waarbij wordt vastgesteld of de ontvanger recht heeft op de authenticatiemiddelen.
Privacy bevorderend: bezoekerswachtwoorden worden in webshop 3.0 niet naar bezoeker per mail verstuurd, maar via link via https

5. CONTROLE & BEHEERSING

Hacking preventie: onnodige poorten waarmee servers of databases benaderd kunnen staan dicht; er is een blokkade op malicious requests; er is controle op SQL-injectie via formulieren (dit kan niet plaatsvinden).

paraaf Verwerkingsverantwoordelijke *paraaf Verwerker*

In ActiveTickets vastgelegde betaaltransacties zijn beveiligd tegen verwijderen (kunnen niet vanuit het systeem worden verwijderd).
Er wordt gebruik gemaakt van publicatieprofielen: Bezoeker krijgt in geval van een technische fout alleen algemene meldingen te zien (debug modus staat uit in productieomgeving); technische foutmeldingen worden alleen getoond aan ontwikkelaars van ActiveTickets.
Http logfiles, foutmeldingen logs en logs met betrekking tot de communicatie met betaalplatforms worden bijgehouden en er is een beleid op het beperkt bewaren van de logfiles.
Kantoorautomatisering bij ActiveTickets is voorzien van adequate beveiliging (firewalls, beveiligingsupdates kantoorapplicaties, mailserver met antispam/antiphishing e.d.) en deze wordt up-to-date gehouden.
Minimaal tweejaarlijks of vaker indien noodzakelijk vindt een evaluatie plaats van het beveiligingsbeleid/de beveiligingsmaatregelen en worden deze waar nodig aangepast aan de actuele situatie (via de PDCA-methodiek). ActiveTickets informeert gebruikers over eventuele wijzigingen in de getroffen maatregelen.

6. PERSONEEL & ORGANISATIE

Instructie: Relevant personeel is opgeleid om systemen en applicaties die worden ingezet voor de Verwerking van Persoonsgegevens op een adequate wijze in te richten en te beheren.
Procedures: Personeel ontvangt de noodzakelijke informatie over de verplichtingen van de privacywetgeving, datalekprocedure, en voorkomende cyberdreigingen, en ontvangen hiervoor instructies. Bijvoorbeeld wat betreft: het tijdig installeren van beveiligingsupdates op pc/laptop, het opslaan van gegevens, het per mail versturen van vertrouwelijke informatie, omgang met wachtwoorden, uitloggen en afsluitprocedure kantoor bij verlaten van de werkplek e.d. Eventuele downloads met persoonsgegevens in verband met supportwerkzaamheden worden na oplossen van het incident waarvoor de download bedoeld was verwijderd van pc's/laptops.
Toegang tot beheer: Waar van toepassing is functie-scheiding aangebracht om toegang tot ontwikkel-, test- en productie-omgevingen te scheiden en alleen de juiste medewerkers toegang te verschaffen tot de juiste systemen en informatie.
Arbeidscontracten: Met alle medewerkers van ActiveTickets is schriftelijk geheimhouding (tijdens en na afloop van het arbeidscontract) overeengekomen als vast onderdeel van het arbeidscontract.
Blokkering van toegangsrechten: Toegangsrechten van medewerkers van ActiveTickets voor inzage of bewerking van persoonsgegevens worden direct geblokkeerd als geen toegang meer nodig is voor de uitoefening van de functie en bij uitdiensttreding.

Versie
Deze bijlage is voor het laatst bijgewerkt op 20 april 2018.

Bijlage 3 – Proces melding Datalek

WAT IS EEN BEVEILIGINGSINCIDENT EN WANNEER MOET DIT GEMELD WORDEN?

Een Datalek is een beveiligingsincident waarbij Persoonsgegevens, die ActiveTickets namens u beheert, mogelijk (deels of geheel) verloren zijn gegaan of onbedoeld toegankelijk waren voor derden. 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.

Voorbeelden van beveiligingsincidenten die moeten worden gemeld bij de Toezichthoudende Autoriteit (in Nederland Autoriteit Persoonsgegevens).

- De website met logingegevens die gehackt is of toegankelijk is voor derden
- Verlies van laptop, smartphone of USB-stick met persoonsgegevens
- Inloggegevens van gebruikers die per ongeluk naar verkeerde personen zijn gestuurd
- Brieven of e-mails worden naar het verkeerde adres gestuurd
- Een aanval van een hacker op het ICT-systeem
- Een verloren of gestolen telefoon waarop persoonsgegevens aanwezig zijn

WAT TE DOEN BIJ TWIJFEL?

Wanneer u op basis van bovenstaande niet zeker weet of er sprake is van een beveiligingsincident, kunt u de volgende hulpvragen stellen:

- 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 gevoelige gegevens zoals ras, gezondheid, informatie over iemands financiële situatie, zoals salaris of gegevens waar (identiteit)fraude mee kan worden gepleegd, zoals een Burgerservicenummer. Of is er om een andere reden sprake van een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van de verwerkte Persoonsgegevens?
- Zijn er grote hoeveelheden Persoonsgegevens onbedoeld toegankelijk geworden voor derden?
- Gaat het om gegevens van kwetsbare groepen zoals kinderen?
- Worden de Persoonsgegevens beheerd door een leverancier?
- Waren niet alle gelekte gegevens goed versleuteld, of heeft het Datalek om andere redenen ongunstige gevolgen voor de persoonlijke levenssfeer van de Betrokkene?

Bij twijfel neemt u contact op met de directie van ActiveTickets (Jose Martinez of Edward Spelt).

WAAR EN HOE WORDT HET BEVEILIGINGSINCIDENT GEMELD?

We stellen elkaar zo spoedig mogelijk, doch uiterlijk binnen 36 uur, per e-mail op de hoogte van ieder beveiligingsincident ontdekt door personen die namens u en ons betrokken zijn bij de gegevensverwerking, door het beveiligingsincident te melden aan de volgende daarvoor aangewezen verantwoordelijke contactpersonen.

Contactpersoon namens ActiveTickets	Naam: Jose Martinez / Edward Spelt Tel: 030-7115159 E-mail: jmartinez@activetickets.com en/of espelt@activetickets.com

paraaf Verwerkingsverantwoordelijke *paraaf Verwerker*

Contactpersonen namens uw Organisatie	Naam: Tel: E-mail:

GEEF IN DE TOELICHTING ZO VOLLEDIG MOGELIJK ANTWOORD OP DE VOLGENDE VRAGEN:

Onderstaande vragen zijn gelijk aan de informatie die aan de Autoriteit Persoonsgegevens moet worden verstrekt.

1. **Samenvatting van het beveiligingslek / beveiligingsincident / Datalek: wat is er gebeurd?**
   Vermeld hierbij de naam van het betrokken systeem.

2. **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.

3. **Van hoeveel personen zijn de persoonsgegevens betrokken bij het beveiligingsincident?**
   Geef a.u.b. een minimaal en een maximaal aantal personen.

4. **Omschrijving van de groep personen om wiens gegevens het gaat.**
   Geef aan of het gaat om medewerkersgegevens en/of gegevens van klanten?

5. **Zijn de contactgegevens van de betrokken personen bekend?**
   Het kan zijn dat betrokkenen geïnformeerd moeten worden over het Datalek, kunt u deze personen in dat geval bereiken?

6. **Wat is de oorzaak (root cause) van het beveiligingsincident?**

7. **Op welke datum of in welke periode heeft het beveiligingsincident plaats kunnen vinden?**
   Geef dit zo specifiek mogelijk aan.

Let op: ook als de Persoonsgegevens versleuteld zijn is het verplicht dat u een Datalek meldt bij de Autoriteit Persoonsgegevens.

MELDING AAN DE AUTORITEIT PERSOONSGEGEVENS EN BETROKKENE(N)

Let op: U bent als Verwerkingsverantwoordelijke verplicht om beveiligingsincidenten vast te leggen en zo nodig te melden bij de Autoriteit Persoonsgegevens.

Bijlage 4 – Lijst van Derde Sub-Verwerkers

ActiveTickets (Cramgo B.V.) maakt gebruik van de volgende Sub-Verwerkers voor:

1. De hosting van actieve databases en back-ups in de Cloud;
2. Verzending van mailingen (vanuit ActiveMailer) en voor de afhandeling van de ticketverzending per e-mail.

Microsoft Azure, Inc.	Hosting van actieve klantdatabases
Amazon Web Services (AWS), Inc.	Hosting van database back-ups
Sendgrid, Inc.	Mailverzending / Ticketverzending