

## VERWERKINGSOVEREENKOMST

[DATUM]

### TUSSEN

Gemeente Herselt met maatschappelijke zetel gelegen te Kerkstraat 1, 2230 Herselt en met ondernemingsnummer 0207.502.103, hierbij rechtsgeldig vertegenwoordigd door het college van burgemeester en schepenen door burgemeester Peter Keymeulen en algemeen directeur Tina Vervloessem;

Contactgegevens: [informatieveiligheid@iok.be](mailto:informatieveiligheid@iok.be)

Hierna: de “Verwerkingsverantwoordelijke”;

### EN

TicketGang BVBA met maatschappelijke zetel gelegen te Bieststraat 87, 3191 Boortmeerbeek en met ondernemingsnummer BE0891.029.132, hierbij rechtsgeldig vertegenwoordigd door Yves Pauwels zaakvoerder;

Contactgegevens DPO: Yves Pauwels,

E-mail: [Yves@ticketgang.be](mailto:Yves@ticketgang.be), Tel. 015/699.700, GSM: 0497/594660

Hierna: de “Verwerker”;

De Verwerkingsverantwoordelijke en de Verwerker worden hieronder ook wel afzonderlijk aangeduid als een “Partij” of gezamenlijk als de “Partijen”;

### NA TE HEBBEN UITEENGEZET

- A. Op 12 juli 2023 hebben de Partijen een overeenkomst of meerdere overeenkomsten (opgesomd in bijlage 1) gesloten met betrekking tot software in het kader van evenementenbeheer (uitleen materiaal, inschrijven en/of kopen van tickets en evenementen en kinderopvang, registratie- en verwerkingstool voor het beheer van de omschreven diensten door de gemeente), hierna genoemd de Opdracht;

- B. In het kader van deze overeenkomst zal de Verwerker bepaalde Persoonsgegevens Verwerken in opdracht en voor rekening van de Verwerkingsverantwoordelijke;

De partijen wensen nu hun afspraken met betrekking tot de uitvoering en organisatie van deze Verwerking van Persoonsgegevens te formaliseren in deze Verwerkingsovereenkomst, die integraal deel uitmaakt van voornoemde dienstverleningsovereenkomst.

**WORDT OVEREENGEKOMEN WAT VOLGT**

**Artikel 1: Definities**

Begrippen die in deze Verwerkingsovereenkomst met hoofdletter worden gebruikt, moeten worden geïnterpreteerd zoals in dit artikel of elders in de Verwerkingsovereenkomst gedefinieerd.

AVG	Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming);
Betrokkene	De geïdentificeerde of identificeerbare natuurlijke persoon op wie een Persoonsgegeven betrekking heeft;
Datalek	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;
Derden	Elke natuurlijke persoon, rechtspersoon, overheidsinstantie, dienst of ander orgaan andere dan de Verwerker, de Verwerkingsverantwoordelijke en hun personeelsleden of aangestelden;
Opdracht	De opdracht zoals omschreven in <u>bijlage 1</u> ;
Persoonsgegevens	Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, zoals ook gedefinieerd in artikel 4, 1) AVG, die de Verwerker in het kader van de Opdracht Verwerkt;

Unierechtelijke of lidstaatrechtelijke bepaling	Een bepaling opgelegd door Unierechtelijke of (EU) lidstaatrechtelijke wetgeving;
Verwerken / Verwerking	Elke bewerking of 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, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens, zoals ook gedefinieerd in artikel 4, 2) AVG;
Verwerkingsovereenkomst	Deze overeenkomst.

### **Artikel 2: Voorwerp (art. 28, lid 3 en 4 AVG)**

- 2.1. De Verwerker Verwerkt Persoonsgegevens voor de Verwerkingsverantwoordelijke uitsluitend zoals omschreven in de Opdracht en overeenkomstig de in deze Overeenkomst vastgelegde verplichtingen. De Opdracht wordt nader omschreven in bijlage 1.
- 2.2. Elke Verwerking anders dan omschreven in de Opdracht is strikt verboden, met inbegrip van de doorgifte van Persoonsgegevens aan Derden, een derde land of een internationale organisatie, behoudens indien één van de hieronder opgesomde voorwaarden vervuld is:
- de Verwerkingsverantwoordelijke heeft schriftelijke instructies gegeven om bijkomende Verwerkingen uit te voeren; of
  - een Unierechtelijke of lidstaatrechtelijke bepaling verplicht de Verwerker tot deze bijkomende Verwerking. De Verwerker zal de Verwerkingsverantwoordelijke desgevallend binnen een redelijke termijn voorafgaand aan de bijkomende Verwerking op de hoogte stellen van voornoemd wettelijk voorschrift, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt. Als de Verwerker een verzoek krijgt om Persoonsgegevens ter beschikking te stellen door een daartoe bevoegde instantie overeenkomstig een Unierechtelijke of lidstaatrechtelijke bepaling, beoordeelt zij eerst of het verzoek bindend is en of zij op grond van gedrags- en beroepsregels aan het verzoek moet voldoen. Als er geen strafrechtelijke of andere juridische belemmeringen zijn, dan stelt de Verwerker de Verwerkingsverantwoordelijke op de hoogte van het verzoek. De Verwerker doet dat binnen een termijn dat het voor de Verwerkingsverantwoordelijke mogelijk is om eventuele rechtsmiddelen tegen de verstrekking van de Persoonsgegevens in te stellen.

- 2.3. De Verwerker stelt de Verwerkingsverantwoordelijke onmiddellijk in kennis indien naar zijn mening een instructie inbreuk oplevert op de AVG of op andere Unierechtelijke of lidstaatrechtelijke bepalingen inzake gegevensbescherming.

### **Artikel 3: Duur (art. 28, lid 3, g)**

- 3.1. Loopt samen met de Opdracht beschreven in punt A.
- 3.2. Artikels 3.3, 5, 6, 7, 9, 10 en 12 blijven van kracht na beëindiging van de Verwerkingsovereenkomst.
- 3.3. Na beëindiging van de Verwerkingsovereenkomst dient de Verwerker aan de Verwerkingsverantwoordelijke zonder onredelijke vertraging, en onverwijld op verzoek, een kopie te bezorgen van alle Persoonsgegevens die door haar in het kader van de Opdracht Verwerkt worden, in gestructureerd, gangbaar en machine leesbaar formaat. Als alle Persoonsgegevens zijn bezorgd, stelt de Verwerker onmiddellijk een einde aan elke verwerking van de Persoonsgegevens en vernietigt hij elke kopie en back-up van de Persoonsgegevens die hij nog zou bezitten, tenzij opslag van de Persoonsgegevens Unierechtelijk of lidstaatrechtelijk is verplicht.

### **Artikel 4: Beveiliging (art. 32 AVG)**

- 4.1. De Verwerker treft alle passende technische en organisatorische beveiligingsmaatregelen die nodig zijn om de Persoonsgegevens te beveiligen, rekening houdend met de stand van de techniek en de kost voor beveiliging, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen. In het bijzonder zal de Verwerker de Persoonsgegevens beveiligen tegen vernietiging, verlies, vervalsing, niet toegelaten verspreiding of toegang en elke andere vorm van onwettige Verwerking. De minimale maatregelen die worden getroffen, worden in bijlage 2 toegevoegd.
- 4.2. De Verwerker wijst een functionaris voor gegevensbescherming aan en heeft tenminste een actueel veiligheidsbeleid- en plan.

### **Artikel 5: Vertrouwelijkheid (art. 29 AVG)**

- 5.1. De Verwerker verbindt zich er uitdrukkelijk toe het vertrouwelijk karakter en de veiligheid van de Persoonsgegevens die zij in het kader van de Opdracht Verwerkt, te waarborgen.

5.2. De Verwerker maakt zich sterk dat alle personeelsleden of aangestelden die toegang hebben tot de Persoonsgegevens het vertrouwelijk karakter en de veiligheid van deze Persoonsgegevens zullen respecteren. De Verwerker zal erop toezien dat personeelsleden of aangestelden enkel toegang verkrijgen tot Persoonsgegevens nadat ze behoorlijk gebonden zijn door een wettelijke of contractuele vertrouwelijkheidsverplichting.

#### **Artikel 6: Onderaanneming en subverwerkers (art. 28 lid 4 AVG)**

6.1. De Verwerker stelt enkel andere verwerkers aan om Persoonsgegevens in het kader van de Opdracht te Verwerken (hierna: de "Subverwerker") na uitdrukkelijke, specifieke goedkeuring van de Verwerkingsverantwoordelijke. De Verwerkingsverantwoordelijke gaat akkoord met de lijst van Subverwerkers opgesomd in bijlage 3.

6.2. Extern ingehuurde medewerkers worden voor deze Verwerkingsovereenkomst niet als Subverwerker beschouwd. De Verwerker zal erop toezien dat deze extern ingehuurde medewerkers dezelfde vertrouwelijkheidsclausule, zoals beschreven in artikel 5 van deze Verwerkingsovereenkomst naleven zoals dit voor de eigen werknemers van de Verwerker het geval is.

6.3. De Verwerker en de Subverwerker sluiten een overeenkomst waarin dezelfde verplichtingen inzake gegevensbescherming opgelegd worden als die welke in de voorliggende Verwerkingsovereenkomst zijn opgenomen. De Verwerker zal de Subverwerkers ook dezelfde geheimhoudingsverplichting als deze die op haar rust opleggen middels een vertrouwelijkheidsovereenkomst. De Verwerker zal op eenvoudig verzoek van de Verwerkingsverantwoordelijke het nodige bewijs voorleggen om aan te tonen dat de overeenkomsten met haar Subverwerkers voldoen aan de in dit artikel gestelde voorwaarden.

6.4. De Verwerker houdt een actueel overzicht bij van de overeenkomsten met Subverwerkers en kan deze binnen redelijke termijn op eenvoudig verzoek bezorgen aan de Verwerkingsverantwoordelijke.

6.5. Indien een Subverwerker haar gegevensbeschermingsverplichtingen niet vervult, zal de Verwerker volledig aansprakelijk blijven ten opzichte van de Verwerkingsverantwoordelijke voor de naleving van deze verplichtingen.

#### **Artikel 7: Bijstand (art. 28, lid 3, e - f)**

7.1. Algemeen

De Verwerker zal de Verwerkingsverantwoordelijke alle informatie verstrekken en alle bijstand verlenen die noodzakelijk is en/of die redelijkerwijze mag worden verwacht opdat de

Verwerkingsverantwoordelijke in staat zou zijn om haar verplichtingen uit de AVG na te komen én van deze nakoming het bewijs te leveren.

#### 7.2. Bijstand bij verzoek van een Betrokkene

De Verwerker verleent aan de Verwerkingsverantwoordelijke door middel van passende technische en organisatorische maatregelen, voor zover mogelijk, bijstand bij het vervullen van diens plicht om verzoeken tot uitoefening van de in hoofdstuk III van de AVG vastgestelde rechten van de betrokkene, te beantwoorden.

Indien een Betrokkene zich rechtstreeks wendt tot de Verwerker om zich te beroepen op één van de rechten die hem ingevolge hoofdstuk III van de AVG zijn toegekend, zal de Verwerker dit onverwijld melden aan de Verwerkingsverantwoordelijke en alleen tegemoet komen aan het verzoek van de Betrokkene na schriftelijk akkoord van de Verwerkingsverantwoordelijke.

#### 7.3. Bijstand bij Datalekken

De Verwerker verbindt zich ertoe elk Datalek en alle ernstige pogingen tot onrechtmatige of ongeautoriseerde Verwerkingen of toegangen tot Persoonsgegevens zonder onredelijke vertraging, en uiterlijk 24 uur na kennisname, te melden aan de Verwerkingsverantwoordelijke conform artikel 33.3 van de AVG. De Verwerker zal alle maatregelen treffen die redelijkerwijs nodig zijn om (verdere) schending van de beveiligingsmaatregelen en eventuele schade te voorkomen of te beperken en zal aan de Verwerkingsverantwoordelijke alle informatie die ze nuttig of nodig acht, verschaffen.

Rekening houdend met de aard van de Verwerking en de hem ter beschikking staande informatie, verleent de Verwerker bovendien bijstand aan de Verwerkingsverantwoordelijke bij het nakomen van diens verplichtingen betreffende:

- het melden van een Datalek aan de toezichthoudende autoriteit conform artikel 33 van de AVG;
- het mededelen van een Datalek aan de betrokkene conform artikel 34 van de AVG.

Het is de Verwerker evenwel niet toegestaan om het Datalek zelf te melden aan de GBA of de mededeling aan de betrokkene zelf te verrichten. Dit is uitsluitend de bevoegdheid van de Verwerkingsverantwoordelijke.

#### 7.4. Andere bijstandsverplichtingen

De Verwerker zal - rekening houdend met de aard van de Verwerking en de hem ter beschikking staande informatie – de Verwerkingsverantwoordelijke bijstand verlenen bij het nakomen van diens verplichtingen betreffende:

- het beveiligen van de verwerking conform artikel 32 van de AVG;
- het uitvoeren van een gegevensbeschermingseffectbeoordeling conform artikel 35 van de AVG;

- het voorafgaand aan een voorgenomen verwerking raadplegen van de toezichthoudende autoriteit, wanneer dit na een gegevensbeschermingseffectbeoordeling nodig zou blijken, conform artikel 36 van de AVG.

### **Artikel 8: Plaats van Verwerking (art. 3, art. 28, lid 3)**

De Verwerker Verwerkt de Persoonsgegevens alleen binnen de Europese Economische Ruimte, tenzij hierover met de Verwerkingsverantwoordelijke andere afspraken zijn gemaakt. Deze afspraken leggen de Partijen gezamenlijk schriftelijk vast.

### **Artikel 9: Controle (art. 28, lid 3, h)**

- 9.1. De Verwerkingsverantwoordelijke of zijn daartoe aangestelde heeft op elk ogenblik het recht om de naleving van deze Verwerkingsovereenkomst te controleren. Daartoe heeft zij het recht om zich ter plaatse te begeven in de lokalen of plaatsen waar de Verwerker de Verwerking uitvoert. De Verwerkingsverantwoordelijke zal de Verwerker minstens tien dagen voorafgaand aan het uitvoeren van de controle schriftelijk inlichten. De Verwerkingsverantwoordelijke zal de controles, tenzij dwingend anders vereist, enkel op werkdagen tijdens kantooruren uitvoeren.
- 9.2. Op eenvoudig verzoek van de Verwerkingsverantwoordelijke is de Verwerker ertoe gehouden alle inlichtingen die van toepassing zijn bij de uitvoering van deze Verwerkingsovereenkomst mee te delen en bijstand te verlenen bij het uitvoeren van de audits of bij het vervullen van de verplichting om verzoeken om uitoefening van de in de AVG vastgestelde rechten van de Betrokkene te beantwoorden.

### **Artikel 10: Aansprakelijkheid (art. 82, lid 2)**

- 10.1. De Verwerker is aansprakelijk ten aanzien van de Verwerkingsverantwoordelijke voor schade die voortvloeit uit een handeling of een nalatigheid wanneer bij de Verwerking niet is voldaan aan de specifiek tot verwerkers gerichte verplichtingen van de AVG, dan wel uit een handeling of nalatigheid in strijd met de rechtmatige instructies van de Verwerkingsverantwoordelijke.
- 10.2. De aansprakelijkheid van de Verwerker is beperkt zoals voorzien in de Opdracht, zonder evenwel afbreuk te doen aan art 82 van de AVG.

### **Artikel 11: Beëindiging**

- 11.1. Indien de Verwerker zijn verplichtingen onder deze Verwerkingsovereenkomst niet naleeft, kan de Verwerkingsverantwoordelijke, onverminderd het recht om een schadevergoeding te

bekomen, na schriftelijke gemotiveerde ingebrekestelling de Opdracht geheel of gedeeltelijk beëindigen indien de Verwerker nalaat passende maatregelen te treffen.

### **Artikel 12: Overige**

- 12.1. Deze Verwerkingsovereenkomst is onderworpen aan het Belgisch recht. Alle geschillen in verband met deze Verwerkingsovereenkomst, zullen worden voorgelegd aan de bevoegde rechter in het arrondissement waar de Verwerkingsverantwoordelijke gevestigd is.
- 12.2. Indien een bepaling in de Verwerkingsovereenkomst geheel of gedeeltelijk ongeldig, onwettig of nietig zou worden verklaard, tast dit op geen enkele wijze de geldigheid, wettigheid en toepasbaarheid van de andere bepalingen aan. De Partijen zullen vervolgens te goeder trouw onderhandelen om de ongeldige, onwettige of nietige bepaling te vervangen door een geldige bepaling die zoveel als mogelijk de gevolgen heeft van de ongeldige, onwettige of nietige bepaling.
- 12.3. Aanvullingen en wijzigingen op deze Verwerkingsovereenkomst dienen schriftelijk te gebeuren door middel van een addendum dat als bijlage aan deze Verwerkingsovereenkomst zal worden gehecht.

Deze Verwerkingsovereenkomst werd op 23 november 2023 te Herselt opgesteld in evenveel exemplaren als er Partijen zijn. Aan elke Partij wordt één ondertekend exemplaar van de Verwerkingsovereenkomst overhandigd.

Voor de Verwerkingsverantwoordelijke

Voor de Verwerker

\_\_\_\_\_  
Tina Vervloessem,  
Algemeen directeur

\_\_\_\_\_  
Yves Pauwels  
zaakvoerder

Peter Keymeulen  
Burgemeester

### **BIJLAGEN**

- Bijlage 1: omschrijving Opdracht
- Bijlage 2: veiligheidsmaatregelen
- Bijlage 3: Opsomming van Subverwerkers





## BIJLAGE 1

[eventueel algemene omschrijving]

In het kader van Verwerkingsovereenkomst voert de Verwerker op de onderstaande Persoonsgegevens de Verwerkingen uit waarvan per gegevenssoort de aard van de verwerking, alsmede het doel ervan en de categorieën van betrokkenen, de classificatie(\*) worden vermeld.

<b>VERWERKINGSACTIVITEIT</b>	<b>Verwerkings-doeleinden</b>	<b>Categorieën van betrokkenen</b>	<b>Categorieën van gegevens</b>	<b>Categorieën van ontvangers</b>
<i>In welk kader worden de gegevens verwerkt?</i>	<i>Waarom worden de gegevens verwerkt?</i>	<i>Van wie zijn de gegevens?</i>	<i>Welk type gegevens zijn het?</i>	<i>Aan wie zullen de gegevens worden verstrekt?</i>
Organisator account	klantenbeheer	klanten	identificatiegegevens	intern
Organisator account	klantenbeheer	klanten	financiële gegevens	intern
Organisator account	klantenbeheer	klanten	IP Adres	intern
Evenementenbeheer	Dienstenlevering	eindgebruikers	identificatiegegevens	Intern betalingsprovider organisator scanningsysteem
Evenementenbeheer	Dienstenlevering	eindgebruikers	Persoonlijke kenmerken (o.a. rijksregisternummer van zowel aanvrager als kind)	Intern organisator
Evenementenbeheer	Dienstenlevering	eindgebruikers	IP Adres	Intern organisator
Evenementenbeheer	Dienstenlevering	eindgebruikers	Tickets en inschrijvingsgegevens	Intern organisator

(\*) optioneel

## **BIJLAGE 2**

### Technische en Organisatorische maatregelen

#### **Bepalingen art 32 AVG**

Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen.

De verwerker is eraan gehouden om maatregelen te treffen die onder meer het volgende kunnen omvatten:

- de pseudonimisering en versleuteling van persoonsgegevens
- het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen
- het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen
- een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking

#### **Technische en organisatorische maatregelen betreffende de interne werking en organisatie van TicketGang.**

- de pseudonimisering en versleuteling van persoonsgegevens
  - TicketGang versleutelt de paswoorden via salted hashing.
- het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen.
  - TicketGang staat ervoor in dat de webapplicatie-gegevens zo goed als redelijkerwijs mogelijk worden beveiligd tegen verlies, diefstal, ongeautoriseerde toegang en wijziging door derden.
- het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen
  - TicketGang maakt gebruik van Clustering technieken om een maximale uptime, en business continuïteit te voorzien. Er is geen single point of failure in onze cluster. Er wordt gebruik gemaakt van synchrone database replicatie (Percona XtraDB Cluster) zodat de gegevens op elk moment up to date zijn in de cluster.
- een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking

- TicketGang evalueert jaarlijks de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking. De laatste evaluatie vond plaats in januari 2019 (in het kader van de GDPR).

Hiertoe geeft de verwerking hieronder een opsomming van de toegepaste beveiligingsmaatregelen.

Beschrijving van de mogelijke technische en organisatorische maatregelen

### 1 Technische maatregelen

- De aanwezigheid van automatische anonimisering of pseudonimisering van de persoonsgegevens nadat het doeleinde van de verwerking (of wettelijke opgelegde bewaartermijnen) zijn overschreden.
  - Automatische anonimisering
- De aanwezigheid van een degelijk uitgebouwd gebruikersbeheer. Dit omvat:
  - De organisator kan zelf interne gebruikers kunnen toevoegen/verwijderen (zonder tussenkomst van TicketGang).

De organisator kan zelf administratoren aanmaken / beheren in TicketGang. Het rechtenbeheer voor administratoren is Role Based Access Control (RBAC) gebaseerd.
  - De mogelijkheid om multi-factor authenticatie (bv. eID) te gebruiken  

TicketGang ondersteund login via paswoord en EID
  - De mogelijkheid om een wachtwoordenpolicy in te stellen (gebruikers - burgers) kiezen zelf hun inloggegevens, deze worden niet in de back-end bepaald)  

De wachtwoordenpolicy is door TicketGang opgezet – minimale login / paswoord lengte, etc. Gebruikers kunnen zelf hun paswoord en login instellen en achteraf hun paswoord wijzigen.
  - De mogelijkheid om het wachtwoord van een gebruiker te resetten.  

De klant zal zelf zijn paswoord kunnen resetten.
  - Minstens 2 niveaus van rechten (een administrator en gebruikers) naargelang gebruik- en beslissingsniveau.  

TicketGang maakt gebruik van Role Based Access Control (RBAC). De organisator kan een of meerdere rollen toewijzen aan zijn administratoren. Er bestaan momenteel circa 110 specifieke rechten die gekoppeld kunnen worden aan een rol.
- Een degelijk uitgebouwde audit log module
  - De mogelijkheid tot loggen van: welke gebruiker, welke acties in het programma heeft uitgevoerd (incl. consultatie).
  - TicketGang beschikt over een Audit log in onze database waarin de acties van organisatoren / gebruikers worden opgeslagen.

- Mogelijkheid tot extractie (export) van gegevens
  - TicketGang biedt een CSV, XLS, PDF export aan voor alle tabellen die eindgebruikers kunnen zien.

Daarnaast moet een **webapplicatie** beschikken over:

- Een grondige beveiliging uitgevoerd op basis van de OWASP top 10 bedreigingen
  - De TicketGang ontwikkelaars zijn vertrouwd met OWASP en zijn jaarlijkse updates (inclusief Jan 2019).
  - Vele potentiële issues (zoals SQL injectie, etc) worden op framework niveau afgehandeld.
- Met minstens een bescherming tegen een brute force aanval.
  - TicketGang blokkeert gebruikers na 5 mislukte pogingen tot inloggen.
- Structurele bijwerkingen op het vlak van security:
  - Aan server (besturingssysteem, webserver, antivirus, ...)
    - TicketGang maakt gebruik van Debian Linux voor haar servers. “Security advisories” worden opgevolgd, en “security patches” worden zo snel mogelijk uitgevoerd in functie van het gelopen risico. De servers van TicketGang zijn uitgerust met een geavanceerde firewall en controlemechanismen die zijn interne netwerk op gepaste wijze beschermt tegen ongeoorloofde toegang tot zijn interne netwerk
    - TicketGang maakt gebruik van ClamAV, de open source antivirus engine voor het detecteren van trojans, virussen en malware.
  - Aan databank
    - TicketGang maakt gebruik van Percona XtraDB Cluster voor de database opslag. Deze oplossing ondersteunt encryptie voor alle gegevens transport in de cluster.

Enige **overdracht** en **opslag** van **persoonsgegevens**, vervat in de toepassing, dient op een **veilige** manier te gebeuren. Indien het om een webapplicatie gaat gelden volgende minimale vereisten:

- De persoonsgegevens worden via een beveiligde verbinding (https) ter beschikking gesteld.
  - Een beveiligde verbinding voor eindgebruikers
  - TicketGang heeft een automatische redirect van http naar https voor <gemeente>.zaalreservatie.be, <gemeente>.ticketgang.eu e, [www.ticketgang.com](http://www.ticketgang.com) en [www.ticketgang.be](http://www.ticketgang.be).

- De persoonsgegevens worden opgeslagen in een Europees datacenter (ISO/IEC 27001 gecertificeerd)
  - TicketGang is gehost in 2 fysiek gescheiden data center parken, beheerd door Hetzner Online AG in Duitsland. Ticketgang's Primary data center bevindt zich Falkenstein. Ons Disaster Recovery data center bevindt zich in Nürnberg.
  - Hetzner is ISO/IEC 27001 gecertificeerd.
- Een back-up van de persoonsgegevens wordt bij het werken met een tweede datacenter – ook via een beveiligde verbinding doorgegeven. Daarnaast wordt de back-up procedure van de leverancier gedocumenteerd.
  - TicketGang maakt gebruik van Percona XtraDB Cluster voor de database opslag. Deze oplossing ondersteunt encryptie voor alle gegevens transport in de cluster.
  - De TicketGang database cluster maakt gebruik van synchrone replicatie van de gegevens (over de verschillende data center parken heen).
  - Er wordt iedere dag een volledige database backup gemaakt. Om de 30 minuten vindt er een incrementele backup plaats.
  - Data opslag gebeurt versleuteld (3DES) voor de wachtwoorden.

## 2 Organisatorische maatregelen

- De leverancier beschikt over een veiligheidsconsulent en Data Protection Officer.
  - Yves Pauwels is de TicketGang DPO
  - Kurt Van Cant, Dreambuilder BVBA is de veiligheidsconsulent.
- De personeelsleden zijn op de hoogte van het veiligheidsbeleid en hebben een vertrouwelijkheidsverklaring ondertekend. De leverancier garandeert de klant d.m.v. afspraken dat de opgeslagen persoonsgegevens door de leverancier enkel worden ingekeken op vraag van de klant en/of incidentbehandeling of na verwittiging voor onderhoud.
  - De personeelsleden zijn op de hoogte van het veiligheidsbeleid en hebben de TicketGang vertrouwelijkheidsverklaring ondertekend.
  - Een autorisatiebeheersysteem controleert dat de toegang tot systemen die persoonsgegevens bevatten wordt beperkt tot toegewezen gebruikers.
  - Een segregatie is ingevoerd om te vermijden dat personen toegang krijgen tot gegevens waarvoor ze geen toegang nodig hebben voor de uitoefening van hun taak.
- Een privacyverklaring geeft de nodige transparantie (principe van privacywet)
  - De TicketGang privacyverklaring is beschikbaar via onze webpagina's. De verklaring vindt u hier: <https://www.ticketgang.be/pp.php>

- De leverancier garandeert in een SLA maximale onderbrekingen en een contactpunt bij incidenten.
  - De Ticketgang samenwerkingsovereenkomsten met organisatoren vermelden expliciet de SLA.

### **BIJLAGE 3**

- Payment provider, Ingenico
- Payment provider, Multisafepay
- Hosting, Hetzner Online AG
- Belgo-Tax-On-Web, FOD Financiën
- Mijn Burgerprofiel (Vlaamse Gemeenschap)