Bijlage 1: Verwerking persoonsgegevens (verwerkersovereenkomst)

Indien Twelve bij de uitvoering van de Overeenkomst ten behoeve van Opdrachtgever Persoonsgegevens verwerkt, zijn in aanvulling op de Algemene Voorwaarden de onderstaande voorwaarden van toepassing.

1. Algemeen

1.1. Twelve heeft een kassa/betaaloplossing voor het registreren en controleren van uitgaven in de horecagelegenheid van de organisaties. Er worden gegevens bijgehouden om beheerders toegang te geven tot het beheersysteem of om eindgebruikers toegang te geven tot een uniek account.

1.2. In sommige gevallen werkt de verantwoordelijke met een closed-loop betaaloplossing, (gepersonaliseerde) passen, bandjes of tokens. In die gevallen slaan wij de gegevens op om eindgebruikers en beheerders toegang te geven tot het beheersysteem of om toegang te geven tot een uniek account.

1.3. Twelve verricht op grond van deze Overeenkomst werkzaamheden in opdracht van Verantwoordelijke en verwerkt hiertoe bepaalde persoonsgegevens in de zin van artikel 4.1 van de Algemene Verordening Gegevensbescherming (hierna: "Persoonsgegevens"), zoals omschreven in bijlage 1, waarvoor Verantwoordelijke verantwoordelijk is;

1.4 Bij de verwerking van Persoonsgegevens kan Opdrachtgever worden aangemerkt als Verwerkingsverantwoordelijke, of indien Opdrachtgever de Persoonsgegevens ten behoeve van een derde partij verwerkt als verwerker. Twelve vervult (afhankelijk van de hoedanigheid waarin de Opdrachtgever Persoonsgegevens verwerkt) de rol van verwerker of sub-verwerker.

1.5. De partijen erkennen en respecteren de toepasselijkheid op de verwerking van de Algemene Verordening Gegevensbescherming (hierna: "AVG") en de Uitvoeringswet Algemene Verordening Gegevensbescherming en andere regelgeving op het gebied van persoonsgegevens;

1.6.Partijen spreken af met betrekking tot de verwerking van persoonsgegevens in overeenstemming met artikel 28 van de Algemene Verordening Gegevensbescherming (AVG) wensen vast te leggen in deze verwerkersovereenkomst;

2. Reikwijdte verwerking

2.1 Verantwoordelijke geeft hierbij opdracht aan Twelve om namens hem Persoonsgegevens te verwerken onder de voorwaarden in deze overeenkomst (de "Verwerkersovereenkomst") en op de wijze zoals omschreven in bijlage 1.

2.2 Twelve verwerkt de Persoonsgegevens uitsluitend op basis van deze Verwerkersovereenkomst en de schriftelijke instructies van Verantwoordelijke en verwerkt de Persoonsgegevens niet voor andere of eigen doeleinden.

2.3 Verantwoordelijke is te allen tijde gerechtigd additionele schriftelijke instructies aan Twelve te geven of de voorwaarden in deze Verwerkersovereenkomst te wijzigen.

2.4 Twelve heeft geen zeggenschap over het doel en de middelen voor de verwerking van de Persoonsgegevens. De zeggenschap over de Persoonsgegevens komt nimmer bij Twelve te rusten.

2.5 Indien een instructie van de verantwoordelijke naar mening van de Twelve een inbreuk oplevert op de AVG of andere regelgeving met betrekking tot persoonsgegevens, stelt de Twelve de Verantwoordelijke daarvan onmiddellijk in kennis.

2.6 Twelve verwerkt de Persoonsgegevens enkel in de Europese Economische Ruimte.

3. Geheimhouding

3.1 Twelve zal Persoonsgegevens waarvan zij kennis neemt strikt geheim houden en derhalve onder geen omstandigheid delen met of verstrekken aan derden, behoudens indien en voor zover

a. Twelve daartoe voorafgaande schriftelijke toestemming of opdracht van Verantwoordelijke heeft gekregen of

b. enig dwingendrechtelijke wettelijk bepaling haar tot verstrekking verplicht.
c. De gegevens geanonimiseerd zijn.

3.2. Indien Twelve op grond van dwingendrechtelijke regelgeving verplicht is om de Persoonsgegevens te delen met of te verstrekken aan derden, zal Twelve Verantwoordelijke hierover voorafgaand informeren, tenzij dit niet is toegestaan op basis van de genoemde regelgeving.
3.3. Twelve waarborgt dat de tot het verwerken van de Persoonsgegevens gemachtigde personen, waaronder haar werknemers en eventuele Sub-verwerkers, zich vooraf schriftelijk hebben verbonden vertrouwelijkheid in acht te nemen.

4. Beveiligingsmaatregelen
4.1. Twelve zal rekening houdend met de stand van de techniek, de uitvoeringskosten, en 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 passende technische en organisatorisch maatregelen treffen om een op het risico afgestemd beveiligingsniveau te waarborgen conform artikel 32 AVG. De beveiligingsmaatregelen zijn omschreven in bijlage 1.2 van deze Verwerkersovereenkomst.

5. Verlenen van bijstand
5.1. Twelve zal
a. Rekening houdend met de aard van de verwerking, voor zover mogelijk bijstand verlenen aan de Verantwoordelijke bij een gegevensbeschermingseffect beoordeling dan wel voorafgaande raadpleging van de Autoriteit Persoonsgegevens.
b. Aan Verantwoordelijke alle informatie ter beschikking te stellen die Verantwoordelijke nodig heeft om te voldoen aan de wettelijke en contractuele verplichtingen die op haar rusten in het kader van de verwerking van Persoonsgegevens door Twelve.
c. Rekening houdend met de aard van de verwerking door middel van passende technische en organisatorische maatregelen, voor zover mogelijk, aan Verantwoordelijke bijstand verlenen bij het vervullen van diens plicht om verzoeken om uitoefening van de wettelijke rechten van betrokkene zoals vastgesteld in hoofdstuk III van de AVG te beantwoorden (o.a. maar niet uitsluitend het recht van inzage, rectificatie, gegevenswissing of verwerkingsbeperking en het recht van bezwaar).

6. Toezicht op naleving
6.1. Twelve stelt Verantwoordelijke in staat om ten minste eenmaal per kalenderjaar, onder aanzegging van een redelijke termijn, de naleving van Twelve te controleren van de Verwerkersovereenkomst en met name de beveiligingsmaatregelen genoemd in artikel 4 en bijlage 1.2.
6.2. Daartoe zal Twelve aan Verantwoordelijke en/of auditors ingehuurd door Verantwoordelijke toegang verschaffen tot (relevante delen van) de ruimtes, systemen en/of servers waarin/waarmee de verwerking van de Persoonsgegevens op enig moment plaatsvindt en zal aan Verantwoordelijke en/of auditors ingehuurd door Verantwoordelijke, alle relevante informatie verstrekken.

7. Toevoeging of vervanging Verwerkers en het inschakelen Sub-Verwerkers
7.1. Twelve neemt slechts andere verwerkers in dienst en/of schakelt slechts derden in voor de verwerking van Persoonsgegevens ("Sub-Verwerker(s)") nadat Verantwoordelijke daartoe schriftelijke toestemming heeft verstrekt en in het geval van Sub-Verwerker(s) aan hem door middel van een Sub-Verwerkersovereenkomst dezelfde verantwoordelijkheden en plichten heeft opgelegd die aan Twelve zijn opgelegd in deze Verwerkersovereenkomst. Verantwoordelijke geeft hierbij toestemming voor het inschakelen van Sub-Verwerkers:

a. Multipost
b. Tapes
c. Dutchband
d. CCV
e. EMS
f. WB Services
g. Leaseweb

7.2. Op eerste verzoek van Verantwoordelijke verstrekt Twelve aan Verantwoordelijke een kopie van de met deze Sub-Verwerkers(s) gesloten Sub-Verwerkersovereenkomst.

7.3. Twelve is ten opzichte van Verantwoordelijke volledig verantwoordelijk en aansprakelijk voor het nakomen van de verplichtingen van Sub-Verwerkers en vrijwaart Verantwoordelijke voor alle kosten en schade die voortvloeien uit schending door de Sub-Verwerker van de wet- en regelgeving en/of de aan de Sub-Verwerker uit hoofde van artikel 8.1 opgelegde verplichtingen.

8. Aansprakelijkheid en vrijwaring

8.1. Twelve is aansprakelijk voor en vrijwaart Verantwoordelijke voor alle schade, boetes of (ander) nadeel, voortvloeiende uit een schending door Twelve van de wet- en regelgeving betreffende de verwerking van Persoonsgegevens in het kader van zijn werkzaamheden onder deze Verwerkersovereenkomst en/of niet-nakoming van verplichtingen van Twelve onder deze Verwerkersovereenkomst.

9. Duur en beëindiging

9.1. Deze Verwerkersovereenkomst is geldig zo lang Twelve Persoonsgegevens verwerkt uit naam van Verantwoordelijke. Deze Verwerkersovereenkomst eindigt automatisch zodra de Overeenkomst is geëindigd.

9.2. Bij beëindiging van deze Verwerkersovereenkomst zal Twelve onmiddellijk, op eigen initiatief, alle documenten, computer disks en andere gegevensdragers, evenals kopieën daarvan, waarop of waarin zich Persoonsgegevens bevinden, retourneren aan Verantwoordelijke, ongeacht of de inhoud is vervaardigd of gecreëerd door Twelve, Verantwoordelijke of een derde. Twelve zal de Persoonsgegevens verstrekken op een wijze zoals verzocht door Verantwoordelijke en zonder additionele kosten. Voor zover de Persoonsgegevens zich in een computersysteem bevinden of in een andere vorm waardoor de Persoonsgegevens redelijkerwijs niet kunnen worden verstrekt aan Verantwoordelijke, zal Twelve aan Verantwoordelijke een toegankelijke, leesbare kopie van de Persoonsgegevens verstrekken.

9.3. Indien Twelve op grond van een wettelijke bewaarplicht bepaalde Persoonsgegevens en/of documenten, computer disks of andere gegevensdragers waarop of waarin zich Persoonsgegevens bevinden gedurende een wettelijke termijn moet bewaren, dan zal Twelve zorgdragen voor de vernietiging van deze Persoonsgegevens en/of documenten, computer disks of andere gegevensdragers binnen vier (4) weken na beëindiging van de wettelijke bewaarplicht.

9.4. Zo lang Twelve Persoonsgegevens onder zich heeft blijven alle in deze Verwerkersovereenkomst genoemde restricties van kracht.

9. Jurisdictie

10.1. Op deze Verwerkersovereenkomst is Nederlands recht van toepassing. Alle geschillen die voortvloeien uit deze Verwerkersovereenkomst zullen worden voorgelegd aan de competente rechter te Amsterdam.

Bijlage 1.1
Omschrijving gegevensverwerking

1. Gegevens
Verantwoordelijke verschaft aan Twelve toegang tot de volgende Persoonsgegevens van website Verwerkers die door Twelve mogen worden verwerkt:

- Naam (wordt gevraagd als herkenningspunt en voor eventuele communicatie)
- E-mailadres (wordt gevraagd voor de communicatie en om het unieke account aan te maken en te koppelen)
- Wachtwoord (om toegang te krijgen tot het unieke account)
- Gebruikersnaam (wordt gevraagd aan beheerders om toegang te krijgen tot het unieke account (oude oplossing maar nog niet iedereen omgezet))
- Adresgegevens (wordt gevraagd om passen toe te kunnen sturen, alleen verplicht als verantwoordelijke dit vereisen)
- Geslacht (zodat de verantwoordelijke onderscheid kan maken tussen eindgebruikers, en Twelve vraagt het om gericht te communiceren)
- Geboortedatum (dit wordt gevraagd om leeftijdscontrole toe te kunnen passen)
- IP-adres (dit wordt opgeslagen om brute force aanvallen te monitoren (om te kijken hoe vaak er achter elkaar ingelogd wordt, wordt niet gekoppeld aan persoonsgegevens))
- Contactgegevens van werknemers van Verantwoordelijke en/of derden die door Verantwoordelijke zijn ingeschakeld.

2. Doeleinden
De doeleinden waarvoor de Persoonsgegevens, indien noodzakelijk, mogen worden verwerkt zijn:

- Het uitvoeren van de werkzaamheden zoals overeengekomen in de overeenkomsten.
- Het voldoen aan wet- en regelgeving.

3. Omschrijving gegevensverwerking
Uitvoering van de werkzaamheden zoals overeengekomen in de Overeenkomsten.

4. Toegang
Uitsluitend de volgende groepen personen zullen toegang hebben tot de Persoonsgegevens:

- Daartoe geautoriseerde personen in dienst van Twelve, op "need-to-know"-basis;
- Daartoe geautoriseerde personen in dienst van door Twelve met instemming van Verantwoordelijke aangestelde Sub-Verwerker(s), op "need-to-know"-basis.

Bijlage 1.2
Beveiligingsmaatregelen

- Er wordt gebruik gemaakt van 2-staps authenticatie en een wachtwoordbeleid om ongeautoriseerde login te voorkomen en om sterk wachtwoordgebruik te borgen;
- er geldt een geheimhoudingsplicht voor medewerkers en ingeschakelde derden;
- op elk proces in het bedrijf waarbij gegevens worden verwerkt is een Data Protection Impact Assessment (DPIA) op uitgevoerd. Met dit instrument zijn de privacy risico's van gegevenswerkingen in kaart gebracht en eventuele maatregelen zijn genomen. Wanneer een proces in het bedrijf veranderd zal er opnieuw een DPIA worden uitgevoerd;
- periodiek worden er 'Pentests' uitgevoerd. Hierbij bekijkt een externe beveiligingsexpert of de beveiliging van het software platform van Twelve op orde is;
- fysieke maatregelen voor toegangsbeveiliging;
- encryptie (versleuteling) van digitale bestanden met persoonsgegevens;
- beveiliging van netwerkverbindingen;
- het bewaringstermijn van gegevens is aangescherpt.

Bijlage 1.3
Protocol melden datalekken

Op 1 januari 2016 is de meldplicht datalekken in werking getreden, welke valt onder de Wet Bescherming Persoonsgegevens (WBP). In de nieuwe privacywetgeving, de Algemene Verordening Gegevensbescherming (AVG) welke op 25 mei 2018 in werking treedt, blijft deze meldplicht datalekken van kracht. De AVG heeft dit aangescherpt door strengere eisen te stellen aan de eigen registratie en documentatie van datalekken binnen de organisatie. Dit protocol beschrijft de procedure met daarin de te nemen maatregelen die binnen Twelve genomen moeten worden. Twelve heeft het protocol afgestemd op de eisen van de AVG.

1. Meldpunt Datalekken Twelve

De leden van het Meldpunt Datalekken Twelve zijn (hierna MDT genoemd):

- Communicatie – Amber Daalmeijer
- CFO – Pieter Paul van Heeswijk
- Manager DevOps – Bram Spliet

De meldingen kunnen worden ingediend bij:

- Telefoonnummer: 030 276 7770
- Amber Daalmeijer – amber@twelve.eu
- Pieter Paul van Heeswijk – pieterpaul@twelve.eu
- Bram Spliet – bram@twelve.eu

2. Datalek

Volgens de AVG is er sprake van een datalek bij verlies of onrechtmatige verwerking van persoonsgegevens.

Er is sprake van verlies, indien:

- niemand de persoonsgegevens meer heeft;
- er geen complete en actuele reservekopie van de persoonsgegevens meer is.

Er is sprake van onrechtmatige verwerking, indien:

- persoonsgegevens zijn aangetast (bij versleuteling);
- onbevoegde kennisneming van de persoonsgegevens plaatsvindt;
- persoonsgegevens ten onrechte zijn gewijzigd;
- persoonsgegevens ten onrechte zijn verstrekt.

Datalekken kunnen ontstaan door:

- moedwillig handelen (cybercriminaliteit, hacking, identiteitsfraude, mailware besmetting);
- technisch falen (ICT-storingen);
- menselijk falen (te eenvoudige wachtwoorden/het verstrekken van username/wachtwoord aan collega's en externen);
- calamiteit (brand datacentrum, wateroverlast)
- verloren USB stick of laptop;
- verzenden van email met emailadressen van alle geadresseerden;
- maar ook het onrechtmatige verwerking van gegevens.

3. Procedure

1. Een mogelijk datalek kan door een medewerker van Twelve, één van haar leveranciers, klanten of andere betrokkenen worden ontdekt.

2. De leveranciers, klanten, medewerkers en andere betrokkenen van Twelve dienen bij een mogelijk datalek dit direct te melden bij het MDT, of bij afwezigheid, één van de andere directieleden.

3. Het MDT zal direct de melding in behandeling nemen en beoordelen.

4. In het geval het datalek één of meer specifieke klanten, leveranciers of andere betrokkenen raakt, worden deze binnen 36 uur ingelicht.

5. In het geval er een datalek wordt geconstateerd wordt binnen 72 uur de Autoriteit Persoonsgegevens ingelicht.

6. Het MDT zal, na onderzoek te hebben gedaan, direct maatregelen treffen tegen het datalek.

7. Het MDT zal een volledige documentatie maken van het voorgevallen datalek.

4. Verantwoordelijkheden

1. Elke medewerker van Twelve dient op de hoogte te zijn van het protocol. Dit protocol wordt opgenomen in het personeelshandboek en zal per e-mail verzonden worden naar de huidige medewerkers.

2. De klanten, leveranciers en andere betrokkenen van Twelve dienen op de hoogte te zijn van het protocol, deze zal meegestuurd worden met de Verwerkersovereenkomst en opgenomen worden in de algemene voorwaarden.

3. In het CRM systeem van Twelve wordt per klant een contactpersoon voor datalekken geregistreerd. Dit dienen klanten, leveranciers en andere betrokkenen zelf door te geven aan Twelve. Wanneer er geen specifiek contactpersoon is geregistreerd, wordt het hoofdcontactpersoon benaderd.

Twelve BV, Utrecht