VERWERKERSOVEREENKOMST

zoals bedoeld in de overeenkomst tussen Verantwoordelijke en eLaunch inzake het gebruik van het ELAUNCH-platform.

OVERWEGINGEN en DEFINITIES

1. Verantwoordelijke is met eLaunch een overeenkomst aangegaan terzake van het gebruik van het ELAUNCH-platform, hierna te noemen: **de Overeenkomst.**

2. In het kader van de uitvoering van de Overeenkomst zullen persoonsgegevens in de zin van artikel 4 lid 1 Algemene verordening gegevensbescherming (hierna te noemen: **AVG**) worden verwerkt waarbij Verantwoordelijke is aan te merken als verwerkingsverantwoordelijke en eLaunch als verwerker.

3. Deze verwerking is onderworpen aan het bepaalde in deze verwerkersovereenkomst die tot stand komt met en deel uitmaakt van de Overeenkomst.

4. Verantwoordelijke en eLaunch worden in deze verwerkersovereenkomst gezamenlijk ook aangeduid als **Partijen.**

BEPALINGEN VAN DEZE VERWERKERSOVEREENKOMST

Artikel 1 Verwerking van persoonsgegevens door eLaunch

1.1 ELaunch zal in het kader van de uitvoering van de Overeenkomst ten behoeve van Verantwoordelijke persoonsgegevens verwerken. In bijlage A (“De verwerking van de persoonsgegevens”) is opgenomen welke persoonsgegevens worden verwerkt, voor welk doel zij worden verwerkt en wat de duur is van de verwerking.

1.2 ELaunch zal de persoonsgegevens op behoorlijke en zorgvuldige wijze en in overeenstemming met de AVG en andere toepasselijke regelgeving verwerken. ELaunch verwerkt de persoonsgegevens slechts in opdracht van Verantwoordelijke en volgt de schriftelijke instructies van Verantwoordelijke dienaangaande op, behoudens afwijkende wettelijke verplichtingen. Verantwoordelijke kan schriftelijke aanwijzingen aan eLaunch geven tot wijziging van de handelingen/verwerkingen door eLaunch.

1.3 ELaunch heeft geen zeggenschap over het doel van de verwerking van de persoonsgegevens. De middelen van de verwerking zijn beschreven in bijlage A (“De verwerking van de persoonsgegevens”). Voor zover niet anders is bepaald krachtens de Overeenkomst, neemt eLaunch geen beslissingen over het gebruik van de persoonsgegevens, de verstrekking aan derden en de duur van de opslag van de persoonsgegevens.

1.4 ELaunch verleent op eerste verzoek aan Verantwoordelijke alle medewerking die in redelijkheid van haar gevergd kan worden, zodat Verantwoordelijke kan blijven voldoen aan zijn verplichtingen uit hoofde van:
- de AVG (zoals bijvoorbeeld inzake de rechten van betrokkenen en het melden van een datalek); en
- andere toepasselijke wet- en regelgeving.

1.5 ELaunch verwerkt geen persoonsgegevens buiten de Europese Unie, tenzij zij daarvoor voorafgaand uitdrukkelijk schriftelijk toestemming heeft verkregen van Verantwoordelijke.

Artikel 2 Beveiliging

2.1 ELaunch treft passende technische en organisatorische maatregelen, en houdt deze in stand en zal deze zo nodig aanpassen om de persoonsgegevens te beveiligen tegen verlies, verminking en/of enige onrechtmatige vorm van beheer en/of verwerking. ELaunch treft in ieder geval de technische en organisatorische beveiligingsmaatregelen, zoals omschreven in de bijlagen (A, B en C).

2.2 Bij het treffen van de technische en organisatorische beveiligingsmaatregelen heeft eLaunch rekening gehouden met de stand van de techniek, de uitvoeringskosten van de beveiligingsmaatregelen, de aard, omvang en de context van de verwerkingen, de doeleinden en het beoogd gebruik van haar producten en diensten, de verwerkingsrisico’s en de qua waarschijnlijkheid en ernst uiteenlopende risico’s voor de rechten en vrijheden van betrokkenen die zij gezien het beoogd gebruik van haar producten en diensten mocht verwachten.

2.3 Verantwoordelijke kan eLaunch verzoeken nadere beveiligingsmaatregelen te treffen. ELaunch is niet verplicht om op een dergelijk verzoek wijzigingen door te voeren in haar beveiligingsmaatregelen. ELaunch kan de kosten verband houdende met de op verzoek van Verantwoordelijke doorgevoerde wijzigingen in rekening brengen bij Verantwoordelijke. Pas nadat de door Verantwoordelijke gewenste gewijzigde beveiligingsmaatregelen schriftelijk zijn overeengekomen en ondertekend door

Partijen, heeft eLaunch de verplichting deze beveiligingsmaatregelen daadwerkelijk te implementeren.

Artikel 3 Subverwerkers

3.1 Het is eLaunch zonder uitdrukkelijke schriftelijke toestemming van Verantwoordelijke niet toegestaan derden als subverwerkers aan te stellen en in te schakelen. Verantwoordelijke zal zijn toestemming niet zonder redelijke grond onthouden.

3.2 Verwerkingsverantwoordelijke geeft hierbij toestemming voor het inschakelen van de in de bijlage A genoemde subverwerkers, die op hun beurt gebruik maken van het in bijlage A genoemde data center.

3.3 ELaunch zorgt dat de door haar ingeschakelde subverwerkers zijn onderworpen aan dezelfde verplichtingen terzake van de bescherming van de persoonsgegevens als waaraan eLaunch jegens Verantwoordelijke op grond van deze verwerkersovereenkomst is gebonden.

Artikel 4 Datalek

4.1 In het geval er bij eLaunch sprake is van een datalek in de zin van de AVG, dient eLaunch dit onmiddellijk (uiterlijk binnen 24 uur na constatering van het datalek) en voorzien van de benodigde toelichting en achtergrond te melden aan Verantwoordelijke.

4.2 Verantwoordelijke doet de wettelijke meldingen van een datalek aan betrokken autoriteit(en) en betrokkenen. ELaunch zegt daartoe op voorhand volledige medewerking toe en zal onder meer op eerste verzoek van Verantwoordelijke (i) de noodzakelijke (additionele) inlichtingen verstrekken en (ii) de nodige bescheiden en informatie aan Verantwoordelijke verstrekken. Deze verplichting geldt ook indien Verantwoordelijke op een later tijdstip zijn initiële melding moet of wenst aan te vullen.

4.3 Het is uitsluitend aan Verantwoordelijke om te bepalen of een bij eLaunch geconstateerd datalek wordt gemeld aan de Autoriteit Persoonsgegevens en/of aan betreffende betrokkenen.

Artikel 5 Controle

5.1 Verantwoordelijke heeft het recht de naleving van de bepalingen van deze verwerkersovereenkomst eenmaal per jaar op eigen kosten te controleren of te laten controleren door een onafhankelijke en gecertificeerde externe deskundige die

aantoonbaar ervaring heeft met het soort verwerkingen dat op basis van de Overeenkomst wordt uitgevoerd.

5.2 ELaunch stelt Verantwoordelijke alle informatie ter beschikking die nodig is om aan te tonen dat wordt voldaan aan de verplichtingen neergelegd in artikel 28 AVG. Indien Verantwoordelijke of een door hem ingeschakelde deskundige in dat verband een instructie geeft die naar mening van eLaunch inbreuk oplevert op de AVG dan stelt eLaunch Verantwoordelijke daarvan onmiddellijk in kennis.

5.3 Het onderzoek van Verantwoordelijke zal zich altijd beperken tot de systemen die voor de verwerking worden gebruikt. Verantwoordelijke zal de bij de controle gevonden informatie geheimhouden en alleen gebruiken om de naleving door eLaunch van de verplichtingen uit deze verwerkersovereenkomst te controleren en de informatie zo snel mogelijk wissen. Verantwoordelijke staat ervoor in dat eventuele door hem ingeschakelde derden deze verplichtingen ook op zich nemen en naleven.

5.4 De bevindingen van het onderzoek worden integraal aan eLaunch bekend gemaakt. Elaunch verkrijgt een exemplaar van de onderzoeksrapportage.

5.5 Partijen zullen zo snel mogelijk in overleg treden over de uitkomsten van het onderzoek. Partijen zullen de voorgestelde verbetermaatregelen die in het rapport zijn neergelegd opvolgen voor zover dat van hen in redelijkheid kan worden verwacht. ELaunch zal de voorgestelde verbetermaatregelen doorvoeren voor zover deze naar haar oordeel passend zijn rekening houdend met de verwerkingsrisico's verbonden aan gebruik van het ELAUNCH-platform, de stand van de techniek, de uitvoeringskosten, de markt waarin zij opereert.

Artikel 6 Vergoeding

ELaunch maakt aanspraak op vergoeding voor alle werkzaamheden die zij ingevolge deze verwerkersovereenkomst op uitdrukkelijk verzoek van Verantwoordelijke heeft te verrichten, met uitzondering van werkzaamheden die het gevolg zijn van nalatigheid van eLaunch met betrekking tot haar verplichtingen jegens Verantwoordelijke, behoudens beroep op overmacht.

Artikel 7 Geheimhouding

ELaunch houdt de persoonsgegevens geheim. ELaunch draagt ervoor zorg dat de persoonsgegevens niet direct of indirect ter beschikking komen van derden. Onder derden wordt ook het personeel van eLaunch begrepen voor zover het niet noodzakelijk is dat dit

kennis neemt van de persoonsgegevens. Dit gebod geldt niet voor zover in de Overeenkomst anders is bepaald en/of voor zover een wettelijk voorschrift of vonnis tot enige bekendmaking verplicht.

Artikel 8 Aansprakelijkheid

8.1 Verantwoordelijke staat ervoor in gerechtigd te zijn de persoonsgegevens voor verwerking ter beschikking te stellen aan eLaunch.

8.2 Verantwoordelijke is verantwoordelijk en aansprakelijk voor (het gestelde doel van) de verwerking, het gebruik en de inhoud van de persoonsgegevens, de verstrekking aan derden, de duur van de opslag van de persoonsgegevens, de wijze van verwerking en de daartoe gehanteerde middelen.

8.3 ELaunch is jegens de Verantwoordelijke uitsluitend aansprakelijk tot vergoeding van schade die het directe gevolg is van het aan eLaunch toerekenbaar niet nakomen van deze verwerkersovereenkomst door of vanwege eLaunch, tot maximaal de door eLaunch krachtens de Overeenkomst met betrekking tot de aan de aansprakelijkstelling voorafgaande periode van 12 maanden aan Verantwoordelijke exclusief BTW in rekening gebrachte som.

Artikel 9 Duur, wijziging en beëindiging

9.1 Deze verwerkersovereenkomst duurt zolang de Overeenkomst voortduurt en eindigt bij beëindiging van de Overeenkomst met dien verstande dat de bepalingen van deze verwerkersovereenkomst ook na beëindiging van de Overeenkomst blijven gelden voor zover dat nodig is uit oogpunt van de AVG, of voor zover dat nodig is voor afwikkeling van het bepaalde in deze verwerkersovereenkomst.

9.2 Partijen zullen deze verwerkersovereenkomst aanpassen aan gewijzigde regelgeving, instructies van de relevante autoriteiten en voortschrijdend inzicht in de toepassing van de AVG en/of andere gebeurtenissen of inzichten die een aanpassing nodig maken.

9.3 Indien wijziging in de verwerking van de persoonsgegevens noodzakelijk is, stemt eLaunch dit vooraf schriftelijk af met Verantwoordelijke. Indien deze wijziging noodzakelijk is als gevolg van gewijzigde wet- en regelgeving en/of aanwijzingen van toezichthouders, dan voert Verwerker deze wijzigingen onverkort en zo snel als mogelijk door.

9.4 ELaunch kan wijziging aanbrengen in de getroffen beveiligingsmaatregelen indien dat naar haar oordeel noodzakelijk is om een passend beveiligingsniveau te blijven bieden. ELaunch zal Verantwoordelijke van substantiële wijzigingen op de hoogte stellen.

9.5 De inhoud van de bijlage (“De verwerking van de persoonsgegevens”) kan van tijd tot tijd door eLaunch worden herzien en aangepast aan veranderende omstandigheden. ELaunch zal Verantwoordelijke van significante aanpassingen op de hoogte stellen. Hierop heeft Verantwoordelijke gedurende 30 dagen gelegenheid om schriftelijk en gemotiveerd tegen deze aanpassing bezwaar te maken. Indien eLaunch ervan afziet aan dit bezwaar tegemoet te komen is Verantwoordelijke gedurende 30 dagen na kennisgeving van de beslissing van eLaunch op het bezwaar gerechtigd de Overeenkomst schriftelijk gemotiveerd op te zeggen. Eén en ander onverminderd de mogelijkheden tot opzegging waarin de Overeenkomst voorziet.

9.6 ELaunch zorgt dat de persoonsgegevens en alle kopieën daarvan na beëindiging van de Overeenkomst worden gewist. Dit wissen geschiedt zodra Verantwoordelijke eLaunch daar schriftelijk toe instrueert, dan wel na verloop van een periode van één jaar na eindiging van de Overeenkomst, gedurende welke periode Verantwoordelijke nog een export kan doen maken van de persoonsgegevens, en de verwerking kan doen herleven.

Artikel 10 Totstandkoming

Deze verwerkersovereenkomst komt tot stand door totstandkoming van de Overeenkomst en maakt deel uit en is afhankelijk van de Overeenkomst.

Bijlage A- De verwerking van de persoonsgegevens

1 Omschrijving van de verwerking

Het middel van de Verwerking is het ELAUNCH-platform van eLaunch CloudLab BV.

Via zijn domein op het ELAUNCH-platform is Verantwoordelijke in staat om Deelnemers en Beheerders toegang te geven tot het platform. Beheerders kunnen vervolgens namens Verantwoordelijke trainingen aan diens Deelnemers beschikbaar stellen. Daartoe kunnen ze eigen trainingen en trainingen van andere Domeinhouders importeren. Eigen trainingen kunnen ze bovendien aan andere Domeinhouders beschikbaar stellen. De response op trainingen binnen het eigen domein kunnen ze gedetailleerd bekijken. Response op eigen trainingen die aan andere Domeinhouders beschikbaar zijn gesteld is slechts op geaggregeerde wijze te bekijken.

2 Om welke (type) betrokkenen gaat het?

Er zijn twee typen betrokkenen: Beheerders en Deelnemers. Deze worden samen de “gebruikers” genoemd.

Deelnemers: dit zijn personen die vanwege Verantwoordelijke gebruik kunnen maken van het platform en waaraan, naar gelang van hun profiel, trainingen beschikbaar worden gesteld en die geacht worden deze te volgen.

Beheerders: dit zijn personen die namens Verantwoordelijke (afhankelijk van hun rol) het domein van Verantwoordelijke beheren en/of trainingen beschikbaar stellen aan Deelnemers en/of inzicht hebben in de response op trainingen. Beheerders hebben bepaalde rechten die per Beheerder kunnen verschillen. Deze rechten worden door de Domeinbeheerder toebedeeld. Daarbij worden de volgende rollen onderscheiden.

Rollen van Beheerders

<u>De Domeinbeheerder (ook wel account admin genoemd)</u>:

- bepaalt en beheert alle instellingen van het domein, inclusief de rollen en rechten van de verschillende Beheerders;
- heeft toegang tot alle onderdelen van het domein inclusief de response op trainingen;
- bepaalt en beheert profielen voor typen Deelnemers (bv. senior verkoopmedewerker);
- beheert de communicatie naar Deelnemers en Beheerders.

Trainer:

- kan trainingen ontwikkelen, importeren en beheren;
- heeft inzicht in de response op trainingen die zijn aangeboden binnen het Domein;
- heeft inzicht in geaggregeerde response op eigen trainingen die zijn aangeboden buiten het Domein.

Waarnemer:

- heeft inzicht in de response op trainingen die zijn aangeboden binnen het Domein.

Divisiemanager/regiomanager:

- heeft inzicht in de response op trainingen die zijn aangeboden binnen het Domein;
- kan, indien daartoe door de Domeinbeheerder gemachtigd, Deelnemers van teams/winkels beheren.

Teammanager/winkelmanager:

- heeft inzichten in de response van Deelnemers gekoppeld aan zijn team(s)/winkel(s);
- kan, indien daartoe door de Domeinbeheerder van het account gemachtigd Deelnemers van teams/winkels beheren.

3 Om welke (persoons)gegevens van welke (type) betrokkenen gaat het?

De volgende (persoons)gegevens worden beheerd en verwerkt.

Deelnemers: voornaam, achternaam, mailadres*, telefoonnummer, winkelnaam, profiel*, voorkeursinstellingen.

Beheerders: voornaam, achternaam, mailadres*, telefoonnummer, rol*, voorkeursinstellingen.

* Deze velden zijn verplicht.

ELaunch registreert de activiteit van Deelnemers en Beheerders en kan deze (geaggregeerd) beschikbaar stellen in rapportages voor Beheerders. Response op trainingen van andere Domeinhouders wordt aan die Domeinhouders in geaggregeerde, niet tot natuurlijke personen herleidbare vorm beschikbaar gesteld.

4 Verwerking van gegevens

1. Invoer van gegevens

Deelnemers en Beheerders voeren gegevens in.

2. Opslag van gegevens

De opslag van de gegevens geschiedt via het ELAUNCH-platform. Technisch beheer en hosting zijn ondergebracht bij subverwerkers.

3. Interactie door Deelnemers en Beheerders

De interactie door Deelnemers en Beheerders met het platform is overeenkomstig hun rechten en rollen binnen het account.

5 Het inzien en laten verwijderen van (persoons)gegevens

Deelnemers kunnen een verzoek plaatsen om hun verwerkte (persoons)gegevens in te zien of te laten verwijderen, door contact op te nemen met een Beheerder van het account, bijvoorbeeld door gebruik te maken van het support mailadres dat door de Domeinbeheerder is ingesteld.

Inzicht verschaffen in de verwerkte (persoons)gegevens

De Beheerder kan via zijn dashboard een rapportage maken van de verwerkte (persoons)gegevens van een Deelnemer en deze naar die Deelnemer sturen.

Het laten verwijderen van verwerkte (persoons)gegevens

De Beheerder kan via zijn dashboard een Deelnemer verwijderen van het platform en hem daarmee de toegang tot het platform ontnemen. Bijvoorbeeld bij uitdiensttreding. Vanaf dat moment zijn desbetreffende (persoons)gegevens niet meer zichtbaar voor de Beheerders.

ELaunch laat deze gegevens overigens niet direct maar pas na 3 maanden verwijderen uit de database. Dit stelt eLaunch in staat om een Deelnemer desgevraagd te reactiveren met behoudt van al zijn data. Ook na 3 maanden blijft de response op trainingen beschikbaar binnen het platform, zij het op niet tot betrokkene herleidbare wijze.

Het is de verantwoordelijkheid van de Domeinhouder om op de juiste manier en tijdig gehoor te geven aan het verzoek van Deelnemers om inzicht te krijgen of persoonlijke gegevens te laten verwijderen.

6 Service en ondersteuning door eLaunch

Ondanks dat het ELAUNCH-platform een selfservice platform is, heeft eLaunch toegang nodig tot het domein van Verantwoordelijke voor periodieke controle, service en ondersteuning

t.b.v. Beheerders. ELaunch heeft daarom te allen tijde toegang tot het domein van Verantwoordelijke.

Alleen op schriftelijk verzoek van (of namens) Verantwoordelijke is het eLaunch toegestaan om additionele hulp (hulp buiten de uit de Overeenkomst voortvloeiende verplichtingen) te bieden bij het verwerken van persoonsgegevens.

Elaunch houdt log-bestanden bij op basis waarvan eLaunch desgevraagd kan vaststellen wanneer een beheerder zich de toegang (heeft) verschaft tot het domein van Verantwoordelijke en welke handelingen hierbij zijn verricht. Deze logbestanden worden gedurende 14 dagen bewaard. Op verzoek van Verantwoordelijke onderzoekt eLaunch deze logbestanden en rapporteert de verzochte informatie m.b.t de oorzaak van onregelmatigheden, mochten deze zijn geconstateerd of door Verantwoordelijke redelijkerwijs worden vermoed.

7 Assessments

Op verzoek kan Verantwoordelijke een security code review en/of een security audit (assessment) doen uitvoeren met betrekking tot het ELAUNCH-platform. Het assessment wordt uitgevoerd op locatie van onze partner (subverwerker) Geckotech. Het bepaalde in artikel 5 (“Controle”) van de verwerkersovereenkomst is onverminderd van toepassing.

De applicatie kan op verzoek van Verantwoordelijke ook onderworpen worden aan een externe ‘black box’ test (zogenaamde ‘penetratie tests’).

8 Duur van de verwerking

Zolang als de Overeenkomst tussen Verantwoordelijke en eLaunch van kracht is.

Verantwoordelijke heeft gedurende de looptijd van de Overeenkomst de mogelijkheid om de persoonsgegevens te exporteren. Na verloop van de Overeenkomst worden de persoonsgegevens door eLaunch gewist, met dien verstande:

- dat dit wissen geschiedt één jaar na eindiging van de Overeenkomst (voor zover de verwerking niet is voortgezet op grond van een nieuwe overeenkomst) tenzij Verantwoordelijke eLaunch schriftelijk instrueert tot eerdere verwijdering; en
- dat niet tot de persoon herleidbare response op trainingen bewaard blijft in het ELAUNCH-platform.

9 Subverwerkers

De subverwerkers bedoeld in artikel 3.2 van de verwerkersovereenkomst zijn:

Sub-verwerker voor softwareontwikkeling en beheer (zie ook bijlage B)

Geckotech BV
Randstad 22 119, 1316 BW Almere

Sub-verwerker voor hosting services (zie ook bijlage C):

Geckotools BV
Randstad 22 119, 1316 BW Almere
Geckotools BV beheert data in het datacenter van TransIP BV, Schipholweg 9B, 2316 XB Leiden.

Bijlage B - Technical Security Policy Introduction

This document provides an outline of the measures taken to provide information security for the ELAUNCH-platform developed by ELAUNCH in cooperation with her software development partner Geckotech BV.

1. Languages and Development Frameworks

Applications are developed using the Grails framework.

> ***Grails** is a **powerful** web framework, for the Java platform aimed at multiplying developers' productivity thanks to a Convention-over-Configuration, sensible defaults and opinionated APIs. It integrates smoothly with the JVM, allowing you to be immediately productive whilst providing powerful features, including integrated ORM, **Domain-Specific Languages**, runtime and compile-time **meta-programming** and **Asynchronous** programming.*

Grails is based on the industry standard Spring Framework used for building enterprise quality software in Java. The software is deployed as a standard WAR file.

2. Infrastructure Configuration Management

2.1 Infrastructure

Infrastructure is located in The Netherlands, at TransIP. Only TransIP authorized staff can access the infrastructure where the virtual private servers are running.

TransIP has the following certifications:

- ISO 9001
- ISO 27001
- ISO 14001
- NEN 7510
- PCI DSS

For more information, see: https://www.transip.nl/knowledgebase/artikel/331-welke-iso-certificeringen-jullie-datacentrum-allemaal/

2.2 Ownership

Development, hosting and infrastructure are all provided by companies with 100% Dutch ownership. The chain of services from software development to hosted services are as follows:

1. Development: Geckotech BV
2. Hosting services: Geckotools BV
3. Data Center: TransIP BV

All entities in the above chain are 100% Dutch owned registered companies.

2.3 Middleware

Applications are hosted on a VPS (Virtual Private Server) provided by Geckotools. By using a VPS, applications are completely isolated from each other.

Each application server runs an instance of a Tomcat application server and a Postgres database server.

The application runs as a Web Application Archive (WAR) in a Tomcat container. We recommend not sharing Tomcat instances for applications, but using different virtual servers, for additional security. By default, every application runs in their own Tomcat instance, with a private Postgres installation.

All traffic is routed through an Apache proxy, which provides protection against abuse. Requests from IP addresses searching for exploits are automatically banned. The application server instance is behind a firewall, and not directly accessible from the internet. The Apache proxy connects to the Tomcat instance through an AJP connector**.**

3. Architecture and Design

3.1 Network security

3.1.1 Firewalls

The network is protected with an advanced IPTables firewall. The firewall consists of two physical machines with an automatic fail-over mechanism. The firewall does not allow direct connections to customer VPS, instead connections are proxied through an Apache reverse proxy server.

3.1.2 Remote Access

A VPS is not directly accessible for clients. No shell access is provided.

Only verified members of the system administrator group have access to systems for administrative purposes. Access is managed through SSL certificates and IP based firewalls and is centrally administered.

A web-based console is available to manage systems (upload, deploy and remove applications and manage databases.) Access is provided over HTTPS only and secured by username and password.

3.2 Application design

3.2.1 Authentication

The application makes use of the industry standard Spring Security framework, which securely authenticates users within the HTTPS session. User credentials are protected by transport level security while in transit. Changing your password requires entering the old password.

All requests to the application are secured by default.

3.2.2 Input Filtering

The application is developed with the Grails framework, which is built upon the Spring Framework and Hibernate. Due to the use of Hibernate, an ORM, user input is automatically escaped and only prepared statements are used, mitigating the risk of an injection attack. The database is the only injection target in the application.

The Grails framework helps to prevent XSS by automatically escaping all user input. No raw output is rendered in the application.

3.2.3 Authorization

The application console is only accessible to users registered under that subscription. A sub-account can be created to allow an additional user access to a subscription.

3.2.3 User Management

Accounts and subaccounts are required to have unique e-mail addresses. When a VPS subscription is created, the customer is added as an allowed user. Access to the console can easily be disabled by removing the subaccount, or closing the subscription.

Clients are discouraged to share their login credentials.

3.2.4 Transport Security

All services offered by Geckotools are secured with SSL certificates, configured with secure cyphers and key exchange algorithms. Clients are encouraged to add an SSL certificate to their own application.

3.2.5. Cryptography and hashes

Passwords in applications are stored using the strong non-reversible bcrypt hashing algorithm, or SHA256 in some older applications. Other sensitive content can be encrypted upon request.

3.2.6. Error Handling

On production systems, the default configuration of Grails for uncaught exceptions is to simply display: "An error has occurred.".

3.3.7. Session Management

The default session management features of the Java Servlet environment are used. No changes have been made to the configuration. Session cookies are marked as both HttpOnly and Secure, preventing malicious scripts from stealing the session id through XSS or sniffing the session id by redirecting to an insecure URL.

3.2.8. OWASP Top 10

The Open Web Application Security Project keeps a list of the most common vulnerabilities in web applications. In particular, the top 10 should be covered in web applications. OWASP describes itself as

The Open Web Application Security Project (OWASP) is an open community dedicated to enabling organizations to develop, purchase, and maintain applications that can be trusted.

Top 10
A1 - Injection

Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

The application is developed with the Grails framework, which is built upon the Spring Framework and Hibernate. Due to the use of Hibernate, an ORM, user input is automatically escaped and only prepared statements are used, mitigating the risk of an injection attack. The database is the only injection target in the application.

A2 – Broken Authentication and Session Management

Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.

The application makes use of the industry standard Spring Security framework, which securely authenticates users within the HTTPS session. User credentials are protected by transport level security while in transit. Changing your password requires entering the old password.

All requests to the application are secured by default.

A3 – Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's

browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

The Grails framework helps to prevent XSS by automatically escaping all user input. No raw output is rendered in the application.

A4 – Insecure Direct Object References

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.

All files served by the application are retrieved through the numerical ids of domain objects, with no possibility for the user to modify the path. Files which are served dynamically, for example based on a username, it is sanitized and the following characters are not allowed:

[#%$+%>!`&*\'|{}?"=/:\\\\@]

This disables the ability to traverse directory paths. Additionally, the application server is configured to only have access to its own directory.

A5 – Security Misconfiguration

Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date.

The security configuration for the application is embedded in the application, and can only be changed at compile time. We use the industry standard Spring Security library, which has a locked down configuration by default: nothing is accessible until a rule explicitly states that it is.

A6 – Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.

Payment details such as credit card or bank account numbers are not stored in the application, but with a payment provider (either DocData or Mollie) which has PCI compliance. All data is protected with transport level security while in transit.

Authentication credentials (passwords) are stored with a cryptographic hashing function (bcrypt) in the database.

A7 – Missing Function Level Access Control

Most web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests in order to access functionality without proper authorization.

The application implements access checks on an "application role" level, which is applied to all requests. Additionally, each service method is individually secured by specific domain level access checks.

A8 - Cross-Site Request Forgery (CSRF)

A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim.

Cookies are protected in transit through the flags SecureFlag and HttpOnly. Both the session cookie and remember-me cookie (a token for persistent logins) are protected.

CSRF is mitigated through the use of a 'synchronizer token' which is added to forms submitted to the server.

A9 - Using Components with Known Vulnerabilities

Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.

The known security vulnerabilities in Grails, Spring and Hibernate are very low, according to the CVE details database. The versions are regularly upgraded which mitigates all of the currently known exploits.

A10 – Unvalidated Redirects and Forwards

Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.

Unvalidated redirects and forwards are not used. The application does not use forwards at all, and redirects are validated. If a redirect does not start with the server url, a warning is displayed.

4. Development, Deployment and Maintenance

4.1. Application and Content Deployment

Applications are deployed as a standard WAR file, through a web-based console. The console is only accessible for users registered within the VPS subscription.

4.2. Assessment

Upon request a **security code review** and/or **security audit** can be performed for the application. The review can be executed by an independent developer at Geckotech, or source code can be delivered for an external audit.

Applications can be subjected to external **black box testing** (a.k.a. "penetration testing") when requested by the customer. Normally this can be done on a testing environment, but if needed a separate copy of the production environment can be provided for a test.

4.3 Source Code Management

Source code is securely stored in a Subversion repository served over HTTPS, protected by a username and password. The user management is provided by Crowd, an SSO solution. When a developer leaves a project, or the company their accounts are disabled and access to the repository is automatically revoked.

4.4 Operational Security Management

4.4.1. Change Control standards/procedures

Any upcoming change is recorded in JIRA, our issue tracker. Source code changes are linked against the related issue, and during release management the version in which a patch has been applied is recorded in the issue. Through this process the stage of the lifecycle of a change is completely transparent.

All changes are checked in to an SCM, after which continuous integration automatically runs automated unit and integration tests. Before going to production, a staging release is performed to a separate environment where a manual assessment is done before pushing a release to production.

The release management process is highly automated, preventing user error. Access to Bamboo (the continuous integration/deployment solution) is restricted using Crowd. Only project administrators are allowed to do deployments.

4.4.2 Incident response standards/procedures/ event logging

Incident management is handled through the Geckotools support ticketing system. The process is governed by the workflow provided by the ticketing system and users have access to all their ticket status and history.

5. ISO-certification

5.0. ISO-Certified

Geckotech B.V. is ISO 27001 certified. For more information you can visit https://www.geckotech.nl/certification/

Bijlage C – Hosting Security Policy

This document provides an outline of the measures taken to provide information security for the ELAUNCH-platform. Hosting performed by Geckotools BV on behalf of eLaunch.

1. Development Tools and Frameworks

It is the policy of Geckotools to keep all hosted software products up to date with the latest stable versions and security patches. To facilitate the process and ensure quality of updates, Geckotools is in the process of automating the change management process using puppet (https://puppet.com), a tool for automating software management over multiple systems.

2.0 Infrastructure Configuration Management

2.1 Infrastructure

Infrastructure is located in The Netherlands, at TransIP. Only TransIP authorized staff can access the infrastructure where the virtual private servers are running.

TransIP has the following certifications:

- ISO 9001
- ISO 27001
- ISO 14001
- NEN 7510
- PCI DSS

For more information, see: https://www.transip.nl/knowledgebase/artikel/331-welke-iso-certificeringen-jullie-datacentrum-allemaal/

2.2 Ownership

Hosting and infrastructure are all provided by companies with 100% Dutch ownership. The chain of services is as follows:

- Hosting services: Geckotools BV
- Data Center: TransIP BV

All entities in the above chain are 100% Dutch owned and registered companies.

2.3 Middleware

Applications are hosted on a VPS (Virtual Private Server) provided by Geckotools. By using a VPS, applications are completely isolated from each other.

Each application server runs an instance of a Tomcat application server and a Postgres database server.

The application runs as a Web Application Archive (WAR) in a Tomcat container. We recommend not sharing Tomcat instances for applications, but using different virtual servers, for additional security. By default, every application runs in their own Tomcat instance, with a private Postgres installation.

All traffic is routed through an Apache proxy, which provides protection against abuse. Requests from IP addresses searching for exploits are automatically banned. The application server instance is behind a firewall, and not directly accessible from the internet. The Apache proxy connects to the Tomcat instance through an AJP connector.

3.0 Architecture and Design

3.1 Network security

3.1.1 Firewalls

The network is protected with an advanced IPTables firewall. The firewall consists of two physical machines with an automatic fail-over mechanism. The firewall does not allow direct connections to customer VPS, instead connections are proxied through an Apache reverse proxy server.

3.1.2 Remote Access

A VPS is not directly accessible for clients. No shell access is provided.

Only verified members of the system administrator group have access to systems for administrative purposes. Access is managed through SSL certificates and IP based firewalls and is centrally administered.

A web-based console is available to manage systems (upload, deploy and remove applications and manage databases.) Access is provided over HTTPS only and secured by username and password. Access is only provided for technical personnel requiring access to the systems.

3.1.3 Application design

Authentication, Input Filtering, Authorization, User Management, Error Handling, Cryptography and hashes

These facets of application security are the responsibility of the software provider and falls outside of the domain of responsibility of Geckotools.

3.1.4. Transport Security

All services offered by Geckotools are secured with SSL certificates, configured with secure cyphers and key exchange algorithms. Clients are encouraged to add an SSL certificate to their own application.

3.1.5 Session Management

The default session management features of the Java Servlet environment are used. No changes have been made to the configuration. Session cookies are marked as both HttpOnly and Secure, preventing malicious scripts from stealing the session id through XSS or sniffing the session id by redirecting to an insecure URL.

3.1.6 OWASP Top 10

The Open Web Application Security Project keeps a list of the most common vulnerabilities in web applications. In particular, the top 10 should be covered in web applications. OWASP describes itself as

The Open Web Application Security Project (OWASP) is an open community dedicated to enabling organizations to develop, purchase, and maintain applications that can be trusted.

4.0 Development, Deployment and Maintenance

4.1 Application and Content Deployment

Applications are deployed as a standard WAR file, through a web-based console. The console is only accessible for users registered within the VPS subscription.

4.2 Assessment

Upon request a **security code review** and/or **security audit** can be performed for a hosted application.
Applications can be subjected to external **black box testing** (a.k.a. "penetration testing") when requested by the customer. Normally this can be done on a testing environment, but if needed a separate copy of the production environment can be provided for a test.

4.4 Source Code Management

Source code is securely stored (where relevant) in a Subversion repository served over HTTPS, protected by a username and password. The user management is provided by Crowd, an SSO solution. When a developer leaves a project, or the company, their accounts are disabled and access to the repository is automatically revoked.

4.5 Operational Security Management

4.5.1 Change Control standards/procedures

Maintenance windows for updates are communicated to clients in advance.

Updates are monitored with Icinga, warnings are issued when non-critical updates are available, critical alerts (email + sms) are issued when critical issues are available. updates are deployed during one of the maintenance windows. updates are deployed on non-production servers first, basic OS functionality is tested before being applied to production systems. For the customer's application only the homepage or login page is tested, application testing is up to the customer.

Patches are applied within 30 days, critical updates within 7 days.

4.5.2. Incident response standards/procedures/ event logging

Incident management is handled through the Geckotools support ticketing system. The process is governed by the workflow provided by the ticketing system and users have access