Information security policy

1. Inleiding

Primoforum is een instrument om groepen, in een classroom setting, te (bege-)leiden bij werkconferenties. Zoals brainstorming, training, co-creatie, evaluatie, inspraak- & consultatierondes, multi-stakeholdersessies en test-/panelsessies. Primoforum zet je in als je kennis of denkkracht uit een groep wilt halen, consensus wilt bereiken, een koers uit wilt zetten met draagvlak vanuit de groep. Snel, gestructureerd en met een actieve rol voor echt iedereen.Die groep kan uit acht, maar ook uit tachtig of meer deelnemers bestaan. Zij kunnen individueel of in teams meedoen.

Primoforum is een online webapplicatie, een cloud-oplossing, dus je hoeft er niets voor te installeren. Je gebruikt Primoforum via je browser en het internet. Bij een Primoforum-sessie waarin gevoelige informatie wordt uitgewisseld wil je er zeker van zijn dat die informatie alleen gedeeld wordt tussen de deelnemers en facilitator van die sessie. Als gebruiker van Primoforum wil je de zekerheid hebben dat alle sessie-informatie veilig is en niet toegankelijk voor anderen.

Informatiebeveiliging is voor ons een heel belangrijk onderwerp. Het is niet alleen een belangrijk thema bij de ontwikkeling van Primoforum, maar het is ook binnen onze organisatie belangrijk. Zelfs bij het selecteren van onze partnerorganisaties. In dit document lichten wij toe hoe de informatie die via Primoforum loopt is afgeschermd en hoe wij de toegang tot klantgerelateerde data hebben georganiseerd.

Voor specifieke vragen omtrent informatie beveiliging kunt u altijd contact met ons opnemen. Via info@primoforum.com of bellen met 020 261 34 60.

2. Primoforum webapplicatie

Primoforum is een webapplicatie, toegankelijk voor iedereen die online een account aanmaakt of abonnement afneemt. Een Primoforumgebruiker heeft de volledige controle over zijn/haar eigen data. Binnen Primoforum onderscheiden wij sessiegerelateerde data (vragen en antwoorden van een sessie) en klant-/accountgerelateerde data (NAW, betaalgegevens, etc.).

2.1 Primoforum sessiedata

Een (betalende) gebruiker van Primoforum heeft toegang tot zijn eigen sessiedata. Sessiedata bestaan uit vragen, stemrondes en input van sessiedeelnemers.

Alle verkeer van en naar de Primoforum-webapplicatieservers loopt over beveiligde verbindingen. We maken gebruik van het Transport Layer Security (TLS) beveiligingsprotocol. TLS is de standaard voor encryptie-protocollen die de communicatie tussen computers (bijvoorbeeld op het internet) beveiligen en die ervoor zorgt dat het zeker is met wie je communiceert.

Tijdens een eenmalige registratieprocedure moet de gebruiker een eigen wachtwoord bedenken en invoeren. Niemand anders dan de gebruiker heeft toegang tot dat wachtwoord. Noch een medewerker van de Forum1-organisatie, noch ontwikkelaars kunnen op welke wijze dan ook toegang verkrijgen tot de wachtwoorden van Primoforum-gebruikers.

Deelnemers aan een sessie kunnen deelnemen dmv een unieke code die door de Primoforum-applicatie wordt gegenereerd op het moment dat een sessie wordt gestart. Het betreft hier dus een sessiespecifieke code. Op het moment dat een sessie wordt gestopt, worden alle deelnemers automatisch uitgelogd en is de sessiecode ongeldig. Vanaf dat moment hebben deelnemers geen toegang meer tot de sessie en/of sessiedata.

Alle sessiedata worden op servers in Nederland opgeslagen bij KPN Internedservices. Zie paragraaf 3.8. De inlog op deze servers is alleen mogelijk via versleutelde verbindingen vanaf een beperkte lijst IP-adressen.

2.2 Klant-accountdata
Financieel gerelateerde klantinformatie wordt buiten Primoforum om en zover het creditcard- en PayPal-betalingen betreft, bijgehouden in Chargify (https://www.chargify.com/). Chargify maakt gebruik van de payment provider Braintree.

Betaling voor het gebruik van Primoforum is gebaseerd op een abonnementenstructuur; een systeem van Recurring payments. Een recurring payments-systeem (ook wel recurring billing -systeem genoemd) is een online systeem waarin periodieke betalingen ontvangen en verwerkt kunnen worden. Chargify heeft zich sinds 2009 volledig toegelegd op het ontwikkelen van een betrouwbaar billing-systeem en heeft zich bewezen als betrouwbare partner op dit gebied. Met Chargify/Braintree regelen wij de betaalafhandeling via credit card en paypal op een betrouwbare en veilige manier.

Voor de beveiliging van ICT-systemen en -architecturen bestaan vele standaarden. Wanneer het gaat om creditcard-gegevens, de opslag van payment-data of de verwerking van betalingen is de standaard voor informatiebeveiliging voor de payment card industry (PCI) een heel belangrijke. Deze standaard, afgekort tot PCI-DSS, of PCI, wordt wereldwijd ingezet ter bescherming van gegevens die gebruikt worden bij creditcard-validaties.

Chargify wordt jaarlijks geaudit om aan het hoogste niveau van PCI compliance te voldoen. Chargify is PCI DSS Level 1 Compliant. Het certificaat daarvan is openbaar en beschikbaar via de website van Chargify: https://www.chargify.com/images/Chargify-2017-PCI-Certificate.pdf
Voor meer informatie over security binnen Chargify: https://www.chargify.com/security/

3. Onze organisatie

Coöperatie Forum1 U.A. hanteert een strikt beveiligingsbeleid dat is gedocumenteerd en van toepassing is op alle leden, medewerkers, ingehuurde krachten en samenwerkingspartners van Cooperatie Forum1 U.A. (Forum1).

3.1 Wachtwoorden
In de dagelijkse bedrijfsvoering wordt gebruik gemaakt van verschillende applicaties. Voor de toegang tot bedrijfsgerelateerde applicaties geldt een strikt wachtwoordbeleid. Wachtwoorden binnen Forum1 worden op twee manier opgeslagen: (1) via Lastpass of een vergelijkbare externe dienst waarbij Forum1 optimaal profiteert van de beveiligde omgeving van de betreffende tool, (2) op laptops van Forum1-leden/-medewerkers en alleen als die laptops zijn voorzien van een virusscanner en een versleutelde harde schijf. Verder mogen wachtwoorden alleen opgeslagen zijn binnen de tool waarvoor ze bedoeld zijn. Dus niet in excel of ‘platte’ bestanden. Er wordt een wachtwoordenprotocol nageleefd dat is vastgelegd in een separaat document.

3.2 Bestanden
Alle documenten van Forum1 staan in een gedeelde Dropbox-map. Stelregel is dat deze Dropbox alleen ‘gesynced’ mag zijn met computers die voldoen aan de eisen die gesteld

worden aan werkstations (zie paragraaf 3.1). Dit geldt ook voor documenten die buiten de gedeelde Dropbox-map staan. Voor Dropbox wordt een two-factor-authenticatie gebruikt.

3.3 Werkstations / laptops
Leden/medewerkers van Forum1 werken uitsluitend op Apple-computers. Voor iedere computer geldt dat de hele harde schrijf versleuteld moet zijn met een wachtwoord dat bij elke reboot van de computer ingevoerd moet worden. Verder mag het niet mogelijk zijn om een computer of laptop te gebruiken als een computer langer dan 10 minuten niet in gebruik is. Wij handhaven dit bijvoorbeeld door middel van een screensaver die de computer in standby laat gaan. Verder dient er altijd een goed functionerende virusscanner geïnstalleerd en actief te zijn. Updates van de virusscanner en het besturingssysteem dienen zo snel mogelijk, maar uiterlijk binnen een week geïnstalleerd te worden. Laptops in onbeveiligde ruimtes mogen nimmer achtergelaten worden, en zodra degene die ermee werkt zijn plek achter de machine verlaat, altijd softwarematig gelocked te worden.

3.4 Telefoon / mobiele apparaten
Indien een telefoon gekoppeld wordt aan een door Forum1 gebruikt account, zoals bijvoorbeeld de mail, dan moet de telefoon voorzien zijn van een wachtwoord/pincode.

3.5 Beveiliging e-mail
Voor Forum1-leden en medewerkers geldt dat het e-mail account van Google Apps verplicht beveiligd moet zijn dmv two-factor-authenticatie. Een apparaat van waaraf de email dmv bijvoorbeeld POP3 of IMAP bereikbaar is moet altijd voorzien zijn van een wachtwoord of pincode.

3.6 Sales- en marketingtools
Ter ondersteuning van sales en marketing wordt gebruik gemaakt van de cloudapplicatie ZOHO CRM en van het emailmarketingsysteem MailChimp.

In ZOHO CRM worden o.a. de NAW-gegevens van Primoforum-gebruikers bijgehouden. ZOHO hanteert een eigen informatiebeveiligingsbeleid. Voor de details verwijzen wij naar de website: https://www.zoho.eu/security.html

In MailChimp worden namen en emailadressen opgeslagen van mensen die via de Primoforum-website hebben aangegeven de nieuwsbrief te willen ontvangen en/of een Primoforum account hebben. Het informatiebeveiligingsbeleid van MailChimp voldoet aan onze eisen. Voor de details, zie: https://mailchimp.com/about/security/

3.7 Autorisatiematrix
Onderstaand overzicht toont wie welke toegang heeft tot welk systeem.

Autorisatie matrix	Primoforum Website	Primoforum Webapplicatie	Server	Chargify/ Braintree	ZOHO CRM	MailChimp
Management Primoforum	Beheer	Beheer admin. Omgeving	-	Beheer	Beheer	Beheer
Medewerkers primoforum	Lezen	Persoonlijk account	-	-	Gebruik	Gebruik
Medewerkers ontwikkelpartner	-	Persoonlijk account	Gebruik	Beheer	-	-
Medewerkers Hostingpartij	-	-	Beheer	-	-	-
Gebruikers Primoforum	Lezen	Persoonlijk account	-	Eigen betaal gegevens	-	-
Niet-klanten	Lezen	-	-	-	-	-

3.8 Partners

Ontwikkelpartner
Onze technische partner, betrokken bij de (door-) ontwikkeling van Primoforum, beschikt over

een eigen securitybeleid dat voorafgaand aan de samenwerking is getoetst op de eisen zoals die zijn geformuleerd in dit document.

Hostingpartij
Voor de opslag van sessiegerelateerde data en hosting van de Primoforum applicatie maken wij gebruik van KPN Internedservices dat beschikt over een drievoudige ISO-certificering (9001, 27001 en 20000) en voldoet aan de NEN 7510 normeringen, beschikt over een ISAE 3402 type II accreditatie en over PCI-DSS-compliant en ISO-14001 gecertificeerde datacenters.

ISO 27001 is een security-standaard en in deze standaard zijn richtlijnen (‘best practices’) opgenomen voor informatiebeveiliging. ISAE3402 is een auditstandaard voor rapportage over de uitbestede processen.

De overheid richt zich bijvoorbeeld op ISO27001, omdat dit aansluit bij de Baseline Informatiebeveiliging Rijksoverheid. De zorg richt zich op de NEN7510 die gebaseerd is op ISO27001. Vanuit de financiële wereld is daarentegen ISAE3402 de norm.

Conformering aan deze normen geeft ons de zekerheid dat processen diep geborgd zijn in de organisatie en wij ons daar geen zorgen over hoeven te maken.

Zie ook https://www.internedservices.nl/over-isg/werkwijze/assurance/

4. Certificering KPN Internedservices

ISO 2000 - Service Management op basis van internationale best practices
Door middel van een hosting-SLA hebben wij duidelijke afspraken gemaakt omtrent dienstverlening, beschikbaarheid, recovery, monitoring, oplos- en reactietijden.

ISO 9001:2008 - Leveren van hoogwaardige kwaliteit
ISO 9001 vereist dat een organisatie continu naar verbetering streeft. KPN Internedservices doet dat door processen steeds effectiever en efficiënter te maken.

ISO/IEC 27001:2013 - Informatie veilig beheerd
Alle gegevens worden op professionele wijze beveiligd en beheerd, volledig volgens de ISO/IEC 27001-norm. Deze norm omvat een breed spectrum aan bedrijfsmiddelen. Van digitale informatie, papieren informatie en fysieke middelen als computers en netwerken tot kennis bij individuele medewerkers.

NEN 7510:2011 - Informatiebeveiliging in de zorgsector
Ook voor de zorgsector willen wij op het gebied van informatiebeveiliging over extra zekerheden beschikken. Daarom vinden wij het belangrijk dat onze hostingpartij beschikt over en NEN 7510 certificering.

PCI-DSS - Informatiebeveiliging voor de Payment Card Industry
Net als Chargify is KPN Internedservices een geregistreerd PCI-DSS Level-1 Service Provider.

ISAE-3402 - Zekerheid over interne processen en maatregelen
De verklaring ISAE-3402 type 2 geeft zekerheid over hoe interne processen en de beheersmaatregelen die worden genomen om kwaliteit van dienstverlening te borgen, werken. Met ISAE-3402 wordt informatie altijd op een uniforme manier verstrekt aan opdrachtgevers en externe auditors die alle beheersmaatregelen beoordelen.

ISAE 3402 - Beheersing van processen
ISAE-3402 type II-accreditatie garandeert dat de door KPN Internedservices uitbestede processen goed worden beheerst. Een wettelijke verplichting voor financiële dienstverleners.