Pluform Privacybeleid

Versie 9, 23 april 2018

Inhoudsopgave

1. Pluform Privacybeleid 3
    1.1 Introductie 3
    1.2 Welke gegevens zijn inzichtelijk voor wie? 3
    1.3 Ons inlogprotocol 4
    1.4 Technisch beheer en hosting 4
    1.5 Hoe houden wij Pluform veilig? 4
    1.6 Ontwikkeling en onderhoud 5
    1.7 Wat kan ik doen? 5

1. Pluform Privacybeleid

1.1 Introductie

In dit document vind je informatie over wat Pluform doet om gegevens te beveiligen en de juiste niveaus van dienstverlening, privacy en veiligheid te waarborgen. Dit privacybeleid van Pluform is gebaseerd op de ICT-veiligheidsrichtlijnen voor webapplicaties van het Nederlands Nationaal Cyber Security Centrum (NCSC). Daarnaast is het privacybeleid gebaseerd op de Algemene Verordening Gegevensbescherming en voorschriften met betrekking tot gegevensbescherming en privacy, uitgegeven door het Autoriteit Persoonsgegevens (AP).

Wij behouden ons het recht voor dit privacybeleid aan te passen. Wijzigingen zullen op deze website worden gepubliceerd. Versie 9 23 april 2018.

1.2 Welke gegevens zijn inzichtelijk voor wie?

Toegankelijkheid gegevens voor de verschillende soorten gebruikers. Binnen Pluform hebben gebruikers alleen toegang tot hun eigen gegevens en gegevens die specifiek binnen de coach-cliëntrelatie zijn gedeeld. Daarbij houdt Pluform rekening met het mogelijke beroepsgeheim van een coach.

Verschillende rollen hebben verschillende toegangsniveaus. De rollen binnen de applicatie zijn Organisatiemanager, Coach en Coachee.

- Organisatiemanagers beheren het organisatieaccount in Pluform. Zij zijn in staat om de profielgegevens (bijvoorbeeld naam en e-mail) van coaches en coachees te beheren. Organisatiemanagers zijn niet in staat om toegang te krijgen tot gegevens met betrekking tot de dialoog tussen coaches en coachees.
- Coaches hebben alleen toegang tot de eigen persoonsgegevens en de gegevens van hun eigen coachees.
- Coachees hebben alleen toegang tot hun eigen persoonsgegevens en de (persoons)gegevens die door de coach met hen gedeeld zijn.

Binnen Pluform worden gegevens niet onnodig lang bewaard. Gegevens van Coachees worden tot twee jaar na het einde van het coachtraject bewaard. Gegevens van Coaches worden tot twee jaar na beëindiging van de overeenkomst bewaard. Op verzoek kan Pluform alle gegevens met betrekking tot een specifiek account eerder verwijderen. Daarnaast kunnen Coachees binnen Pluform zelf gemakkelijk hun account en daarmee de bij Pluform bekende persoonsgegevens verwijderen. Dit privacyrecht, net zoals de andere privacyrechten, is gemakkelijk en snel uit te oefenen bij Pluform. Medewerkers van Pluform dragen er zorg voor dat uitoefening van privacyrechten correct en tijdig worden afgehandeld. Zie voor meer informatie het privacystatement (verderop in dit document).

De privacyrechten zijn:

1. Recht op inzage (het recht om kennis te nemen van de op u betrekking hebbende persoonsgegevens en daarvan een kopie te ontvangen)
2. Recht op rectificatie (het recht om de op u betrekking hebbende persoonsgegevens te verbeteren of aan te vullen teneinde fouten of omissies te herstellen)
3. Recht op vergetelheid (het recht op het onverwijld doen wissen van de op u betrekking hebbende persoonsgegevens. Let op! Als coachee kunt u zelf uw account verwijderen, waarmee alle gegevens in de applicatie worden gewist).
4. Recht op beperking van de verwerking (het enkel opslaan en niet verder verwerken van de gegevens)
5. Recht op overdraagbaarheid van gegevens (het recht om de op u betrekking hebbende persoonsgegevens in een gestructureerde, gangbare en machinaal leesbare vorm te verkrijgen zodat deze gegevens overdraagbaar aan derden zijn)
6. Recht op het indienen van een klacht (indien bepalingen in dit reglement en/of de Algemene Verordening Gegevensbescherming niet worden nageleefd, heb je het recht hier een klacht over in te dienen bij de Autoriteit Persoonsgegevens). Bij vragen of opmerkingen kunt u ook altijd contact opnemen met Pluform.

Notificatie e-mails in Pluform. E-mail is een onveilig medium, daarom zullen alle e-mails die verstuurd worden vanuit de toepassing nooit enige vertrouwelijke informatie bevatten. De e-mails die u ontvangt vanuit Pluform worden gebruikt als kennisgevingen aan de werkelijke boodschap. Die bevindt zich binnen de applicatie en is enkel toegankelijk na inloggen met een wachtwoord. Het is niet mogelijk naar gebruikersnamen te vissen met behulp van de verloren wachtwoord-functionaliteit.

Delen gegevens met derde partijen. Gegevens worden niet verkocht aan derde partijen. Gegevens worden enkel overgedragen aan derde partijen als dit noodzakelijk is voor de uitvoering van de overeenkomst tussen Pluform en de klant of als wij gedwongen worden door de Nederlandse wet. Voor de partijen met wie Pluform gegevens deelt, geldt dat wij alleen samenwerken met partijen die dezelfde beveiligingsniveaus als wij erop nahouden. Er worden geen gegevens overgebracht naar 'Patriot Act' aansprakelijke partijen.

Gebruikersstatistieken. Pluform maakt **geen** gebruik van Google Analytics. Dit betekent dat er geen analyses van uw gedrag op onze website worden gemaakt om o.a. gepersonaliseerde reclames aan u aan te bieden.

1.3 Ons inlogprotocol

Wachtwoorden. Gebruikers bepalen zelf hun wachtwoorden. Wachtwoorden dienen tenminste 8 tekens te bevatten, inclusief 1 nummer en ten minste één hoofdletter. Hierdoor is het wachtwoord minder gemakkelijk te raden door anderen. Als u uw wachtwoord bent vergeten, sturen wij een unieke link naar uw e-mailadres. Hiermee kunt u zelf een nieuw wachtwoord instellen. Er worden geen wachtwoorden per e-mail verzonden. Wachtwoorden worden versleuteld opgeslagen in de database.

Tweestapsverificatie via SMS. Naast inloggen door de gebruikersnaam en het wachtwoord biedt Pluform ook de optie om de tweestapsverificatie in te stellen. Als tweestapsverificatie is ingeschakeld voert u, naast uw gebruikersnaam en wachtwoord, ook een extra code in. Deze code heeft u via een SMS'je op uw mobiele telefoon ontvangen. Door deze extra actie is uw account extra beveiligd.

1.4 Technisch beheer en hosting

Pluform heeft zijn IT-hosting-infrastructuur beheerd door True Managed Hosting van True. True verzorgt en beheert de technische aspecten van Pluform, zoals de infrastructuur en datacenters. True levert zogeheten dedicated servers aan ons en is continu bezig met de optimalisatie van de serveromgeving.

Certificaten. Wij hebben voor True gekozen vanwege de grote mate van veiligheid. True is ISO 27001:2013 (informatiebeveiliging), ISO 9001 (kwaliteitsmanagement) en NEN 7510:2011 (informatiebeveiliging in de zorg) gecertificeerd en gebruikt gecertificeerde datacenters die in Nederland gevestigd zijn. Met deze certificeringen voldoet True aan de hoogste standaarden wat betreft informatiebeveiliging.

Datacenter locatie beveiliging. Alle datacenters die gebruikt worden door True hebben metingen van hoog niveau om ongeautoriseerde fysieke toegang tot de servers te voorkomen, met inbegrip van biometrische toegangscontroles, camera's, digitale code locks en veiligheidspersoneel. Alleen geautoriseerde medewerkers hebben toegang tot de serverruimte.

Controle. Op het gebied van informatiebeveiliging is True gecertificeerd voor alle beheerde bedrijfsmiddelen die de dagelijkse managed hosting dienstverlening vormen. De veiligheid en de prestaties van de Pluformservers en applicaties worden continu bewaakt.

1.5 Hoe houden wij Pluform veilig?

Drupal. De Pluform applicatie is gebouwd met Drupal-technologie. Drupal is een raamwerk voor het bouwen van veilige websites en webapplicaties. Drupal wordt al voor meer dan 10 jaar gebruikt en heeft een uitstekend veiligheidstrackrecord.

Beveiliging van dataverkeer. Gebruikersgegevens worden alleen getransporteerd als zij achter slot en grendel zijn door middel van een hoogwaardige SSL (Secure Sockets Layer) encryptie. Gegevens zijn als zij worden onderschept hierdoor niet leesbaar zonder de sleutel. Technische updates, verbeterings- en onderhoudsdata

worden ook alleen getransporteerd als zij zijn gecodeerd (via beveiligde SSH verbindingen). SSH is een cryptografisch netwerkprotocol voor het beveiligen van datacommunicatie.

Audits. IT-systemen en procedures van onze partners worden onderworpen aan audits. Ook Pluform wordt onderworpen aan audits en beschikt over een Third Party Memorandum (een verklaring die wordt afgegeven door een onafhankelijke auditpartij over de kwaliteit van de ICT-dienstverlening, kwaliteit en beheersing van een organisatie).

Firewalls. Om Pluform te beschermen van aanvallen van buitenaf zijn alle Pluform servers uitgerust met een Linux iptables gebaseerde Firewall. Dit betekent dat Pluform als een soort grenscontrole al het inkomende netwerkverkeer checkt en tegenhoudt. Het verkeer wordt pas doorgelaten als het is geclassificeerd als een betrouwbare bron voor inkomend HTTP- en HTTPS-verkeer. De Firewall / grenscontrole is geïnstrueerd om aanvallen met als doel de onbeschikbaarheid van de applicatie (Denial-Of-Service) of intentionele vertraging van de applicatie (throttle traffic) te blokkeren.

Back-ups. Er wordt dagelijks een back-up van de gegevens die op de applicatie staan gemaakt. Elke avond wordt er een back-up overgebracht naar een offsite back-up server. Hierdoor gaan de in Pluform gedeelde gegevens niet zomaar verloren als er zich een probleem voordoet.

Serverbeveiliging. Om een goede server-beveiliging te waarborgen zijn de volgende best practices opgevolgd: Truebeheerders hebben SSH toegang tot de productiemachines. De gebruikersaccounts hebben geen wachtwoorden, alleen SSH-key-based login. De servers zijn alleen toegankelijk via IP beperkte beheerservers. Root-wachtwoorden worden opgeslagen in een versleuteld bestand en gedeeld enkel tussen beheerders. Besturingssysteem software-updates worden eerst getest op testmachines, alvorens ze worden uitgerold naar de acceptatie-en productie-omgeving. De beheerders abonneren zich op verschillende security bulletins om up-to-date te blijven op veiligheidsbedreigingen.

1.6 Ontwikkeling en onderhoud

Pluform wordt voortdurend gemonitord en ontwikkeld. Als wij onderhoud plegen aan de applicatie of een beveiligingsupdate doen, wordt dit gedaan op veilige wijze. Ons onderhoud en ontwikkeling doen wij middels staged development. Hierbij worden alle updates en nieuwe functies eerst op een testserver gezet, waar zij uitgebreid worden getest en gecheckt. Dit wordt alleen door geautoriseerde mensen gedaan. Pas bij akkoord gaan ze naar een acceptatie- en productieserver. Hierdoor kunnen wij tijdig beveiligingsproblemen en kritieke punten herkennen. De daadwerkelijke wijziging voeren wij dus pas door als we er zeker van zijn dat het geen problemen in de beveiliging of beschikbaarheid van de applicatie gaat opleveren.

1.7 Wat kan ik doen?

Bij Pluform doen wij er alles aan om gegevens zo goed mogelijk te beveiligen. Jij, als gebruiker van Pluform, kunt zelf ook acties ondernemen om zo veilig mogelijk te werken. Wij hebben hieronder een paar tips voor jou op een rijtje gezet:

- ***Wachtwoorden.*** Je wilt voorkomen dat iemand anders zomaar toegang heeft tot jouw account. Houd daarom je wachtwoord geheim en deel deze nooit met anderen. Zorg ervoor dat het wachtwoord niet gemakkelijk te raden is. Daarnaast raden wij aan niet automatisch in te loggen (je wachtwoord te laten onthouden door de browser). Hierdoor weet je dat als jouw computer, smartphone of laptop in de handen van iemand anders valt, deze persoon niet zomaar toegang heeft tot jouw Pluform-profiel. Ook raden wij aan tweewegverificatie te gebruiken in je profiel (zie 1.4 in dit privacybeleid).
- ***Wees op de hoogte van privacyrechten.*** Ben je coach? Informeer jouw coachees over de privacyrechten die zij kunnen uitoefenen. Pluform doet dat ook als de coachee voor het eerst inlogt in de applicatie. Als jij het nogmaals doet, weet je zeker dat jouw coachees hun rechten kennen. Ben je coachee? Ga na of je goed bent geïnformeerd en zo niet, trek aan de bel bij jouw coach en stel vragen.
- ***Verzamel niet onnodig gegevens.*** Als coach moet je je altijd afvragen of je niet meer gegevens verzamelt dan je nodig hebt voor het uitvoeren van het traject. Minimaliseer de hoeveelheid data die je hebt zo veel mogelijk, zodat de kans op privacyproblemen zo klein mogelijk blijft.