Informatiebeveiligingsbeleid Kiksaus

Versie: 20180514

Inleiding
Kiksaus heeft privacy, security en transparantie hoog in het vaandel staan. Wij vinden het belangrijk om jou goed te informeren over de maatregelen die we treffen om jouw (persoons)gegevens en die van jou klanten te beschermen. Dit doen we enerzijds om je een gerust gevoel te kunnen geven. Tegelijk biedt dit handvatten voor jou om de juiste inschatting te maken of deze maatregelen voldoende zijn voor het soort gegevens dat je door ons wil laten verwerken.

Algemene organisatorische maatregelen
Binnen ons bedrijf zijn er een aantal maatregelen die we treffen om persoonsgegevens te beschermen tegen verlies, diefstal of onrechtmatig gebruik. Hieronder staan de maatregelen die wij op organisatorisch vlak getroffen hebben.

1. Eventueel ingeschakelde 3e partijen krijgen alleen toegang tot de persoonsgegevens die ze nodig hebben voor het vervullen van hun functie.
2. Voor het verkrijgen van toegang tot persoonsgegevens hebben we meerdere (onafhankelijke) lagen van beveiliging toegepast. Een aantal voorbeelden van maatregelen zijn: Het toepassen van SSH-keys, firewalling en het gebruik van sterke wachtwoorden.
3. Persoonsgegevens mogen in ons bedrijf nooit op andere plekken opgeslagen worden dan afgesproken. Deze locaties zijn: Op de server van de hostingprovider, op de ontwikkelomgeving op de computer van de programmeur en op de schijven die backups bevatten van deze data.
4. We maken gebruik van een password management systeem. Hiermee worden alle door ons zelf gebruikte wachtwoorden altijd van hoge moeilijkheid.
5. De computers en schijven waarop lokale ontwikkelomgevingen staan en backups worden gemaakt, worden nooit met anderen gedeeld.
6. De data opgeslagen op computers en backups zijn voorzien van encryptie, gebruikmakend van Apple's FileVault en Time Machine encryption.

Technische maatregelen tegen ongeoorloofde toegang tot persoonsgegevens
Naast organisatorische maatregelen zijn er ook technische maatregelen die we treffen. Een deel hiervan zijn een vast onderdeel van onze dienstverlening en kunnen niet door jou als eindgebruiker in- of uitgeschakeld worden. Een aantal andere maatregelen bieden wij aan jou aan, maar zijn niet standaard geactiveerd.

1. Onze systemen zijn voorzien van een firewall. Alleen IP-verkeer dat expliciet toegestaan is, kan netwerkverkeer met onze systemen uitwisselen.
2. Voor de toegang tot beheerpanelen bieden wij de mogelijkheid om twee-factor-authenticatie in te schakelen.
3. Voor het opslaan van wachtwoorden maken wij gebruik van sterke en moderne hashing- algoritmes.
4. Je hebt de mogelijkheid om voor elke account op elk gewenst moment je wachtwoord te veranderen. Ons advies is om dit ook regelmatig te doen.
5. Alle websites die wij ontwikkelen, zijn voorzien van een standaard SSL-certificaat met sterke en moderne netwerkversleuteling.
6. We houden bij wat de standaarden m.b.t. cryptografie zijn en werken onze versleutelingsalgoritmes bij wanneer dit nodig is.
7. Wij zullen er zorg voor dragen dat de software die we gebruiken voor het aanbieden van onze diensten up-to-date is.
8. Netwerkcommunicatie van systemen onder ons beheer verloopt altijd over een versleutelde verbinding.
9. Het bedrijf dat de hosting voor Kiksaus verzorgt, waar wij ook een verwerkingsovereenkomst mee hebben, beveiligen hun systemen zoals beschreven in dit document: https://www.antagonist.nl/downloads/informatiebeveiligingsbeleid

kiksaus