VERSIE: 1.3
DATUM: 24/05/2018

INFORMATIEBEVEILIGINGSBELEID ADAPTIVITY BV

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. Onze medewerkers krijgen alleen toegang tot de persoonsgegevens die ze nodig hebben voor het vervullen van hun functie.
2. Persoonsgegevens mogen in ons bedrijf nooit op andere plekken opgeslagen worden dan afgesproken. Hiervoor hebben we interne procedures. Indien van toepassing, dan hoort hier ook een bijhorend retentie-beleid bij om (kopieën) van persoonsgegevens na gebruik te verwijderen.
3. Met onze medewerkers hebben we een geheimhoudingsverklaring.
4. We maken gebruik van een password management systeem. Alle wachtwoorden worden hierin opgeslagen. Op deze manier hebben we controle over welke werknemer toegang heeft tot welke wachtwoorden. Een werknemer krijgt alleen de noodzakelijke wachtwoorden.
5. Medewerkers hebben een eigen laptop. Deze apparatuur wordt nooit met anderen gedeeld en mag niet voor externe doeleinden worden gebruikt.
6. We zorgen ervoor dat medewerkers die ons bedrijf verlaten geen toegang meer hebben tot gegevens.

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 het opslaan van wachtwoorden maken wij gebruik van sterke en moderne hashingalgoritmes.
3. 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.
4. Om brute-force aanvallen te detecteren en automatisch te blokkeren, maken we gebruik van een inbraakdetectiesysteem.
5. Alle beheerpanelen die we aanbieden, zijn voorzien van een 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. Als extra service om te helpen je website veilig te houden, maken wij op al onze servers gebruik van Patchman. Dat is beveiligingssoftware die automatisch kwetsbaarheden in populaire cms'en dicht.

8. Netwerkcommunicatie van systemen onder ons beheer verloopt altijd over een versleutelde verbinding.
9. De basis van een onze ontwikkelde systemen is een eigen framework en geen open-source. Deze source code is alleen maar beschikbaar voor ontwikkelaars van Adaptivity en wordt onder geen enkele voorwaarde openbaar beschikbaar gesteld.
10. We zullen zorgdragen dat de PHP, MySQL versies up-to-date zijn. Op het moment dat dit niet mogelijk is vanwege compatibiliteit, wordt je hiervan op de hoogte gebracht.
11. We houden beveiligingsissues van open-source packages die we gebruiken in projecten in de gaten. Op het moment dat deze worden geüpdatet zullen wij dit doorvoeren in alle beschikbare omgevingen.

Maatregelen voor het borgen van bedrijfscontinuïteit en correctheid van data

1. We controleren periodiek de integriteit van de bij ons opgeslagen data.
2. In het geval van verstoringen van onze dienstverlening is er 24 uur per dag, 7 dagen per week personeel beschikbaar om deze verstoringen zo snel mogelijk te verhelpen.
3. We maken gebruik van een losse ontwikkel-, test- en productieomgeving.
4. We maken periodieke back-ups en slaan deze op een geografisch gescheiden locatie op. Op deze back-ups is een retentiebeleid toegepast.
5. We rusten gebruikte apparatuur, zover dit binnen onze mogelijkheden ligt, redundant uit.
6. We beschikken over twee aparte internetverbindingen van twee verschillende (internet)providers.