Informatiebeveiligingsbeleid Meerdan Media

Versie: 20180703

Inleiding

Meerdan Media vindt privacy, security en transparantie erg belangrijk.

Daarom dit beveiligingsbeleid om u goed te informeren over de maatregelen die we treffen om uw (persoons)gegevens te beschermen.

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. Voor het verkrijgen van toegang tot persoonsgegevens hebben we meerdere(onafhankelijke) lagen van beveiliging toegepast. Een aantal voorbeelden van maatregelen zijn: versleuteling van netwerkverkeer en het toepassen van IP Access Control Lists, firewalling op poorten die niet publiek toegankelijk dienen te zijn en het gebruik van sterke wachtwoorden.

3. Persoonsgegevens mogen in ons bedrijf nooit op andere plekken opgeslagen worden dan afgesproken. Indien van toepassing, dan hoort hier ook een bijhorend retentie-beleid bij om (kopieën) van persoonsgegevens na gebruik te verwijderen.

4. Met onze medewerkers hebben we een geheimhoudingsverklaring.

5. Medewerkers hebben een eigen laptop of eigen vaste computer. Deze apparatuur wordt nooit met anderen gedeeld.

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.

2. Voor het opslaan van wachtwoorden maken wij gebruik van sterke en moderne hashing-algoritmes. In het geval van Open Source, de bij het Open Source pakket aanwezige algoritmes.

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. Wij zullen er zorg voor dragen dat de software die we gebruiken voor het aanbieden van onze diensten up-to-date is, tenzij opdrachtgever geen SLA dan wel servicepack heeft afgenomen.

5. Op verzoek van opdrachtgever kunnen we Patchman, WordFence, Cloudflare of KeyCDN installeren als extra dienst om te helpen je website veilig te houden. Dat is beveiligingssoftware die automatisch kwetsbaarheden in populaire cms'en dicht.

6. Wij bieden aan al onze klanten een mogelijk tot het afnemen van een SSL-certificaat voor het versleutelen van websiteverkeer aan.

7. Wij plaatsen onze servers en overige apparatuur uitsluitend in de meeste moderne datacenters van subverwerkers. Deze datacenters bieden voor ons de juiste beveiliging tegen inbraak, brand, stroomuitval en overige calamiteiten.