Informatiebeveiligingsbeleid Trendesign B.V.

Versie: 20180516

Inleiding

Trendesign B.V. (hierna: Trendesign) 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 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. 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: multi-factor authentication, het gebruik van VPN t.b.v. versleuteling van netwerkverkeer en het toepassen van IP Access Control Lists, firewalling en het gebruik van sterke wachtwoorden.
3. 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.
4. Met onze medewerkers hebben we een geheimhoudingsverklaring.
5. We hebben een intern Security Awareness-programma voor onze medewerkers.

(responsive) webdesign - zoekmachine optimalisatie - online adverteren - analytics

6. We werken met een beoordelingssysteem voor code. Nieuwe functionaliteiten of aanpassingen aan huidige systemen gaan door een vast review- en uitrolproces.
7. We maken gebruik van een password management systeem. Hiermee kunnen we een beveiligingsbeleid m.b.t het gebruik van wachtwoordgebaseerde accounts aan onze medewerkers opleggen en controleren.
8. Medewerkers hebben een eigen laptop. Deze apparatuur wordt nooit met anderen gedeeld. Ook is de dataopslag op deze systemen voorzien van encryptie.
9. 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 het Sucuri 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. Wij zullen er zorg voor dragen dat de software die we gebruiken voor het aanbieden van onze diensten up-to-date is.
8. We passen zo veel mogelijk segmentatie tussen systemen toe. Hiervoor maken we gebruik van containerisatie, virtualisatie en in andere gevallen fysiek gescheiden hardware. Deze segmentatie passen we toe om systemen met een verschillend risicoprofiel, functie en omvang te voorzien van zo veel mogelijk lagen van beveiliging.

9. Netwerkcommunicatie van systemen onder ons beheer verloopt altijd over een versleutelde verbinding.
10. Wij bieden aan al onze klanten een gratis SSL-certificaat voor het versleutelen van websiteverkeer aan. Dit certificaat is zonder tussenkomst van ons te gebruiken.
11. Om te voorkomen dat andere gebruikers van het systeem inzage krijgen tot jouw bestanden maken we onder andere gebruik van containerisatie.

Maatregelen voor het borgen van bedrijfscontinuïteit en correctheid van data

1. We controleren periodiek de integriteit van de bij ons opgeslagen data.
2. We controleren integriteit van de data ‘in-transit’ en nadat het op vaste opslag is weggeschreven.
3. We gebruiken uitsluitend enterprise-grade hardware. Een aantal voorbeelden hiervan zijn het gebruik van Error-Correcting Code (ECC) geheugen en SAS-drives.
4. We hebben diepgaande monitoring op ons platform en systemen.
5. 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.
6. We zijn onafhankelijk van een netwerkleverancier en beheren onze eigen verbindingen van en naar het internet.
7. De netwerkpaden die we gebruiken, zijn geografisch van elkaar gescheiden.
8. We maken gebruik van een losse ontwikkel-, test- en productieomgeving.
9. We maken periodieke backups, controleren de integriteit hiervan en slaan deze op een geografisch gescheiden locatie op. Op deze backups is een retentiebeleid toegepast.
10. Voor alle gebruikte hardware hebben we (op locatie) vervangende apparatuur beschikbaar of leveringsafspraken met leveranciers.
11. We rusten gebruikte apparatuur, zover dit binnen onze mogelijkheden ligt, redundant uit.

Informatie over de door ons gebruikte datacenters

Wij plaatsen onze servers en overige apparatuur uitsluitend in de meeste moderne datacenters. Deze datacenters bieden voor ons de juiste beveiliging tegen inbraak, brand, stroomuitval en overige calamiteiten. Deze datacenters hebben de onderstaande maatregelen genomen om te voldoen aan deze eisen.

1. Er zijn strikte aanmeldprocedures om toegang te krijgen: • Alleen personen die op de vooraf aangelegde toegangslijst staan hebben toegang. • Bij binnenkomst wordt je identiteit gecontroleerd door vakbekwaam beveiligingspersoneel. • Er gelden strikte aanmeldprocedures voor werkbezoeken.
2. De datacenters zijn 24 uur per dag toegankelijk voor onze medewerkers.
3. Onze apparatuur staat in afgesloten racks.
4. We maken uitsluitende gebruik van Nederlandse datacenters.
5. Er is permanente camerabewaking.
6. Elektriciteitstoevoer wordt gegarandeerd door het gebruik van UPS-systemen en noodstroomaggregaten. Voor langdurige verstoringen in het elektriciteitsnetwerk zijn leveringsafspraken voor het aanvullen van de brandstof voor deze noodstroomaggregaten aanwezig.
7. Voor de toevoer van elektriciteit naar onze apparatuur maken we gebruik van gescheiden feeds. Elke feed heeft op zijn beurt een eigen UPS-systeem. 8. De door ons gebruikte elektriciteitsfeeds hebben ruim voldoende overcapaciteit. 9. Apparatuur is geplaatst op verhoogde datavloeren. 10. De datacenters beschikken over redundant uitgeruste klimaatbeheersing. Pagina 2 van 3 11. Er zijn voldoende maatregelen aanwezig om fysieke inbraak tot deze locaties te voorkomen of vertragen. Een aantal voorbeelden hiervan zijn: beveiligd hekwerk, grafelbakken en extra verdikte muren. 12. Deze datacenters beschikken over geavanceerde branddetectie- en blussystemen. Pagina 3 van 3