iReachm.com GDPR Compliancy Document

1. Accountability

1.1 Heeft IReachm.com een data protection officer aangesteld ?

1.1.1 Ja, IReachm.com heeft inderdaad een persoon in dienst die hiervoor is aangesteld. Deze persoon is verantwoordelijk voor het beveiligen van alle data die binnenkomt en buitengaat bij IReachm.com.

1.2 Houdt IReachm.com een processing register bij ?

1.2.1 Ja, IReachm.com houdt een processing register bij.

1.3 Beschikt IReachm.com over een data breach notificatie plan ?

1.3.1 Ja, IReachm.com beschikt over een dergelijk plan.

1.4 Hoe zorgt IReachm.com ervoor dat privacy van de data geïmplementeerd is in de organisatie op zichzelf?

1.4.1 IReachm.com heeft een VLAIO beurs ontvangen die specifiek gebruikt is voor het implementeren van privacy by design in de organisatie. Hierbij werden verschillende initiatieven genomen waaronder data-encryptie, -validatie,…

1.5 Hoe zorgt IReachm.com voor privacy in de interne programma's op zichzelf?

1.5.1 IReachm.com heeft ervoor gezorgd dat de interne programma's enkel toegankelijke zijn met lokale IP adressen alsook alle data geëncrypteerd is.

1.6 Vraagt IReachm.com toestemming aan de gebruikers voor het verwerken van de data?

1.6.1 IReachm.com heeft dit opgenomen in de privacy statement/algemene voorwaarden. Ook zal de app van IReachm.com altijd toestemming vragen voor bepaalde gegevens op te halen. De gebruiker heeft altijd zelf de mogelijkheid om hier negatief op te antwoorden, en daaropvolgend zal IReachm.com geen gebruik maken van de geblokkeerde data door de gebruiker.

2 Klantenrechten

IReachm.com is altijd bereikbaar via chat, mail of telefonisch om de gebruikers de mogelijkheid te geven om de volgende informatie op te vragen. IReachm.com zal de volgende informatie altijd vrijgeven indien nodig ;

2.1.1 Informatie beschikbaar van de gebruiker en de gebruiksdoeleinden
2.1.2 Informatie omtrent de gegevens toegang

2.1.3 Het recht voor rectificatie van bepaalde informatie
2.1.4 Het recht op geruststelling met betrekking tot de geleverde informatie door de gebruiker
2.1.5 Het recht op restricties met betrekking tot het verwerken van de data die beschikbaar wordt gesteld door de user
2.1.6 IReachm.com is verplicht om voor elke actie een notificatie te geven aan de gebruiker. De gebruiker kan zelf beslissen of die via mail of via mobiel verloopt
2.1.7 Informatie met betrekking tot gegevensoverdracht. Deze informatie kan worden aangeleverd in JSON formaat.
2.1.8 Het recht op objectie of protest.
2.1.9 Het recht op objectie tegen geautomatiseerde individuele besluitvorming

3 Organisatorische maatregelen

3.1 Volgt IReachm.com een industrieel geaccepteerde norm zoals bijvoorbeeld ISO27001?

3.1.1 IReachm.com maakt geen gebruik van een norm binnen dit kader. IReachm.com is met andere woorden niet gecertifieerd voor ISO, COPC, ….

3.2 Heeft IReachm.com als organisatie een beleid met betrekking tot het limiteren van toegang tot sensitieve data voor zowel werknemers als aannemers?

3.2.1 IReachm.com heeft een dergelijk beleid waarbij volgende initiatieven zijn genomen:

- Een beperkt aantal personen binnen het bedrijf hebben rechten toegekend gekregen om aan bepaalde informatie te kunnen geraken door middel van gelimiteerde SSH toegang.
- Toegang tot data wordt enkel verleend op subsets van de totale datasets en worden beheerd in verschillende database omgevingen.

3.3 Heeft IReachm.com een beleid waarbij er op regelmatige basis wordt nagekeken of er nog bepaalde medewerkers of aannemers zijn die geen toegang meer moeten hebben tot bepaalde zaken ?

3.3.1 IReachm.com heeft een beleid waarbij elke maand alle wachtwoorden worden gewijzigd en gebruikers worden aangemaand een nieuw wachtwoord te kiezen. Indien bepaalde medewerkers of aannemers niet meer werkzaam zijn in of voor iReachm hebben deze geen toegang meer tot de data.

3.4 Beschikt IReachm.com over een beleid dat rekening houdt met het nakijken of het gebruik van onder aannemingen of derde partijen?

3.4.1 IReachm.com stelt zogenaamde Data Subprocessor overeennkomsten op voor elke partij met dewelke ze samenwerken

3.5 Heeft IReachm.com als organisatie een confidentialiteitsdocument en/of data beveiliging overeenkomsten afgesloten met zijn medewerkers en aannemers?

3.5.1 IReachm.com beschikt over deze documentatie en deze wordt standaard bij elke nieuwe medeweker/aannemer ondertekend door beide partijen.

3.6 Voorziet IReachm.com als organisatie een verplichte training omtrent security ?

3.6.1 Er is geen expliciete training voorzien, maar het arbeidsreglement bevat de nodige richtlijnen hieromtrent

3.7 Heeft IReachm.com als organisatie een beleid voor het disciplineren van personeel wanneer deze de data beveilingsprocessen & procedures schenden ?

3.7.1 IReachm.com heeft geen dergelijk beleid.

3.8 Heeft IReachm.com een clean desk policy?

3.8.1 IReachm.com heeft voor zijn medewerkers intern een clean desk policy die geldt binnen het kantoor.

3.9 Zijn er beveiligingsmaatregelen voor de fysieke plaats(en) waar de informatie wordt behandeld.

3.9.1 IReachm.com werkt samen met Nucleus als datacenter. Voor verdere vragen omtrent het datacenter , verwijzen we u naar Nucleus. Om het kantoor van IReachm.com te kunnen betreden, zijn er voor elke medewerker badges voorzien om het kantoor te kunnen betreden. Concreet heeft een medewerker zowel een badge als een sleutel nodig om het kantoor te kunnen betreden.

4 Technische maatregelen

4.1 Zorgt IReachm.com voor een encryptie bij het versturen van persoonlijke informatie?

4.1.1 Alle communicatie van dergelijke informatie wordt beveiligd met een SSL encryptie, er zal nooit een niet geïncrypteerde communicatie worden verzonden.

4.2 Zorgt IReachm.com voor een encryptie van de persoonlijke informatie in het algemeen?

4.2.1 IReachm.com zorgt ervoor dat elk paswoord Sha256 geïncrypteerd is.

4.3 Maakt IReachm.com gebruik van firewalls voor het beveiligen van gevoelige informatie?

4.3.1 De hosting partner van IReachm.com, Nucleus, voorziet een zeer strikte beveiliging inclusief het gebruik van firewalls.

4.4 Zorgt IReachm.com voor regelmatige updates van de computers / servers & technische infrastructuur?

4.4.1 Nucleus verzorgt alle updates voor ons op regelmatige basis. Indien het om een urgente update gaat, voeren zij dit ook onmiddellijk uit.

4.5 Maakt IReachm.com gebruik van de meest huidige anti-virus & anti-spyware?

4.5.1 Nucleus voorziet een Trend Micro malware protection wat ervoor zorgt dat kwaadaardige software kan tegenhouden vooraleer het de servers bereikt. Voorlopig beschikt IReachm.com niet over deze software.

4.6 Zijn onze interne programma's zo opgemaakt dat zij regels bevatten omtrent complexe paswoorden ?

4.6.1 IReachm.com maakt gebruik van software toepassingen die elk een regelgeving omtrent de complexiteit van een wachtwoord hebben (lengte, complexiteit, historiek etc..)

4.7 Maakt IReachm.com gebruik van een beveiligde omgeving om softwarecode te schrijven zoals bijvoorbeeld CERT, OWASP ?

4.7.1 IReachm.com maakt gebruik van het Meteor platform als framework. Voor meer informatie kan u terecht op ; https://guide.meteor.com/security.html

4.8 Heeft IReachm.com de mogelijkheid om audit logs te genereren om te checken wie access had tot welke middelen op een bepaald tijdstip ?

4.8.1 IReachm.com beschikt hierover alsook over een API audit logging.

4.9 Heeft IReachm.com reeds te maken gehad met veiligheidsinbreuken in de laatste 5 jaar?

4.9.1 IReachm.com heeft geen veiligheidsinbreuken ondervonden in de afgelopen 5 jaar.

4.10 Voorziet IReachm.com als organisatie back-ups van alle informatie ?

4.10.1 IReachm.com voorziet inderdaad back-ups van alle beschikbare informatie.Elke Nucleus server voorziet automatisch een 7 dagen back-up systeem by default. Back-ups worden op elke dag gemaakt doormiddeld van een storage snapshot te maken en deze op te slaan bij een ander datacenter. In het geval van IReachm.com worden deze servers gehost in Antwerpen. De back-ups worden bijgehouden in een datacenter in Brussel.

4.11 Maakt IReachm.com gebruik van een third paty voor onafhankelijke check-up omtrent de security systemen en hun effectiviteit ?

4.11.1 IReachm.com doet geen beroep op een externe partij voor deze checks.

4.12 Zorgt IReachm.com ervoor om informatie anoniem te maken op non-production omgevingen ?

4.12.1 IReachm.com beheert de gegevens van personen in verschillende database omgevingen waardoor er geen verbanden kunnen worden gelegd tussen de verschillende databronnen a.g.v. de gelimiteerde subset toegang van de medewerkers en klanten tot deze data.

5 3rd party risk

5.1 Wordt alle data opgeslagen in de EEA?

5.1.1 IReachm.com werkt hiervoor samen met Nucleus. Nucleus werkt met 4 datacenters in België ; Antwerpen , Nossegem, Diegem & Zaventem. Zowel het datacenter in Nossegem & Antwerpen zijn compleet opgebouwd als high density datacenters. Het datacenter in Diegem is voorzien als een network datacenter waar wij ons fiber netwerk connecteren naar verschillen uplink providers.

5.1.2 Nucleus voorziet op zijn beurt op volgende initiatieven in het kader van GDPR:

5.1.3 Nucleus heeft een dubbele rol: die van dataverwerker (voor de data van jouw klanten die jij bij ons plaatst) én die van dataverwerkingsverantwoordelijke (voor jouw persoonlijke data als klant van Nucleus).

5.1.4 Als dataverwerker zorgen wij voor de data die jij als dataverwerkingsverantwoordelijke verzameld hebt. In die rol zorgen wij ervoor dat

- het duidelijk is wie legale verantwoordelijkheid draagt. Afhankelijk van het type dienst dragen wij als verwerker meer of minder verantwoordelijkheid.
- elke medewerker perfect op de hoogte is van alles wat GDPR inhoudt
- je data maximaal beveiligd is (dankzij ons ISO 27001-certificaat voor databeveiliging)
- we logs bijhouden van dataverwerkingen die we doen op jouw data
- een eventuele schending van de beveiligingen op door ons beheerde infrastructuur, zo snel mogelijk aan jou gemeld wordt
- we van dichtbij opvolgen welke inspanningen onze leveranciers en partners doen om GDPR-compliant te worden
- je beveiligde toegang krijgt tot jouw gegevens of we je een kopie ervan bezorgen wanneer je als klant kiest voor een andere dataverwerker

5.1.5 Als dataverwerkingsverantwoordelijke beheren wij dan weer jouw eigen persoonlijke informatie (als klant van Nucleus). We zorgen ervoor dat we ook in die rol GDPR-compliant zijn. Dat betekent dat jij als datasubject een aantal rechten hebt.

- Je mag je data inkijken en indien nodig laten verbeteren
- Je mag ten allen tijde je mailvoorkeuren wijzigen of je actieve toestemming terugtrekken. Dat kan hier.
- Je mag informatie over je data vragen (hoe lang wij je data bewaren, waarom wij die data verzamelen, welke personen/organisaties er toegang toe hebben, enz.).
- Je mag vragen om je gegevens te wissen. Dit betreft gegevens waarvoor actieve toestemming gegeven is of wanneer er een gerechtvaardig belang is. Data die om contractgerelateerde redenen nodig is (om facturen te kunnen sturen of bepaalde technische aanpassingen te melden, bijvoorbeeld), vallen onder wettelijk bepaalde bewaartermijnen. Na deze termijnen worden de gegevens automatisch gewist.