Verwerkersovereenkomst 2023 - Trinity Sales B.V.

Ter bescherming van uw gegevens zullen wij gepaste technische en organisatorische maatregelen nemen die in overeenstemming zijn met de toepasselijke wetgeving op het gebied van gegevensbeveiliging. Afhankelijk van de stand van de technologie, de kosten van implementatie en de aard van de te beschermen gegevens, treffen wij technische en organisatorische maatregelen ter voorkoming van risico's zoals vernietiging, verlies, wijziging en ongeautoriseerde bekendmaking van of toegang tot uw gegevens. Dit met als doel om voldoende bescherming te bieden aan de persoonsgegevens van de klant in overeenstemming met artikel 32 van de AVG. De technische en organisatorische maatregelen zorgen voor de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de systemen en diensten in verband met deze Verwerkersovereenkomst.

1. Toegangscontrole

Trinity Sales B.V. treft verscheidene maatregelen om te voorkomen dat onbevoegden fysiek toegang krijgen tot gegevensverwerkingssystemen waarop Persoonsgegevens worden verwerkt of gebruikt (fysieke toegangscontrole), denk hierbij aan:

- Toegangscontrole
- Toegangsautorisatie concepten
- Regulering omtrent de verschaffing van sleutels
- Toezicht op bezoekers door personeel
- Buiten kantooruren beveiliging door middel van een alarmsysteem
- Compartimentering met gecontroleerde toegang
- Entreebeveiliging
- Veiligheidsmaatregelen voor het gebouw en terrein (alarmsysteem)
- Beveiligde toegang tot serverruimte
- Serverruimte ondergebracht in afsluitbare ruimten/ datacentra
- Back-up data opgeslagen op locatie met beperkte toegang

2. Toegangsbeheer

Trinity Sales B.V. heeft de volgende maatregelen geïmplementeerd om te voorkomen dat onbevoegden gegevensverwerkingssystemen gebruiken:

- Het gebruik van two-factor authenticatie bij inloggen van buiten het eigen netwerk
- Restrictie voor inloggen vanaf geverifieerde & geaccordeerde vaststaande IP-adressen van werknemers bij inloggen op SFTP verbindingen
- Afsluitbare dataverwerkingssystemen
- Beveiliging van computerwerkplekken
- Regulatie van gebruikersautorisatie

- Gebruik van individuele paswoorden
- Automatisch blokkeren van gebruikersaccounts na het invoeren meerdere foutieve paswoorden
- Automatische, met paswoord-beschermde, schermbeveiliging van computers na inactiviteit
- Wachtwoord beleid met minimale eisen voor paswoord complexiteit:
    - Op zijn minst 8 tekens
    - Op zijn minst gebruik van twee van de volgende: Hoofd- en kleine letters, speciale tekens, cijfers
- Processen voor het toewijzen van toegangsrechten voor nieuwe werknemers
- Processen voor het terugtrekken van toegangsrechten van werknemers die van afdeling wisselen
- Processen voor het terugtrekken van toegangsrechten van werknemers die uit dienst treden
- De verplichting om te voldoen aan geheimhoudingsvoorzieningen voor gegevens op grond van de AVG
- Vastleggen en analyseren van systeemgebruik
- Vertrouwelijke vernietiging van gegevens

3. Bewerkingscontrole

Maatregelen die erop gericht zijn om ervoor te zorgen dat personen, die het recht hebben om een gegevensverwerkingssysteem te gebruiken, alleen toegang kunnen krijgen tot die gegevens waar ze een specifieke autorisatie voor hebben.

- Persoonsgegevens kunnen niet zonder toestemming worden gelezen, gekopieerd, gewijzigd of verwijderd tijdens verwerking, gebruik of na opslag.
- Trinity Sales B.V. werkt met bedrijfssoftware waarbij medewerkers telkens slechts 1 (één) set van contactgegevens kunnen opvragen en inzien.
- Het exporteren van datasets (meer dan 1 set aan contactgegevens) is onmogelijk voor individuele medewerkers.

4. Transmissiecontrole

Trinity Sales B.V. hanteert de volgende maatregelen om ervoor te zorgen dat Persoonsgegevens niet zonder kunnen worden gelezen, gekopieerd, gewijzigd of verwijderd autorisatie tijdens elektronische overdracht of transport of tijdens opslag op gegevensdragers:

- We gebruiken waar mogelijk in afstemming met de klant een SFTP-server waar de gegevensbestanden kunnen worden opgehaald
- De leads worden vooraf via een e-mailverificatie in twee stappen verzonden
- Bestanden die via mail verzonden worden aan een klant zullen altijd beveiligd zijn met een wachtwoord.
- Wachtwoord worden separaat (bij voorkeur via een ander elektronisch medium) aan de ontvanger verstrekt.

5. Invoercontrole

Maatregelen om ervoor te zorgen dat met terugwerkende kracht kan worden onderzocht en vastgesteld of en door wie persoonsgegevens zijn ingevoerd, gewijzigd of verwijderd uit een gegevensverwerkingssysteem. In alle klant gerelateerde processen wordt een logdatum en -tijd bijgehouden.

- Identificatie/labelen van ingevoerde gegevens
- Definities van de verantwoordelijkheden omtrent gegevensinvoer
- Vastleggen van invoer/verwijdering
- Er bestaat er een procedurele-, programma- en werkfloworganisatie
- Controle van gegevensinvoer
- De verplichting om te voldoen aan de wet bescherming persoonsgegevens
- Controle over de toegangspermissies

6. Taakcontrole

Taakcontrole is vereist om ervoor te zorgen dat persoonsgegevens die namens anderen worden verwerkt strikt volgens de instructies van de Klant worden verwerkt.

Maatregelen:

Trinity Sales B.V. gebruikt controlemechanismen en processen om de naleving van de contracten tussen Trinity Sales B.V. en haar klanten, subverwerkers en andere dienstverleners te bewaken. Persoonsgegevens vergen in het kader van de GDPR wetgeving minimaal hetzelfde beveiligingsniveau als vertrouwelijke informatie.

- Alle medewerkers en contractuele subverwerkers van Trinity Sales B.V. zijn contractueel verplicht om de vertrouwelijkheid van alle gevoelige informatie, inclusief bedrijfsgeheimen van klanten en -partners, te respecteren.
- Trinity Sales B.V. medewerkers kunnen zonder medeweten en toestemming van de klant geen toegang krijgen tot een klantsysteem of klantspecifieke data.

7. Beschikbaarheidscontrole

Maatregelen om ervoor te zorgen dat persoonsgegevens worden beschermd tegen willekeurige vernietiging of verlies:

- Data back-up plannen (er wordt dagelijks een volledige back-up gemaakt, waarbij 1 back-up per week extern versleuteld wordt opgeslagen)
- Toegangsrechten tot serverruimte is beperkt tot het noodzakelijk personeel
- Brandalarmen & Airconditioning is aanwezig in de serverruimte
- Back-up systemen staan in aparte locatie
- CO2 brandblussers in de serverruimte aanwezig

8. Gegevensscheidingscontrole

Persoonsgegevens die voor verschillende doeleinden worden verzameld, kunnen gescheiden worden verwerkt.

Maatregelen:

- Trinity Sales B.V. gebruikt passende technische controlemechanismen om te allen tijde voor scheiding van klantgegevens te zorgen. Iedere klant/elk project heeft zijn eigen map.
- Wij hanteren een autorisatieconcept voor de gescheiden verwerking van gegevens van verschillende klanten.