Beleidsdocument Gegevensbeveiliging Trinity BV

Dit document is bedoeld voor medewerkers, sollicitanten en zakelijke partners van Trinity BV en beschrijft de informatiebeveiliging van de organisatie in overeenstemming met de wet Algemene Verordening Gegevensbescherming (AVG). Dit document bevat details over de technische en organisatorische maatregelen die zijn geïmplementeerd voor de bescherming van persoonsgegevens.

1. Toegangscontrole tot de locatie van de organisatie
Om ongeoorloofde toegang tot gegevensverwerkingssystemen te voorkomen, zijn de volgende maatregelen genomen:

- Alarmsysteem met meldcentrale;
- Camerabewaking;
- Twee-factor authenticatie;
- Sleutelmanagement;
- Alle bezoekers worden begeleid door geautoriseerd personeel.

2. Toegang tot systemen
Trinity BV heeft maatregelen getroffen, waardoor niet-geautoriseerde partijen geen gebruik kunnen maken van de systemen omtrent gegevensverwerking:

- Principle of least privilige: Specifieke gebruiksprofielen gekoppeld aan verschillende IT-systemen, zodat medewerkers alleen benodigde personeelsgegevens kunnen inzien;
- Beperkte toegang voor wijzigingen en onderhoud;
- Toegang alleen mogelijk via een beveiligde lijn: extern via HTTPS en intern via gebruikersnaam en wachtwoord;
- Inspectie en updates door CRM en HRM leverancier (AFAS);
- Gebruik van VPN-technologie.

3. Toegang tot data
Medewerkers hebben alleen toegang tot de persoonsgegevens die onder hun gebruikersrecht vallen. Daarnaast hebben niet-geautoriseerde medewerkers geen toegang tot de persoonsgegevens, waardoor zij geen gegevens kunnen lezen, wijzigen, kopiëren of wissen. Hiervoor heeft Trinity BV de volgende maatregelen genomen:

- Authenticatie met gebruikersnaam en wachtwoord;
- Aanmaken van gebruikersprofielen en toewijzen van gebruikersrechten;
- Automatische time-out na inactiviteit van gebruikers;
- Extra beveiliging door HTTPS, waardoor het internetverkeer tussen bezoekers van de website en de servers van Trinity BV niet kunnen worden onderschept;
- Sterke wachtwoorden kunnen worden afgedwongen (AFAS);
- Gebruikers kunnen hun wachtwoord bij eerste toegang te wijzigen (intranet en Inplanning);

4. Controle op data-invoer en data-overdracht
Trinity BV heeft maatregelen getroffen om inzichtelijk te hebben door wie persoonlijke gegevens zijn ingevoerd, gewijzigd of verwijderd op gegevensverwerkingssystemen. Tevens heeft Trinity BV er voor gezorgd dat persoonlijke gegevens niet kunnen worden gelezen, gekopieerd of gewijzigd tijdens elektronische verzending.

Data-invoer

- Verwerkingsregister waarin alle data en informatiestromen met persoonsgegevens overzichtelijk zijn weergegeven;
- Logboekregistratie van alle gegevensbewerkingen;
- Traceerbaarheid van invoer, wijziging en verwijdering van gegevens door individuele gebruikers;
- Toewijzing van gebruikersrechten;
- Beperkte autorisatie kan worden opgelegd voor specifieke gebruikers om te voorkomen dat gegevens verwijderd worden.

Data-overdracht

- Toevoeging van Re-Capta aan het sollicitatieformulier;
- Gebruik van VPN-technologie;
- Dataoverdracht vindt plaats via een beveiligde lijn (HTTPS);
- Persoonsgegevens worden nooit opgeslagen op draagbare gegevensdragers;
- Alle servers bevinden zich binnen de Europese Economische Ruimte (EER).

5. Interne training en beleid

Trinity BV zorgt ervoor dat haar medewerkers op de hoogte zijn van en weten te handelen naar de richtlijnen van AVG door middel van:

- Een presentatie aan medewerkers omtrent AVG;
- Het opstellen van interne beleidsdocumenten voor omgang met persoonsgegevens;
- Een aanvulling aan het arbeidscontract wat betreft de vertrouwelijke omgang van persoonsgegevens;
- Het communiceren van het AVG-beleid bij de inwerktrajecten.

6. Controle op blijvende beschikbaarheid van persoonlijke gegevens

Trinity BV zorgt voor bescherming tegen onbedoeld(e) verlies of vernietiging van persoonlijke gegevens:

- Automatisch back-up en herstel proces;

7. Controle op gegevensverwerking

Trinity BV ziet er als gegevenseigenaar op toe dat persoonsgegevens die door een gegevensverwerker worden verwerkt, alleen worden verwerkt zoals Trinity BV heeft opgedragen door de volgende maatregelen:

- Afspraken worden vastgelegd in een verwerkersovereenkomst;
- Het aanstellen van de Backoffice-afdeling als contactpersoon voor AVG;
- Voortdurende beoordeling van activiteiten;
- Verplichting van de werknemers om de vertrouwelijkheid van gegevens te handhaven;
- Veilige vernietiging van gegevens na beëindiging van het contract.

Naleving Algemene Verordening Persoonsgegevens (AVG)

Investeringen in hardware- en software, huidige processen en technologieën, beleid en audits zorgen ervoor dat de beschermende maatregelen worden nageleefd en voortdurend worden verbeterd.