ICT-veiligheidsbeleid in het kader van GDPR

Groep INTRO vzw met maatschappelijke zetel in de Charles Parentéstraat 6, 1070 Brussel en ingeschreven in de K.B.O onder nummer 461936071, is verwerkingsverantwoordelijke van persoonsgegevens.

Groep INTRO Maatwerk vzw met maatschappelijke zetel in de Charles Parentéstraat 6, 1070 Brussel en ingeschreven in de K.B.O. onder nummer 0472098703, is verwerkingsverantwoordelijke van persoonsgegevens.

Groep INTRO Schoonmaak vzw met maatschappelijke zetel in de Charles Parentéstraat 6, 1070 Brussel en ingeschreven in de K.B.O. onder nummer 0472098703, is verwerkingsverantwoordelijke van persoonsgegevens.

Hierna worden deze vzw's 'Groep INTRO' genoemd.

Groep INTRO leeft als verwerkingsverantwoordelijke de Belgische privacywetgeving en de bepalingen van de General data Protection Regulation (GDPR) of de Algemene Verordening Gegevensbescherming (AVG) na.

Groep INTRO geeft diegenen van wie zij persoonsgegevens verwerkt alle rechten die zij vanuit de GDPR-regeling hebben. Deze nota beschrijft de procedure voor de uitoefening van de rechten van die betrokkenen.

Bij het eerste contact met klanten-deelnemers en met medewerkers maakt Groep INTRO duidelijk welke rechten zij hebben en hoe ze die (gratis) kunnen uitoefenen.

1. Inleiding

Dit ICT-veiligheidsbeleid beschrijft de richtlijnen, verantwoordelijkheden en maatregelen die onze organisatie implementeert om de persoonsgegevens van klanten, medewerkers en andere belanghebbenden te beschermen in overeenstemming met de Algemene Verordening Gegevensbescherming (GDPR). Het beleid heeft tot doel de integriteit, vertrouwelijkheid en beschikbaarheid van persoonsgegevens te waarborgen.

2. Doel

Het doel van dit beleid is om een veilige ICT-infrastructuur te bieden die voldoet aan de wettelijke eisen van de GDPR. Het beleid stelt richtlijnen vast voor het beheer en de bescherming van persoonsgegevens tegen ongeoorloofde toegang, verlies, diefstal of vernietiging.

3. Toepassingsgebied

Dit beleid is van toepassing op alle medewerkers, contractanten, en derden die toegang hebben tot de ICT-systemen en persoonsgegevens van Groep INTRO. Het beleid geldt voor alle persoonsgegevens die worden verzameld, opgeslagen, verwerkt of gedeeld door de organisatie.

4. Verantwoordelijkheden

Functionaris Gegevensbescherming (FG): Verantwoordelijk voor toezicht op de naleving van de GDPR en dit beleid, inclusief advisering en rapportage.

ICT-afdeling: Verantwoordelijk voor de technische beveiliging van systemen en de implementatie van de maatregelen zoals beschreven in dit beleid.

Alle medewerkers: Verantwoordelijk voor het naleven van dit beleid en het melden van beveiligingsincidenten.

5. Beveiligingsmaatregelen

Voor meer details over de verschillende onderdelen en gebruikte technologieën, zie Bijlage.

5.1 Toegangsbeheer

- toegang tot persoonsgegevens is beperkt tot geautoriseerd personeel
- sterke wachtwoorden en multifactor-authenticatie (MFA) zijn vereist voor toegang tot systemen die persoonsgegevens verwerken
- de toegang wordt periodiek geëvalueerd en ingetrokken wanneer niet langer nodig

5.2 Versleuteling en gegevensbescherming

- alle persoonsgegevens worden versleuteld tijdens opslag en overdracht om de vertrouwelijkheid te waarborgen
- bitLocker-encryptie is geïmplementeerd voor laptops en desktops om gegevensbescherming te garanderen
- er wordt gebruik gemaakt van up-to-date versleutelingsprotocollen (zoals TLS, AES)

5.3 Back-ups

- regelmatige back-ups van kritieke systemen en persoonsgegevens worden uitgevoerd en opgeslagen op veilige locaties

5.4 Patchmanagement en updates

- ICT-systemen worden regelmatig geüpdatet om bekende kwetsbaarheden te verhelpen.
- een proactieve patchmanagementstrategie is geïmplementeerd

5.5 Incidentbeheer

- beveiligingsincidenten worden onmiddellijk gemeld aan de Functionaris Gegevensbescherming

- er is een incidentresponsplan opgesteld dat beschrijft hoe beveiligingsincidenten worden behandeld

5.6 Logging en monitoring

- er wordt gebruik gemaakt van auditlogboeken en monitoringtools waarmee verdachte activiteiten worden gedetecteerd en vastgelegd

5.7 Continuïteit en bescherming tegen DDoS-aanvallen

- er wordt gebruik gemaakt van geavanceerde maatregelen voor continuïteit, failover, en bescherming tegen DDoS-aanvallen

5.8 Printen

Groep INTRO maakt gebruik van beveiligd afdrukken. Medewerkers van Groep INTRO die hiervan gebruik maken ontvangen hiervoor een persoonlijke code.

Voor alle locaties waar deze service wordt aangeboden is het verplicht om enkel af te drukken door het gebruik te maken van de aangeleverde persoonlijke code. Rechtstreeks afdrukken naar deze printers wordt enkel toegestaan na akkoord van de informaticadienst.

Personen van externe bedrijven of tijdelijke medewerkers die gebruik maken van eigen computermateriaal mogen geen gebruik maken van de printers van Groep INTRO.

Er wordt enkel afgedrukt vanuit computermateriaal dat werd aangeleverd door de informaticadienst.

6. Evaluatie en actualisatie

Dit ICT-veiligheidsbeleid wordt minstens jaarlijks geëvalueerd en, indien nodig, aangepast om te blijven voldoen aan de veranderende wettelijke vereisten en technologische ontwikkelingen.

7. Handhaving

Naleving van dit beleid is verplicht voor alle medewerkers en contractanten.