Gegevensbeschermingsbeleid

Intercare NV

Inhoudstafel

1 Het belang van gegevensbescherming

INTERCARE NV hecht grote waarde aan het juist beschermen van de gegevens die zij verwerkt, in het bijzonder persoonsgegevens. Middels dit beleid wil INTERCARE NV op strategisch niveau vastleggen op welke wijze gegevens beschermd worden, welke verantwoordelijkheden hierrond zijn toegewezen en welke prioriteiten INTERCARE NV heeft bepaald rond de bescherming van gegevens.

In het bijzonder willen INTERCARE NV de gegevens van klanten en de persoonsgegevens die zij ter beschikking stellen, beschermen tegen:

- verlies: gegevens zijn niet meer beschikbaar
- lekken: gegevens komen in verkeerde handen terecht
- fouten: gegevens zijn niet correct, bijvoorbeeld verouderd of onvolledig
- niet toegankelijk: op het moment van de noodzaak zijn gegevens niet toegankelijk
- onterecht inkijken: ingekeken door personen die hiertoe niet gemachtigd zijn
- het niet kunnen nagaan wie de gegevens inkeek, wijzigde of verwijderde
- verwerkingen die niet in lijn liggen met regelgeving, richtlijnen en normen

INTERCARE NV wil in dit beleid een beroep doen op iedereen die betrokken is bij de elektronische en papieren verwerking om samen, vanuit een gemeenschappelijke visie én vanuit onze gezamenlijke wil om kwaliteitsvolle dienstverlening aan te bieden, de verwerking van persoonsgegevens correct te laten verlopen.

Dit beleidshandboek gaat dieper in op de bescherming van de persoonlijke levenssfeer van en meer in het bijzonder, de informationele privacy. Dit beleidshandboek dient als richtnorm voor het verwerken van de persoonsgegevens van de klanten, leveranciers, personeel en andere relaties door INTERCARE NV. Het is een leidraad voor alle verwerkingsprocessen en biedt een referentienorm voor audit en controle. Het beleidshandboek biedt elke belanghebbende, medewerker of betrokken externen een inzage in het gegevensbeschermingsbeleid en de manier waarop we omgaan met persoonsgegevens.

Het handboek is tevens geschreven voor iedereen die een functie heeft binnen INTERCARE NV waarbij persoonsgegevens verwerkt worden. Ze gebruiken (delen van) dit beleidshandboek voor het ontwerpen van procedures en richtlijnen voor medewerkers en externen, zoals ICT-leveranciers. De relevante onderdelen van dit beleidshandboek worden verwerkt in overeenkomsten met personeel en leveranciers.

2 De organisatie van gegevensbescherming

Bevoegdheid Als verantwoordelijke voor de verwerking, ligt de bevoegdheid van dit beleid bij INTERCARE NV.

De DPO

De inhoudelijke opvolging van het gegevensbeschermingsbeleid ligt bij het Managementteam en de IT-Manager.

Omwille van het feit dat we geen overheidsinstantie zijn, noch op grote schaal persoonlijke gegevens verzamelen en wegens het niet uitvoeren van automatische monitoring/profilering heeft INTERCARE NV besloten om geen officiële DPO aan te stellen en het takenpakket dat bij hem hoort toe te wijzen aan het Managementteam en de IT-Manager.

Het Managementteam en de IT-Manager voert deze taak uit volgens de bepalingen in de GDPR. Het Managementteam en de IT-Manager rapporteert aan INTERCARE NV en is meer in het bijzonder belast met:

- Adviezen en aanbevelingen voorleggen
- Bevorderen van de bewustwording van alle actoren binnen INTERCARE NV
- Ziet toe op de naleving van het gegevensbeschermingsbeleid binnen INTERCARE NV.
- Documenteert het nodige rond gegevensbescherming, zoals een veiligheidsplan en het verwerkingsregister
- Voert de specifieke taken uit die aan het Managementteam en de IT-Manager zijn toegekend in het kader van de GDPR
- Registreert overtredingen en maakt deze, samen met een advies, over.

De medewerker

Iedereen (intern of extern) die gegevens verwerkt (bijvoorbeeld inkijkt, registreert, wijzigt, …), doet dit volgens de beleidsprincipes uit dit beleidshandboek. De gebruiker verwerkt gegevens in overeenstemming met de discretieplicht, en conform volgende principes:

- Is verantwoordelijk voor de gegevens die hij/zij verwerkt
- Voert de veiligheidsrichtlijnen uit tijdens zijn/haar verwerkingsopdracht.
- Verwerkt enkel die gegevens die horen bij de taak
- Draagt zorg voor de gegevens
- Meldt inbreuken
- Heeft respect voor de vertrouwelijkheid van de gegevens

ICT-medewerker of key user

De ICT-medewerker of key user zijn, bovenop de verantwoordelijkheden voor de gebruiker, verantwoordelijk voor:

- De implementatie van de technische maatregelen
- De veiligheidsinstellingen te implementeren in lijn met dit beleidshandboek.
- De veiligheidsproblemen die ontstaan voor, tijdens of na de implementatie van ICT-middelen te melden.
- Te fungeren als expert. Vanuit deze rol neemt hij/zij deel aan de identificatie zowel als aan de remediëring van de gegevensbeschermingsrisico’s
- De gedragscode na te leven.

ICT-leverancier

De ICT-leverancier heeft dezelfde verantwoordelijkheden als deze van een ICT-medewerker. Bijkomstig:

- Wijst hij op veiligheidsrisico's van geleverde toepassingen
- Wijst de leverancier op de op te nemen veiligheidstaken Streeft de leverancier een transparant gegevensbeschermingsbeleid na door te communiceren over het eigen actuele veiligheidsniveau en bij de afhandeling van veiligheidsincidenten.

3 Scope van het gegevensbeschermingsbeleid

Dit beleid, samen met de IT-Policy aanwezig in het arbeidsreglement, is van toepassing voor de gehele levensduur van informatie binnen INTERCARE NV, van het verkrijgen van informatie tot de uiteindelijke verwijdering van informatie binnen de Intercare NV.

Dit beleid geldt voor geheel INTERCARE NV:

- Het kantoor van INTERCARE NV
- Alle personeelsleden van INTERCARE NV, zowel interne medewerkers die tewerkgesteld zijn binnen INTERCARE NV voor bepaalde of onbepaalde duur als externen waarop INTERCARE NV in een zelfstandige samenwerking beroep doet
- Alle bedrijfsmiddelen en informatieverwerkende systemen beheerd door INTERCARE NV evenals systemen beheerd door externen ten behoeve van informatieverwerkingen voor INTERCARE NV zoals databases, informatie ongeacht de drager ervan, netwerken, datacenters, etc.
- Alle verwerkingsactiviteiten, zowel als verwerkingsverantwoordelijke als verwerker.

Voor bepaalde domeinen of processen binnen INTERCARE NV kunnen aanvullende richtlijnen of procedures worden uitgewerkt die in detail omschrijven welke maatregelen genomen worden om het gewenste niveau van gegevensbescherming te bereiken. Dit beleid, samen met de IT-Policy aanwezig in het arbeidsreglement, is de kapstok waar alle andere richtlijnen of procedures onder vallen.

Gezien de belangrijke rol van de ICT-leveranciers bij het opzetten van de ICT-omgeving om gegevens te verwerken, legt het beleidshandboek hiervoor ook de beleidsprincipes vast.

Deze beleidsprincipes en genomen maatregelen hebben niet de roeping om een resultaatgebonden uitwerking te realiseren, maar beogen het voldoen aan de passende technische en organisatorische maatregelen zoals voorzien door de GDPR/AVG.

4 Het beheer van risico's

INTERCARE NV brengt de risico's inzake gegevensbescherming in kaart aan de hand van een risico analyse, die voor het eerst werd uitgevoerd in het 1e kwartaal van 2018. De risico analyse werd uitgevoerd op basis van volgende criteria (toetsingskader):

- De richtsnoeren met betrekking tot de informatiebeveiliging van persoonsgegevens, zoals deze werden gepubliceerd door de Commissie voor de Bescherming van de Persoonlijke Levenssfeer
- De Algemene Verordening Gegevensbescherming
- De ISO 27001 norm rond informatiebeveiliging

De analyse bracht operationele en tactische risico's in kaart. Deze risico's werden voor het eerst besproken op 28/02/18. De bevindingen uit de risico analyse werden besproken en worden

opgenomen in een actieplan om de gevonden risico's te behandelen. Hierin onderkent INTERCARE NV vier mogelijk risicobehandelingen:

- Accepteren: een risico wordt geaccepteerd, er worden geen aanvullende maatregelen genomen. INTERCARE NV streeft er naar zo min mogelijk risico's te accepteren.
- Overdragen: een risico wordt overgedragen waardoor de verantwoordelijkheid ten aanzien van het risico niet langer bij INTERCARE NV rust.
- Beperken: INTERCARE NV neemt de noodzakelijke maatregelen om een risico te beperken zodat het risico wordt teruggebracht tot een niveau waarop het te accepteren is.
- Uitsluiten: INTERCARE NV neemt maatregelen om te voorkomen dat een risico zich überhaupt kan voordoen.

Het doel is dat de risico analyse minstens jaarlijks wordt herzien. Dit maakt onderdeel uit van de werkzaamheden van het Managementteam en de IT-Manager.

De actiepunten die momenteel prioritair zijn in functie van de uitgevoerde risico analyse vindt u terug in het hoofdstuk 6.

5 Beleidsdoelstellingen voor gegevensbescherming

INTERCARE NV, zowel in haar rol als verwerkingsverantwoordelijke als verwerker:

1. Is transparant over de persoonsgegevens die het verwerkt en het verwerkingsdoel, zowel naar de betrokkene, de klanten als naar de toezichthouders. De gevoerde communicatie is eerlijk, eenvoudig toegankelijk en begrijpelijk. Het transparantieprincipe is ook van toepassing wanneer de persoonsgegevens worden uitgewisseld.
2. Verwerkt enkel de gegevens die relevant zijn voor het uitvoeren van haar taken. Elke taak waarbij persoonsgegevens worden verwerkt, is rechtmatig. Dit betekent onder meer dat de verwerking in overeenstemming is met de wettelijke en statutaire doelen van INTERCARE NV. Dit wordt telkens geëvalueerd bij een nieuw verwerkingsdoel, waar nodig aan de hand van een gegevensbeschermignseffectbeoordeling.
3. Verwerkt enkel de persoonsgegevens die strikt noodzakelijk voor de uitvoering van de activiteiten. Zo worden identificatoren die horen bij de persoonsgegevens tot een minimum herleid.
4. Kijkt toe op de integriteit van de persoonsgegevens gedurende de ganse verwerkingscyclus.
5. Bewaart gegevens niet langer dan noodzakelijk. De noodzakelijkheid is afgetoetst tegenover wettelijke verplichtingen en de rechten en vrijheden van de betrokkene.
6. Voorkomt inbreuken die voortvloeien uit het verwerken van persoonsgegevens. Informatieveiligheid, gegevensbescherming bij ontwerp en privacy-vriendelijke standaardinstellingen zijn hiervoor hulpmiddelen. Wanneer een inbreuk plaatsvindt, wordt hierover gerapporteerd in lijn met de regelgeving ter zake.
7. Is in staat om alle geldende rechten van een betrokkene, zoals het recht op inzage, afschrift en eventueel ook schrapping uit te voeren. INTERCARE NV waakt hierbij over de eventuele beperkingen die op deze rechten van toepassing zijn.
8. Waakt er actief over dat bij het verwerken van de persoonsgegevens voor een welbepaald doel, de rechten en vrijheden van de betrokkene gevrijwaard blijven.
9. Verwerkt gegevens in lijn met de rechten en vrijheden die gelden in de Europese Economische Ruimte en controleert de toepassing hiervan wanneer de gegevens worden

uitgewisseld daarbuiten. INTERCARE NV leeft bijgevolg alle wettelijke en normerende kaders na (i.e. zowel Vlaamse, Federale als Europese regels) bij het verwerken van persoonsgegevens en heeft daartoe haar verantwoordelijkheid over de persoonsgegevens en die van andere duidelijk in kaart gebracht.

10. Kan aantonen dat het alle beleidsdoelstellingen naleeft, conform de wettelijke bepalingen. Deze verantwoordingsplicht wordt bewaakt door interne toezicht en controle en is uitvoerbaar volgens de wettelijk geldende principes.

6 Gegevensbescherming en informatieveiligheid

6.1 Onderscheid gegevensbescherming en informatieveiligheid

Informatieveiligheid is een belangrijk onderdeel binnen gegevensbescherming, beiden zijn echter wel degelijk verschillend.

Gegevensbescherming omvat alle aspecten zoals benoemd in de GDPR/AVG over de wijze waarop persoonsgegevens mogen worden verwerkt. Het betreft in feite de principes zoals deze ook benoemd zijn in hoofdstuk 5. Een onderdeel hiervan is de beveiliging van de gegevens, maar gegevensbescherming is dus breder dan enkel het beveiligen van gegevens.

Informatieveiligheid betreft de beveiliging van alle soorten informatie binnen een organisatie, waaronder persoonsgegevens. Dit is waar informatieveiligheid relevant is voor gegevensbescherming, en waar de twee elkaar ontmoeten: informatieveiligheid omvat het beveiligen, naast alle andere informatie, van persoonsgegevens en gegevensbescherming omvat dan weer alle aspecten rond de omgang met persoonsgegevens, waaronder de beveiliging.

6.2 Doelstellingen informatieveiligheid

De wetgeving vraagt dat de gepaste technische en organisatorische maatregelen worden genomen ter beveiliging van de persoonsgegevens. Hieronder worden de belangrijkste uitgangspunten rond informatieveiligheid uiteen gezet, verdeeld over de verschillende organisatorische maatregelen die genomen zijn, en de technische maatregelen die genomen zijn.

6.2.1 Organisatorische maatregelen

ISO Hoofdstukken 5, 6, 7, 9 (deels, access control policies), 11 (deels, beleid, afspraken), 15, 16 (deels, de incident mgt policy), 17 en 18 BV:

Beleid:

- INTERCARE NV voorziet in de nodige informatieveiligheidsrichtlijnen en -procedures welke vallen onder het algemene informatieveiligheidsbeleid. Deze richtlijnen zijn vastgesteld en goedgekeurd door het Managementteam en IT-Manager en worden gecommuniceerd naar de relevante interne en externe partijen (b.v. personeel, consultants, klanten, etc.).
- INTERCARE NV evalueert deze beveiligingsrichtlijnen periodiek om er voor te zorgen dat ze relevant en juist zijn en blijven, en dat de richtlijnen effectief zijn.

Organisatie informatieveiligheid

- INTERCARE NV heeft intern verantwoordelijkheden toegewezen op het gebied van informatieveiligheid
- Het Managementteam en IT-Manager van INTERCARE NV is betrokken bij informatieveiligheid.

- Binnen INTERCARE NV draagt men, rekening houdend met de omvang van de organisatie en beschikbare capaciteit, zorg voor de nodige functiescheiding waarbij conflicterende functies of verantwoordelijkheden niet toegewezen worden aan dezelfde persoon.
- Bij de uitvoering van projecten, ongeacht het type van project, is informatieveiligheid een vast onderdeel van het project.

Medewerkers gerelateerde veiligheid

- Medewerkers beheren hun gebruikersmateriaal als een “goed huisvader/moeder”, installeren geen illegale content op het beschikbaar gemaakte materiaal en zullen geen materiaal ontvreemden
- Medewerkers worden geacht gegevens zo min mogelijk lokaal op te slaan, en waar nodig lokaal opgeslagen gegevens z.s.m. gecentraliseerd opslaan.
- Medewerkers worden periodiek gesensibiliseerd.

Mobiel & teleworking

- INTERCARE NV heeft een aparte richtlijn opgesteld m.b.t. het overdragen van informatie en deze is opgenomen als IT Policy in het Arbeidsreglement. Hierin is onder meer aandacht voor het gebruik van mobiele toestellen en de voorwaarden waaronder INTERCARE NV informatie verwerkt kan worden op deze toestellen.
- Telewerken is binnen INTERCARE NV gangbaar en hiervoor zijn dezelfde regels van toepassing als bij intern gebruik.

Toegangsbeheer

- Medewerkers gebruiken enkel hun eigen accounts en houden de toegang tot deze accounts (b.v. wachtwoorden) strikt persoonlijk
- Wachtwoorden dienen voldoende complexiteit te hebben en strikt vertrouwelijk te worden behandeld, waar mogelijk wordt dit afgedwongen in de applicatie
- Medewerkers dienen zelf proactief te melden wanneer zij rechten hebben die buiten hun functionele behoeften gaan
- In functie van de vertrouwelijkheid of gevoeligheid van de gegevens worden gepaste toegangsmaatregelen genomen zoals multifactor-authentication
- Periodiek worden de toegangsrechten van gebruikers nagekeken.

Fysieke beveiliging

- Medewerkers laten geen IT materiaal onbeheerd achter (clear screen policy)
- Medewerkers laten geen gevoelige gegevens (persoonsgegevens, gevoelige bedrijfsinformatie, e.d.m.) onbeheerd achter (clean desk policy)
- Toegang tot beveiligde omgevingen (HR dossiers, server room, etc.) is afgeschermd door middel van fysieke beveiliging (badge, sleutel, etc)

Onderhoud en ontwikkeling

- Alvorens wijzigingen aan te brengen aan de configuratie van kritische systemen zal de impact bekeken worden om zo de kans op uitval tot een minimum te beperken
- Voor kritische systemen zijn garantieuitbreidingen of –waarborgen voorzien (carepacks, SLA afspraken, e.d.m.)

Leveranciers

- Toegang van leveranciers tot INTERCARE NV informatie of informatieverwerkende systemen zal beperkt zijn tot hetgeen de leverancier nodig heeft voor de invulling van het contract of de gemaakte afspraken.
- INTERCARE NV beschikt over een vaste voorwaarden waaraan een leverancier moet voldoen alvorens toegang wordt verleend tot informatie of informatieverwerkende systemen van INTERCARE NV, bijvoorbeeld een verwerkersovereenkomst.
- Afspraken rond veilige toegang en verwerking van informatie of informatieverwerkende systemen van INTERCARE NV door de leverancier worden vastgelegd.

Incidenten beheer

- Periodiek worden veiligheidscincidenten geëvalueerd om te kijken welke lessen geleerd kunnen worden of verbeteracties moeten worden ingezet
- Inbreuken op de beveiliging worden geregistreerd in een intern register, en worden waar noodzakelijk gemeld aan de Gegevensbeschermingsautoriteit en betrokkenen

Continuiteit

- Backups worden periodiek getest om vast te stellen dat ze betrouwbaar werken • Minstens 2 personen op de hoogte brengen van alle taken / procedures.
- Betere documentatie van taken die zich bij 1 persoon bevinden.

6.2.2 Technische maatregelen

ISO hoofdstukken 8, 9, 10, 11 (deels, badge systemen, access control fysieke systemen), 12, 13, 14, 16, 17

Operationele IT

- Updates en patches worden zo snel als mogelijk (b.v. na eventuele testen) geïnstalleerd, zowel op applicatie niveau als besturingssystemen
- INTERCARE NV zal ook voorzien in de juiste endpoint bescherming
- Toegang tot, en gebruik van, administrator toegangen wordt beperkt tot het noodzakelijke
- Geprivilegieerde toegangen zijn strikt vertrouwelijk en worden niet gedeeld met anderen
- INTERCARE NV heeft voldoende access control via gebruikers accounts, niet voldoende logging in bepaalde toepassingen is een risico dat we accepteren

Ontwikkeling en onderhoud

- INTERCARE NV controleert binnen projecten (zowel interne als externe) rond informatiesystemen of voldaan is aan de minimale vereisten rond informatieveiligheid zoals bepaald door het Managementteam en IT-Manager van INTERCARE NV. Het kan hierbij zowel gaan om de aanschaf van nieuwe hardware, de aanschaf of ontwikkeling van software, etc.
- Wanneer nodig geacht door het Managementteam en IT-Manager zal INTERCARE NV voor nieuwe systemen of software een onafhankelijke review laten uitvoeren van de gebruikte systemen of software, zoals een kwetsbaarheidsanalyse of penetratietest.