Beleid voor gegevensbescherming en informatieveiligheid

Goedgekeurd door de raad van bestuur van 24 april 2019

Inhoud

1. Belang van informatieveiligheid en gegevensbescherming

ADO Icarus organiseert en verstrekt ondersteuning aan personen met een handicap zodat deze personen op een kwaliteitsvolle manier geïntegreerd en zelfstandig kunnen wonen en leven. Bij het uitvoeren van deze opdracht gaat ADO Icarus uit van drie kernwaarden, namelijk: autonomie, respect en privacy. Bij het bieden van ondersteuning in de thuissituatie dringen werknemers van ADO Icarus onvermijdelijk binnen in het dagelijkse leven van de budgethouder en zijn eventueel gezin. Daarnaast organiseert ADO Icarus de werking van een lokaal dienstencentrum. Deze dienstverlening bestaat uit een waaier van activiteiten en ondersteuning waarbij beroep gedaan wordt op lokale vrijwilligers die onder coördinatie van een centrumverantwoordelijke mee vorm geven aan de werking.

De **werknemers** van ADO Icarus zijn gebonden aan het beroepsgeheim en het respect voor de privacy van de budgethouders. Alle informatie over het privéleven van de budgethouders wordt daarom strikt geheim gehouden.

Ook van de **budgethouders** wordt verwacht dat zij het nodige respect opbrengen voor de privacy van zowel de werknemers als van andere budgethouders.

De **vrijwilligers** zijn gebonden aan een afsprakennota waarmee zij zich akkoord dienen te verklaren alvorens hun engagement te kunnen opnemen. In deze afsprakennota zijn er bepaalde afspraken opgenomen m.b.t. de privacy van de bezoekers.

Ook van de **bezoekers** van het lokale dienstencentrum wordt verwacht dat zij het nodige respect opbrengen van zowel de vrijwilligers, de werknemers als voor andere bezoekers.

Ook **ADO Icarus** levert haar diensten met aandacht voor de bescherming van persoonsgegevens van elke betrokkene: cliënten, medewerkers en derden.

We staan er als ADO Icarus voor garant dat het verzamelen en verwerken van de gegevens van de betrokkenen gebeurt met de grootst mogelijke zorgvuldigheid, op een professionele manier, en met aandacht voor het beschermen van de persoonlijke levenssfeer van de betrokkene. We streven continu naar verbetering, met als doel een veilige informatieomgeving te creëren, en alle persoonsgegevens te beschermen conform de Europese Algemene Verordening voor Gegevensbescherming.

In het bijzonder willen we:

- de persoonsgegevens beschermen tegen **verlies**, zorgen dat de gegevens beschikbaar blijven voor de goede werking van de organisatie
- de persoonsgegevens beschermen tegen **lekken**, zorgen dat ze niet in verkeerde handen terecht komen;
- de persoonsgegevens beschermen tegen **fouten**, zorgen dat de gegevens correct zijn (niet verouderd of onvolledig)
- zorgen dat de persoonsgegevens niet ingekeken kunnen worden door personen die hiertoe niet gemachtigd zijn
- zorgen dat **de verwerkingen** in lijn liggen met de regelgeving, richtlijnen en normen
- via **logging** kunnen nagaan wie de gegevens inkeek, wijzigde of verwijderde
- ervoor zorgen dat de gegevens door de verwerker **toegankelijk** zijn op het moment van de verwerking

De directie wil beroep doen op iedereen die betrokken is bij het verwerken van persoonsgegevens om samen, vanuit een gemeenschappelijke visie én vanuit onze gezamenlijke wil om kwaliteitsvolle dienstverlening aan te bieden, de verwerking van de persoonsgegevens van onze cliënten/gebruikers en medewerkers correct te laten verlopen.

Dit beleid dient als norm voor het verwerken van persoonsgegevens. Het is een leidraad voor alle verwerkingsprocessen en biedt een referentienorm voor audit en controle. Het biedt elke cliënt/gebruiker, medewerker en externe een inzage in het veiligheidsbeleid en de manier waarop we omgaan met gevoelige persoonsgegevens. Deze tekst draagt ook bij aan de bewustwording omtrent informatieveiligheid.

Deze beleidstekst voor gegevensbescherming en informatieveiligheidsbeleid is opgesteld voor iedereen die een beleidsfunctie heeft binnen ADO Icarus en kan gebruikt worden bij het ontwerpen van procedures en richtlijnen voor medewerkers en externen. De relevante onderdelen worden verwerkt in overeenkomsten met personeel en leveranciers.

2. Het toepassingsgebied van het beleid voor gegevensbescherming en informatieveiligheid

Het beleid Gegevensbescherming en informatieveiligheid is van toepassing op de verwerking van persoonsgegevens waarbij ADO Icarus als verwerkingsverantwoordelijke (al dan niet samen met anderen) of verwerker wordt aangeduid.

2.1 Materieel toepassingsgebied

Het beleid is van toepassing op alle persoonsgegevens die ADO Icarus verwerkt. We verstaan hieronder niet alleen de gegevens van onze cliënten/gebruikers, maar ook bijvoorbeeld van medewerkers, al dan niet in dienstverband, van bezoekers, sollicitanten, kandidaat-cliënten… Dus van elke geïdentificeerde of identificeerbare persoon.

Het gegevensbeschermingsbeleid is van toepassing op alle verwerkingsdoelen. Zowel gegevens die worden verwerkt voor de dienstverlening van ADO Icarus voor cliënten, wetenschappelijk onderzoek, rapporteringsdoeleinden, gemachtigde extramurale gegevensstromen (vb. naar het VAPH), administratie van medewerkers, financiële gegevens, persoonsgegevens die verwerkt worden in het kader van kwaliteitscontroles of risicobeoordelingen, behoren tot de scope van dit beleid.

2.2 Personeel toepassingsgebied

Deze beleidstekst is geschreven voor iedereen die in opdracht van ADO Icarus persoonsgegevens verwerkt, zoals de directie, de personeelsleden, maar ook elke (externe) medewerker of leverancier. Deze tekst wordt via verschillende kanalen, zoals de website en het kwaliteitshandboek, uitgedragen.

De functionaris voor de gegevensbescherming (DPO) waakt erover dat de principes van dit gegevensbeschermingsbeleid worden toegepast in alle samenwerkingsverbanden die ADO Icarus opzet.

3. Organisatie van gegevensbescherming en informatieveiligheid

3.1 Bevoegdheid en verantwoordelijke uitvoerder

Het dagelijks bestuur is verantwoordelijk voor het formuleren van de beleidsprincipes en fungeert als formeel beslissingsplatform voor informatieveiligheid voor de naleving ervan binnen ADO Icarus. De financieel en administratief directeur is belast met de implementatie en de uitvoering ervan.

3.2 Plaats

Het beleidshandboek wordt geïntegreerd in het kwaliteitsmanagement van ADO Icarus, onder het toeziend oog van de financieel en administratief directeur en in nauwe samenwerking met de veiligheidsconsulent en DPO.

3.3 Toezicht en Advies

Zowel het Vlaams decreet van 15 mei 2009 betreffende veiligheidsconsulenten als de Europese Algemene verordening gegevensbescherming voorzien in de oprichting van een functie die toezicht houdt op en advies levert betreffende de informatieveiligheid en de status van gegevensbescherming binnen een organisatie.

3.3.1 De informatieveiligheidsconsulent

De inhoudelijke opvolging van het informatieveiligheidsbeleid ligt bij de informatieveiligheidsconsulent (IVC). Hij voert deze taak uit volgens de bepalingen in het Vlaams decreet van 15 mei 2009 betreffende veiligheidsconsulenten. De veiligheidsconsulent rapporteert aan de financieel en administratief directeur van ADO Icarus en is meer in het bijzonder belast met:

- Adviezen en aanbevelingen voorleggen aan het financieel en administratief directeur.
- Opdrachten uitvoeren op vraag van de financieel en administratief directeur en het dagelijks bestuur).
- Bevorderen van de bewustwording van alle actoren binnen ADO Icarus.
- Toezien op de naleving van het veiligheidsbeleid binnen ADO Icarus.
- Documenteren van het veiligheidsbeleid, in overleg met de financieel en administratief directeur.
- Opstellen van het veiligheidsplan voor een periode van 3 jaar en waken over de uitvoering ervan.
- In samenwerking met de financieel en administratief directeur: opstellen van een jaarverslag met de vorderingen van het veiligheidsplan en dit voorleggen aan het dagelijks bestuur en de raad van bestuur.
- Registreren van incidenten & overtredingen en deze overmaken, samen met een advies, aan het dagelijks bestuur.

3.3.2 De functionaris voor gegevensbescherming (DPO)

De DPO verleent bijstand, verstrekt informatie over en kijkt toe op de verplichtingen van ADO Icarus ten aanzien van de verordening. Minimaal behandelt de DPO de verplichtingen aangaande:

- Bijstand en advies verlenen inzake
    - De principes van het verwerken van persoonsgegevens en in het bijzonder gevoelige persoonsgegevens
    - De rechten van de betrokkene en in het bijzonder de rechten van de cliënt
    - De gegevensbescherming bij ontwerp en standaardvoorzieningen, het register voor de verwerkingsactiviteiten
    - De informatieveiligheid

    - De elementen die horen bij het afhandelen en melden van inbreuken
- Toekijken op de naleving van de verordening
    - De correcte toepassing van onderhavig beleid voor gegevensbescherming
    - De correcte toepassing van alle Europese, Federale en Vlaamse regelgeving over het verwerken van persoonsgegevens
    - Toekijken of eenieder de in dit beleidsdocument omschreven verantwoordelijkheid opneemt
    - Toekijken op het bewustzijn inzake gegevensbescherming bij de stakeholders
    - Toekijken en kennisnemen van de inhoud van andere audits en controles die handelen over (of elementen bevatten van) gegevensbescherming
- Advies verstrekken over gegevensbeschermingseffectenbeoordelingen (DPIA: Data Protection Impact Assessment)
- Contactpunt zijn voor de Gegevensbeschermingsautoriteit en hiermee samen werken
- Coördineren van incidentmeldingen in verband met gegevensbescherming.

3.3.2 De medewerker

Iedereen (intern of extern) die persoonsgegevens verwerkt (bijvoorbeeld inkijkt, registreert, wijzigt, verwijdert, …), doet dit volgens de principes uit dit beleid. De medewerker verwerkt gegevens in overeenstemming met de discretieplicht, en conform volgende principes: hij/zij

- Is verantwoordelijk voor de gegevens van cliënten en/of medewerkers 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.
- Respecteert het beroepsgeheim (artikel 458 van het Strafwetboek) en de discretieplicht zoals beschreven in het arbeidsreglement.

3.3.3 De leidinggevende

Bijkomend zien de leidinggevenden toe op de goede uitvoering van de veiligheidsbepalingen : zij

- volgen de veiligheidsrichtlijnen op en informeren de medewerkers hierover (vb. personaliseren van gekregen paswoorden, na gebruik van een dossier afmelden, informatie op papier niet laten liggen,…).
- zorgen voor een veiligheidscultuur en onderhouden deze, brengen deze regelmatig onder de aandacht op individueel en collectief overleg.
- ondersteunen controleactiviteiten, (vb. door het controleren van logging).

3.3.4 IT-medewerker en beheerder van het datasysteem

De IT-medewerker en de beheerder van het datasysteem zijn, in toevoeging van de verantwoordelijkheden voor medewerkers, verantwoordelijk voor:

- Implementatie van de technische maatregelen
- Implementatie van de veiligheidsvoorzieningen in lijn met dit beleid.
- Melden van veiligheidsproblemen die ontstaan voor, tijdens of na de implementatie van IT-middelen aan de veiligheidsconsulent
- Fungeren als expert. Vanuit deze rol nemen zij deel aan de identificatie zowel als aan de remediëring van de informatieveiligheidsrisico's
- Naleven van de gedragscode.

3.3.5 ICT-leveranciers en -consultants

Een ICT-leverancier en –consultant heeft dezelfde verantwoordelijkheden als een ICT-medewerker. Bijkomend : hij/zij

- Wijst op eventuele veiligheidsrisico's van geleverde toepassingen (ook door derde partijen)
- Wijst op de op te nemen veiligheidstaken
- Streeft een transparant veiligheidsbeleid na door te communiceren over het eigen actuele veiligheidsniveau
- Geeft ondersteuning bij de afhandeling van veiligheidsincidenten.

4. Beleid voor gegevensbescherming

4.1 Algemene doelstelling: rechtmatigheid

Met de Algemene Verordening Gegevensbescherming als gids, streeft ADO Icarus de beleidsdoelstelling 'rechtmatigheid' na. Voor alle verwerkingen van persoonsgegevens waarvoor ADO Icarus verantwoordelijk is, wordt de rechtmatigheid beheerd en afgetoetst. ADO Icarus gebruikt hierbij de algemene voorwaarden die in de Algemene Verordening Gegevensbescherming zijn opgenomen.

Voor de verwerking van gevoelige gegevens gaat ADO Icarus daarenboven na of de door de wetgever specifieke opgesomde voorwaarden van toepassing zijn, zoals het verstrekken van de diensten, voor de onderbouwing en uitoefening van een rechtsvordering, voor verplichtingen in het kader van het arbeidsrecht of socialezekerheidsrecht, …. In vooropgesteld geval zal de verwerking enkel plaatsvinden onder verantwoordelijkheid van het bestuur en de directie van ADO Icarus en onder de naleving van het beroepsgeheim.

Naast de in de Algemene Verordening Gegevensbescherming opgesomde rechtmatigheidsregels, leven we ook de geldende Vlaamse, Federale en Europese regels na over het verwerken van persoonsgegevens.

ADO Icarus monitort het bestaan en de evoluties van de in de sector geldende gedragscodes en past deze toe volgens de regels die deze voorschrijven. Dit betekent dat ADO Icarus de intentie uitspreekt om zich aan te sluiten bij alle toepasselijke gedragscodes.

4.2 Behoorlijk en transparant

ADO Icarus volgt een 'fair use' principe in de omgang met persoonsgegevens, waarbij we behoorlijke gegevensverwerking nastreven, eerlijk en transparant naar alle betrokkenen en de toezichthouder.

4.2.1 Gerechtvaardigd doel

We verwerken persoonsgegevens voor welbepaalde en uitdrukkelijk omschreven doeleinden, die we duidelijk communiceren naar de betrokkene (via de privacyverklaring, de beleidsnota, het arbeidsreglement en het charter van collectieve rechten en plichten) en opnemen in een register van verwerkingsactiviteiten. We waken erover dat deze doelen steeds gerechtvaardigd zijn, in lijn met onze juridische eigenheid, onze visie en missie.

Wanneer deze persoonsgegevens verder verwerkt worden voor andere doeleinden dan waken we erover dat deze doelen verenigbaar zijn.

Voor de verdere verwerking in het kader van wetenschappelijk of historisch onderzoek of statistische doeleinden, waarborgen we de rechten en vrijheden van de betrokkene. De voorziene waarborgen zorgen ervoor dat er technische en organisatorische maatregelen zijn getroffen om de minimale gegevensverwerking te garanderen, zoals opgelegd door de regelgever. We trachten bij deze verwerkingen de identificatiegegevens maximaal te verwijderen (anonimiseren). Indien dit niet mogelijk blijkt om het beoogde doel te verwezenlijken, passen we de regels inzake pseudonimisering[1] toe, tenzij deze het beoogde doel onmogelijk maken.

[1] *Pseudonimisering is de loskoppeling van de persoonsgegevens van de persoon. Er zijn aanvullende gegevens nodig die afzonderlijk bewaard en afgeschermd worden om de persoonsgegevens aan een persoon te linken.*

4.2.2 Minimale gegevensverwerking

Bij het verwerken van persoonsgegevens waken we erover dat de persoonsgegevens die we verwerken toereikend, ter zake dienend en noodzakelijk zijn binnen het beoogde doel.

4.2.3 De juistheid

ADO Icarus bewaakt zorgvuldig de correctheid van de verwerkte persoonsgegevens. Dit betekent in essentie dat persoonsgegevens volledig en juist zijn rekening houdende met het beoogde verwerkingsdoel. Wanneer de kans bestaat dat de persoonsgegevens niet actueel of fout zijn zullen we extra inspanningen leveren om de gegevens te corrigeren of zo nodig te wissen. We gebruiken hierbij alle mogelijke verificatiebronnen die ons ter beschikking worden gesteld. Wanneer de correctheid van gegevens door de betrokkene worden betwist, nemen we weloverwogen beslissingen, in overeenstemming met het toepasselijk recht, met het oog op de juistheid van de gegevens en de vrijwaring van het recht op een kwalitatief dossier.

4.2.4 De opslagbeperking

ADO Icarus bewaart gegevens niet langer dan noodzakelijk. De noodzakelijkheid is afgetoetst tegenover wettelijke verplichtingen en het beoogde verwerkingsdoel. Wanneer persoonsgegevens worden gearchiveerd respecteren we de wettelijke en administratieve voorschriften die hierop van toepassing zijn.

4.2.5 De integriteit en vertrouwelijkheid

ADO Icarus neemt de passende technische en organisatorische maatregelen met het oog op een passende beveiliging van de persoonsgegevens. Op die manier beschermen we de persoonsgegevens onder meer tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging. Om deze beleidsdoelstelling te verwezenlijken heeft ADO Icarus een veiligheidsbeleid uitgewerkt.

4.2.6 De Verantwoordingsplicht

Onder de Verordening Gegevensbescherming is de plicht ingevoegd voor de verwerkingsverantwoordelijke om te kunnen aantonen ten aanzien van de Gegevensbeschermingsautoriteit dat hij de basisprincipes voor gegevensverwerking en de overige voorwaarden van het regelgevend kader naleeft.

Deze verantwoordingsplicht wordt bewaakt door interne audit en controle en is uitvoerbaar volgens de wettelijk geldende principes.

4.3 Verplichtingen als verwerkingsverantwoordelijke

Om de beleidsdoelstellingen te bereiken zijn een aantal taken vastgelegd. Deze taken zijn in lijn met alle wettelijke verplichtingen die ADO Icarus dient na te leven ter ondersteuning van de verantwoordingsplicht. Waar nodig zijn deze beginselen aangevuld met de beginselen voortvloeiend uit de algemene zorgvuldigheidsnorm (art. 1382 BW).

De verantwoordelijkheid voor het uitvoeren van deze taken berust bij de verwerkingsverantwoordelijke (= ADO Icarus). De delegatie van de taken en de concrete uitvoering daarvan, evenals de controletaken die hierop van toepassing zijn, zijn opgenomen in deze tekst (zie verder).

In het kader van onze verantwoordingsplicht worden alle opgesomde taken uitgevoerd in volledige transparantie voor de Gegevensbeschermingsautoriteit. Dit betekent dat de beoogde taken dienen te worden gedocumenteerd. Deze documentatie omvat zowel de koppeling met de beleidsdoelstellingen,

de uit te voeren taken, de bijhorende verantwoordelijkheden en de controlemaatregelen die hierop van toepassing zijn.

4.3.1 Toezicht op de uitvoering van taken onder verantwoordelijkheid van ADO Icarus

ADO Icarus houdt toezicht op de uitvoering van deeltaken die worden toevertrouwd aan een (externe) verwerker of intern aan een personeelslid van ADO Icarus.

Intern - personeelsleden
ADO Icarus dient te zorgen voor duidelijke instructies en richtlijnen in overeenstemming met de verantwoordelijkheden die medewerkers van ADO Icarus in het kader van verwerkingen hebben. Deze instructies worden via functiebeschrijvingen (uitvoering van de taken), procedures, bewustwordings-sessies, en opleidingen gecommuniceerd. De naleving van de verplichtingen wordt afgedwongen aan de hand van het arbeidsreglement, de leidraad voor de verschillende personeelscategorieën en de policies.

Extern - verwerkers
Wanneer een verwerking namens ADO Icarus wordt verricht door een verwerker (extern), doet ADO Icarus enkel beroep op verwerkers die afdoende garanties bieden met betrekking tot het toepassen van passende technische en organisatorische maatregelen.

De gemaakte schriftelijke afspraken met een verwerker worden opgenomen in een verwerkersovereenkomst. De afspraken betreffen onder meer de opsomming van de specifieke taken van de verwerker in het verwerkingsproces, de te nemen veiligheidsmaatregelen en de plicht tot bijstand bij het uitvoeren van de op ADO Icarus rustende verplichtingen die in deze tekst zijn opgenomen.

ADO Icarus voert toezicht uit op deze contractuele bepalingen met een verwerker, onder meer door modaliteiten op te nemen in de verwerkersovereenkomst dat de mogelijkheid biedt controle en inspectietaken uit te voeren op informatie en systemen die persoonsgegevens verwerken waarvoor ADO Icarus verantwoordelijk is.

4.3.2. Het bijhouden van een register van verwerkingsactiviteiten

ADO Icarus beheert een register van alle activiteiten waarbij persoonsgegevens worden verwerkt. Het beheer omvat het opstellen, permanent bijwerken en de controlemaatregelen die hierop van toepassing zijn. Dit register geldt als instrument in het kader van de verantwoordingsplicht ten aanzien van de Gegevensbeschermingsautoriteit, maar is niet bestemd voor de betrokkenen noch voor het publiek. Het register wordt bijgehouden in elektronische vorm.

Telkens voorafgaand aan het inrichten van een nieuwe of gewijzigde verwerkingsactiviteit wordt het verwerkingsregister bijgewerkt.

De inhoud van het register wordt vastgelegd door de wettelijke bepalingen die hierop van toepassing zijn, aangevuld met elementen die andere verplichtingen ondersteunen, zoals de controle van doelbinding, het nagaan van een geldige toelaatbaarheidsgrond bij de verwerking, het nazicht van de maatregelen met het oog op minimale gegevensverwerking, gegevensbescherming bij ontwerp of de noodzaak om een gegevensbeschermingseffectenbeoordeling uit te voeren.

4.3.3 Maatregelen ter beveiliging van de verwerking

Persoonsgegevens mogen slechts verwerkt worden indien er passende technische en organisatorische maatregelen zijn genomen voor het waarborgen van de beschikbaarheid, de integriteit en de vertrouwelijkheid van de verwerkte persoonsgegevens.

ADO Icarus voorziet een informatieveiligheidsbeleid, waarin de verschillende verantwoordelijkheden en maatregelen worden vastgesteld. Het toezicht op informatieveiligheid en de relatie met gegevensbescherming wordt verder in deze beleidstekst opgenomen.

4.3.4 Melden van inbreuken in verband met verwerking van persoonsgegevens

Uit de Verordening Gegevensbescherming volgt tevens een plicht voor ADO Icarus om een incidentmeldingssysteem voor de interne registratie van inbreuken die betrekking hebben op het verwerken van persoonsgegevens.

ADO Icarus voorziet in de nodige procedures voor een adequate beveiliging van persoonsgegevens en dit zowel op proactief als op reactief vlak.

4.3.5 Het uitvoeren van een gegevensbeschermingseffectenbeoordeling (DPIA of Data Protection Impact Assessment)

ADO Icarus stelt een lijst op van criteria die kunnen worden gebruikt om te identificeren of een voorgenomen verwerking een verhoogd risico inhoudt voor de betrokkene en onderhoudt deze.

Wanneer op basis van de criteria blijkt dat de voorgenomen verwerking een hoog risico inhoudt, wordt een gegevensbeschermingseffectenbeoordeling uitgevoerd voorafgaand aan de verwerking. Op basis van de beoordeling worden de nodige maatregelen genomen om het risico op een inbreuk tijdens de verwerking zo veel mogelijk te beperken. Indien de risico's ondanks maatregelen niet afdoende kunnen worden ingeperkt, moet de verwerkingsverantwoordelijke de Gegevensbeschermingsautoriteit consulteren.

4.3.6 Aanstellen van een functionaris voor de gegevensbescherming (DPO)

Op basis van de criteria vastgelegd in de Algemene Verordening Gegevensbescherming heeft ADO Icarus een DPO aangesteld.
De DPO geeft advies over en houdt toezicht op de verwerkingsprocessen van alle persoonsgegevens en voert deze functie onafhankelijk uit. Hij mag dus niet gebonden zijn door inhoudelijke instructies. ADO Icarus betrekt de DPO vanaf het begin bij alle gelegenheden die raken aan de bescherming van persoonsgegevens (o.a. tijdig inlichten, uitnodigen op vergaderingen, …). Tevens verleent ADO Icarus aan de DPO toegang tot de nodige persoonsgegevens, de verwerkingsactiviteiten.

ADO Icarus waakt over de expertise van de DPO bij het uitvoeren van diens taken.

4.3.7 Naleving van de rechten van de betrokkene

ADO Icarus voorziet in de nodige processen die ervoor zorgen dat de betrokkene wordt geïnformeerd over de verwerking. De verstrekte informatie omvat alle wettelijk opgelegde elementen, waaronder: de functionaris voor de gegevensverwerking, het verwerkingsdoel en de ontvangers van de gegevens.

Voor cliënten gebeurt dit via de privacyverklaring, de beleidsnota en het charter van collectieve rechten en plichten. Voor personeel gebeurt dit van de privacyverklaring, de beleidsnota en het arbeidsreglement.

De processen die uitvoering geven aan de rechten van de betrokkene worden gedocumenteerd. Deze processen houden rekening met wettelijke beperkingen.

5. Beleid voor informatieveiligheid

Informatieveiligheid omvat het geheel van technische en organisatorische maatregelen die ervoor zorgen dat een vooropgesteld veiligheidsniveau wordt nagestreefd. Hierbij staat de integriteit, de beschikbaarheid en de vertrouwelijkheid van de gegevens centraal. Deze maatregelen kunnen zowel administratief, technisch, beheersmatig als juridisch van aard zijn en omvatten het beleid, procedures, richtlijnen, werkwijzen en organisatiestructuren.

5.1 Identiteitsbeheer

Een personeelslid heeft, afhankelijk van zijn functie, al dan niet een digitale identiteit (= gebruikersaccount). ADO Icarus zorgt voor de nodige processen dat deze digitale identiteit betrouwbaar is om handelingen uit te voeren in naam van de organisatie. De identiteit dient te worden beheerd gedurende de ganse levenscyclus.

De digitale identiteit is de gebruikersnaam waarmee een personeelslid, die gebruik maakt van een ICT-middel of -toepassing, zich identificeert. Hiermee kan de gebruiker inloggen op zijn PC/laptop en toegang krijgen tot het netwerk, de applicaties en IT-diensten van ADO Icarus.

Ook de bestuursleden van ADO Icarus hebben een digitale identiteit om via intranet toegang te hebben tot documenten zoals verslagen en nota's van de bestuursvergaderingen.

5.2 Wachtwoordenbeleid

Voor de personeelsleden met een digitale identiteit en voor bestuursleden is er een 'wachtwoordenbeleid' opgezet om ervoor te zorgen dat de toegang tot applicaties en IT-diensten sterk beveiligd is. Het is van belang om:

- een sterk wachtwoordenbeleid op te zetten om het inlogproces en de inlogprocedures te beheren
- personeelsleden het belang van sterke wachtwoorden bij te brengen.

5.3 Toegangsbeheer

ADO Icarus zorgt voor de organisatorische maatregelen en procedures die ervoor zorgen dat de toegang tot informatie gecontroleerd is en afgestemd op het "need to know" principe. De toegangsrechten tot gevoelige gegevens zijn adequaat ingesteld.

5.4 Kennisgeving

In het kader van de verwerking van persoonsgegevens brengt ADO Icarus de betrokkene op de hoogte van zijn rechten en de procedures om deze te doen gelden.

Voor de inwerkingtreding van de GDPR-wetgeving werd door de organisatie een beleidsnota inzake informatieveiligheid en gegevensbescherming opgesteld. Deze beleidsnota werd door de raad van bestuur goedgekeurd. Verder werd een meer bevattelijke nota opgesteld, genaamd de 'privacyverklaring', en op de website van ADO Icarus geplaatst. Via de privacyverklaring kan tevens de uitgebreide beleidsnota worden geraadpleegd.

Aangezien privacy in het algemeen één van de kernwaarden is van ADO Icarus, komt de aandacht hiervoor regelmatig terug tijdens de dagelijkse werking, vergaderingen en vormingen.

5.5 Logging

Gezien ADO Icarus gevoelige persoonsgegevens verwerkt, is het belangrijk om te kunnen rapporteren wie op welke moment bepaalde persoonsgegevens heeft geraadpleegd, gewijzigd, verwijderd, ingegeven of aangepast. Het is hierbij van belang dat de veiligheidsconsulent weet waar deze logging wordt bewaard en hoe deze kan worden geraadpleegd. Daarenboven dient deze logging betrouwbaar te zijn: bij het eventueel opsporen van misbruik moet kunnen worden aangetoond dat de logging consistente gegevens bewaart over de handelingen door de eindgebruiker. Tot slot is het belangrijk dat de organisatie waarborgen treft die ervoor zorgen dat de cliënt een accuraat beeld krijgt over wie welke gegevens heeft geraadpleegd.

5.6 Bewustwording

Elke medewerker van ADO Icarus dient zich bewust te zijn van de impact van (verkeerde) handelingen met persoonsgegevens. Bovendien is het belangrijk dat medewerkers weten welke de veiligheidsvoorschriften zijn bij het verwerken van persoonsgegevens.

- Afspraken, rechten en plichten zijn opgenomen in het arbeidsreglement. Deze worden bijkomend aangevuld door leidraden voor de verschillende personeelscategorieën. Ook worden policies gehanteerd (wachtwoordenbeleid, internet en e-mail policy, ..)
- Minstens vier maal per jaar wordt een actie ondernomen om gegevensbescherming en informatieveiligheid onder de aandacht te brengen en te houden. Dit kan via diverse kanalen. Dit gebeurt door de DPO in samenwerking met de communicatieverantwoordelijke.

5.7 Verwerkers

ADO Icarus dwingt informatieveiligheid niet alleen af bij de eigen medewerkers. Ook derde partijen zijn onderhevig aan de regels rond het correct verwerken van persoonsgegevens. Deze doelgroep is in het vakjargon een verwerker. Zij dienen onderworpen te worden aan de noodzakelijke contractuele afspraken omtrent gegevensverwerking. De afspraken bevatten bepalingen rond wat er met persoonsgegevens wel en niet mag gebeuren en welke veiligheidsmaatregelen hierbij van toepassing zijn.

5.8 Faciliteer veilige informatieopslag en uitwisseling

Om deel te nemen aan het uitwisselen van persoonsgegevens met andere actoren die actief zijn in de hulpverlening, voert ADO Icarus een beleid waarbij adequate veiligheidscontrolepunten gelden, afhankelijk van de classificatie van de informatie.