GEDRAGSREGELS IPB KINDANTE

1 Inleiding

Informatie en ICT zijn noodzakelijk in de primaire dienstverlening en in de ondersteunende bedrijfsprocessen van Stichting Kindante. Omdat we met persoonsgegevens (van kinderen, ouders en medewerkers) werken, is de privacywetgeving daarop van toepassing.

De informatie en ICT van Stichting Kindante worden blootgesteld aan een groot aantal bedreigingen, al dan niet opzettelijk van aard. Alle informatie die we bewaren en verwerken kan worden bedreigd door een aanval, een vergissing, de natuur (bijv. overstroming of brand), et cetera. Het niet beschikbaar zijn van ICT, incorrecte administraties en het uitlekken van gegevens leidt tot inbreuken op het geven van onze dienstverlening en het vertrouwen in onze organisatie. Om dit structureel op te pakken is het noodzakelijk dat we duidelijk maken waar het om gaat, een doel stellen en de manier waarop we dit doel willen bereiken.

2 Informatiebeveiliging en privacy

2.1 Informatiebeveiliging

Informatiebeveiliging is een proces voor het beschermen van Stichting Kindante tegen risico's en bedreigingen met betrekking tot informatie en ICT. Het richt zich op drie aspecten:

- Beschikbaarheid; informatie en aanverwante bedrijfsmiddelen zijn toegankelijk wanneer nodig;
- Integriteit; informatie en verwerkingsmethoden bevatten zo min mogelijk fouten;
- Vertrouwelijkheid; informatie is alleen toegankelijk voor diegenen die daartoe bevoegd zijn. Dit wordt ook wel de BIV-classificatie genoemd.

2.2 Privacy

Privacy gaat om de bescherming van persoonsgegevens conform de huidige wet- en regelgeving. Door het goed toepassen van informatiebeveiliging kan aan deze wetgeving worden voldaan.
Daarom zien we het als één onderwerp: **informatiebeveiliging en privacy (IBP).**

3.1 Vuistregels privacy

Stichting Kindante hanteert vijf vuistregels voor privacy:

1. **Doelbepaling en doelbinding**: persoonsgegevens worden alleen gebruikt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking vastgesteld. Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doelen waarvoor ze zijn verkregen.
2. **Grondslag**: verwerking van Persoonsgegevens is gebaseerd op een van de wettelijke grondslagen: toestemming, overeenkomst, de wet, publiekrechtelijke taak, vitaal belang van de betrokkene, of gerechtvaardigd belang.
3. **Dataminimalisatie**: bij de verwerking van Persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt: het type persoonsgegevens moet redelijkerwijs nodig zijn om het doel te bereiken; ze staan in verhouding tot het doel (= proportioneel). Het doel kan niet met minder, alternatieve of andere gegevens worden bereikt. Dit betekent ook dat data niet langer wordt bewaard dan noodzakelijk.

4. **Transparantie**: de organisatie legt aan betrokkenen (klanten en medewerkers) op transparante wijze verantwoording af over het gebruik van hun persoonsgegevens, alsmede over het gevoerde IBP-beleid. Deze informatievoorziening vindt ongevraagd plaats. Daarnaast hebben deze betrokkenen recht op verbetering, aanvulling, verwijdering of afscherming van hun Persoonsgegevens. Daarnaast kunnen betrokkenen zich verzetten tegen het gebruik van hun gegevens.
5. **Data-integriteit**: er zijn maatregelen getroffen om te waarborgen dat de te verwerken Persoonsgegevens juist en actueel zijn.

3.2 Ondersteunende privacy uitgangspunten

6. **Bij alle registraties op basis van toestemming** zal door Stichting Kindante aan de betrokkenen een eenduidige zogenaamde Opt-out procedure worden aangeboden. (een gegeven toestemming kan net zo gemakkelijk ingetrokken worden als dat ze gegeven werd)
7. **Voor nieuwe verwerkingen** van persoonsgegevens dient vooraf goedkeuring aan de directie te worden voorgelegd met onderbouwing en privacy-afweging door de privacy officer, waarbij speciale aandacht is vereist voor bijzondere of gevoelige persoonsgegevens.
8. **Voor verwerking van bestaande persoonsgegevens voor nieuwe resp. onderzoeks- doeleinden** zal eveneens vooraf goedkeuring aan de directie worden voorgelegd inclusief onderbouwing en privacy-afweging door de privacy officer.
9. **Persoonsgegevens moeten adequaat worden beveiligd** volgens algemeen en breed geaccepteerde beveiligingsnormen, zoals o.a. clear screan en cleandesk en sterke wachtwoorden.
10. **Bijzondere persoonsgegevens** zijn als zodanig gelabeld en worden met aanvullende technische en organisatorische maatregelen beveiligd (waaronder multi-factor authenticatie, logging en encryptie tijdens transport). Gevoelige persoonsgegevens uitsluitend transporteren volgens specifieke werkinstructie IBP.

4 Beveiligingsincidenten en datalekken

Alle verdachte incidenten worden gemeld bij leidinggevende en op privacy@kindante.nl
De afhandeling van deze incidenten volgt een gestructureerd proces, dat ook voorziet in de juiste stappen rondom de meldplicht datalekken.

5.1 Rol leidinggevenden

Binnen Stichting Kindante onderscheiden we de meerdere afdelingen. Informatiebeveiliging en privacy zijn een **lijnverantwoordelijkheid**: dat betekent dat de proceseigenaren de primaire verantwoordelijkheid dragen voor een goede informatiebeveiliging en privacy ten aanzien van (proces gebonden) informatie die op hun afdeling / eenheid wordt gebruikt dan wel gegenereerd. Dit omvat ook de keuze van maatregelen en de uitvoering en handhaving ervan.
Naleving van het informatiebeveiligingsbeleid is onderdeel van de integrale bedrijfsvoering. Iedere leidinggevende heeft op uitvoerend niveau de taak om:

- er voor te zorgen dat zijn medewerkers op de hoogte zijn van het privacy- en beveiligingsbeleid;
- toe te zien op de naleving van het IBP-beleid door de medewerkers, waarbij de leidinggevende een voorbeeldfunctie heeft;
- periodiek het onderwerp IBP onder de aandacht te brengen in werkoverleggen, beoordelingen etc.;
- als aanspreekpunt beschikbaar te zijn voor alle personeel gerelateerde IBP-onderwerpen.

5.2 Rol medewerkers

Veilig en betrouwbaar omgaan met informatie in het dagelijkse werk is **ieders professionele verantwoordelijkheid**. Medewerkers dragen actief bij aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie. Dit kan door meldingen te maken van security incidenten en het doen van verbetervoorstellen.

Bovendien gelden voor alle medewerkers onderstaande IPB-gedragsregels:

1. Deel of hergebruik geen wachtwoorden.
2. Vergrendel je scherm als je de werkplek verlaat.
3. Laat geen vertrouwelijke documenten achter op je werkplek.
4. Haal je documenten direct op uit de printer.
5. Laat geen smartphone, laptop, docs of USB onbeheerd in auto of vergaderzaal liggen.
6. Bedenk goed welke persoonsgegevens je deelt en met wie.
7. Let op wie er meeluistert als je zit te bellen.
8. Verzamel alleen beperkte persoonsgegevens volgens werkinstructie.
9. Meld beveiligingsincidenten per omgaande bij leidinggevende en privacy@kindante.nl
10. Bij uitgaande email check voor verzenden of je de juiste geadresseerde hebt geselecteerd.
11. Open geen e-mails, links of usb waarvan je de herkomst niet vertrouwt.
12. Gevoelige persoonsgegevens uitsluitend transporteren volgens werkinstructie (Crypt- share).