Privacy & Informatiebeveiliging beleid

Inhoud

Dit beleid is van toepassing op de volgende bedrijfseenheden;

- Stichting Kinderopvang Purmerend (SKOP)
- Kind en Ouders (K&O)
- Deel!
- Stichting Overblijf Purmerend (STOP)

Voor de duidelijkheid van dit document hierna te noemen SKOP.

1. Doel informatiebeveiliging

Het doel van informatiebeveiliging is er voor zorgen dat de informatie en gegevens van SKOP en haar klanten beschikbaar, integer en vertrouwelijk blijft. Informatie en gegevens zijn een belangrijke factor voor de realisatie van de strategie van SKOP maar ook voor Privacy van haar klanten.
Onder informatiebeveiliging wordt verstaan:
Het treffen en onderhouden van een samenhangend pakket maatregelen om de betrouwbaarheid (beschikbaarheid, integriteit en vertrouwelijkheid)van de informatievoorziening te waarborgen.

Betrouwbaarheid is de overkoepelende term voor *beschikbaarheid* (continuïteit, responstijd), *integriteit* (juistheid, volledigheid, tijdigheid, geoorloofdheid) en *vertrouwelijkheid* (exclusiviteit).
Informatievoorziening is het geheel van activiteiten met betrekking tot het verzamelen, vastleggen en verwerken van gegevens, gericht op het verstrekken van informatie ten behoeve van het besturen, het doen functioneren en het beheersen van een organisatie alsmede ten behoeve van het afleggen van verantwoording.

2. Doelgroep en context

Dit informatiebeveiligingsbeleid is bestemd voor iedereen die op enige wijze gebruik maakt van informatie en informatiesystemen van SKOP. Het beleid geldt zowel voor medewerkers als voor personen die anderszins verbonden zijn aan de organisatie of haar onderdelen (waaronder

bijvoorbeeld klanten, gedetacheerden, personeel dat wordt ingehuurd of personeel van een bedrijf waaraan werk is uitbesteed). Al deze groepen personen worden in dit kader gebruikers genoemd. Daarnaast geeft het beleid aan, hoe vorm wordt gegeven aan de beveiliging van informatie en informatiesystemen, dus ook bedrijfsmiddelen en interne processen, met speciale aandacht voor persoonsgegevens en het proces van privacy bewustwording. Beleid wordt door de directie kenbaar gemaakt aan alle gebruikers binnen de organisatie door bij de indiensttreding de aandacht op het bestaan en de inhoud te vestigen.
SKOP maakt gebruik van de (systemen) van derde partijen voor de verwerking van de persoonsgegevens. Met al deze partijen zijn verwerkersovereenkomsten gesloten, waarin afspraken over de privacybescherming en verantwoordelijkheden zijn vastgelegd.

3. Doelstellingen en scope

Zoals aangegeven is informatievoorziening een belangrijke factor en daarom van groot belang voor de organisatie en haar klanten. Gegeven deze prominente rol is het noodzakelijk dat er voldoende aandacht wordt geschonken aan het waarborgen van de betrouwbaarheid van de informatievoorziening ter ondersteuning van het besturen van de organisatie en de beheersing van bedrijfsprocessen.
De risico's met betrekking tot informatie en informatieverwerking waaraan SKOP is blootgesteld, dienen beperkt te worden tot een aanvaardbaar niveau. De manier waarop de organisatie met deze risico's wil omgaan heeft ertoe geleid dat zij heeft gekozen voor het risicoprofiel neutraal. Hierdoor staan de kosten voor de beveiligingsmaatregelen in aanvaardbare verhouding tot de kosten die gemoeid zouden zijn met de schade waartegen de organisatie zich beveiligt.

4. Verantwoordelijkheid voor Informatiebeveiliging

Bestuurder

De bestuurder is eindverantwoordelijk voor de invoering en naleving van het informatiebeveiligingsbeleid. Zij geeft invulling aan deze verantwoordelijkheid door o.a. het aanstellen van de Functionaris Gegevensbescherming en middelen vrij te maken. De bestuurder is verantwoordelijk voor de beveiliging van de gebouwen en daarbij voornamelijk voor het voorkomen van ongeautoriseerde toegang.

Functionaris Gegevensbescherming (FG)

De FG is verantwoordelijk voor:

- Het informeren en adviseren van SKOP medewerkers en andere verwerkers die persoonsgegevens verwerken over hun verplichtingen uit hoofde van de AVG (Algemene Verordening Gegevensbescherming) en andere EU wet- en regelgeving en nationale bepalingen omtrent gegevensbescherming;
- Het toezien op naleving van AVG, en andere EU wet- en regelgeving en nationale bepalingen omtrent gegevensbescherming;
- Het toezien op naleving van het Privacy-/informatiebeveiligingsbeleid met betrekking tot de bescherming van persoonsgegevens;
- Het toezien op toewijzing van verantwoordelijkheden, bewustmaking en opleiding van het bij de verwerking betrokken personeel en de betreffende audits;

- Het geven van advies met betrekking tot de Data Protection Impact Assessment (DPIA) en het toezien of de uitvoering daarvan in overeenstemming is met de AVG
- Het samenwerken met de AP (Autoriteit Persoonsgegevens);
- Het optreden als contactpunt voor de AP.

Manager bedrijfsvoering
De manager bedrijfsvoering is verantwoordelijk voor de werkzaamheden die worden uitgevoerd door externe ICT partners. Ook is hij/zij verantwoordelijk voor de melding van (systeem)incidenten.

De ICT Partner is verantwoordelijk voor het beschikbaar zijn van het systeem in overeenstemming met de wensen van de applicatiebeheerders. Daartoe moet hij/zij zorgdragen dat er maatregelen zijn genomen op het gebied van back-up, recovery en computer uitwijk (continuïteitsplanning). Ook is hij/zij verantwoordelijk voor het regelmatig testen van deze maatregelen. Daarnaast onderhoudt de Manager bedrijfsvoering autorisatietabellen in zijn rol als autorisatiebeheerder, op aangeven van de applicatiebeheerder(s) en rapporteert hij/zij over verrichtte aanpassingen.

5. Categorieën persoonsgegevens

Kind
- Naam, voornaam
- Geboortedatum
- BSN
- Geslacht
- Bijzonderheden (gezondheid, dieet eisen, medicatie, ontwikkeling, gedrag)
- Ongevallenregistratie
- Beeldmateriaal: foto’s, video’s

Ouder
- Naam, voornaam, voorletters
- BSN
- Telefoonnummer
- E-mailadres
- Gezinssituatie
- Soort opvang
- Klachtenregistratie
- Bankrekeningnummer

6. Grondslag voor verwerking

SKOP verwerkt bijzondere en reguliere persoonsgegevens. Voor reguliere persoonsgegevens beroepen wij ons op de volgende grondslagen;
- Toestemming van de betrokken persoon.
- De gegevensverwerking is noodzakelijk voor de uitvoering van een overeenkomst.
- De gegevensverwerking is noodzakelijk voor het nakomen van een wettelijke verplichting.
- De gegevensverwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen.

Voor de Bijzondere persoonsgegevens komen daar de volgende grondslagen bij;

- Uitdrukkelijk toestemming van de betrokkene voor de verwerking van zijn/haar persoonsgegevens;
- De noodzakelijke verwerking met het oog op de uitvoering van verplichtingen en de uitoefening van specifieke rechten van u of de betrokken persoon. Dit op het gebied van het arbeidsrecht en het sociale zekerheids- en sociale beschermingsrecht;

7. Organisatorische maatregelen

Bewaartermijnen

SKOP heeft als uitgangspunt de persoonsgegevens niet langer op te slaan dan noodzakelijk en houdt zich voor het overige aan wettelijk vastgelegde bewaartermijnen.

Meldplicht datalekken

Er kunnen zich beveiligingsincidenten voordoen die de betrouwbaarheid in gevaar brengen. Wanneer deze worden gesignaleerd wordt onmiddellijk ingegrepen en de veiligheid hersteld. Wanneer daarbij echter persoonsgegevens verloren zijn gegaan of ongeoorloofd overhandigd, gezien of gewijzigd, wordt het incident als datalek bij de AP gemeld en worden betrokkenen onmiddellijk geïnformeerd. In het kader van de meldplicht wordt een administratie bijgehouden welke periodiek aan de bestuurder wordt gerapporteerd.
SKOP heeft een

Er kunnen zich beveiligingsincidenten voordoen die bij de AP gemeld moeten worden, zoals een datalek. Bij een datalek zijn persoonsgegevens mogelijk in onbevoegde handen gevallen. Er is een procedure om datalekken te melden. Niet alle incidenten hoeven gemeld te worden bij de AP/betrokkene. Onderdeel van de datalekprocedure is een incidentregistratie van waaruit wordt besloten om de het datalek wel of niet te melden. Deze incidenten worden periodiek aan het MT gerapporteerd.
SKOP heeft een procedure opgesteld die voor iedereen in de organisatie van toepassing is.

Rechten van klanten en (ex)medewerkers

Klanten en medewerkers hebben het recht om persoonsgegevens in te zien, te corrigeren of te verwijderen. Daarnaast bestaat het recht om de eventuele toestemming voor de gegevensverwerking in te trekken of bezwaar te maken tegen de verwerking van hun persoonsgegevens en hebben ze het recht op overdraagbaarheid van je gegevens. Voor zover persoonsgegevens door betrokkenen niet direct zelf ingezien of aangepast kunnen worden (bijvoorbeeld via het ouderportaal ‘Konnect’), kan een verzoek hiertoe worden ingediend bij info@kinderopvangpurmerend.nl.

Privacy by design / Privacy by default
Voor de werkzaamheden die wij uitvoeren maken we gebruik van diverse oplossingen van derden. Bij de ontwikkeling van nieuwe diensten of het aangaan van een overeenkomst met een nieuwe leverancier wordt dat de Functionaris Gegevensbescherming, aan de hand van een privacytoets, om advies gevraagd.
Tevens streven we ernaar dat alle diensten standaard zo privacy vriendelijk mogelijk worden ingericht.

Beeldmateriaal
SKOP gebruikt beeldmateriaal van pedagogische medewerkers en kinderen voor verschillende doeleinden;

1. Ter bevordering van de deskundigheid van de pedagogische medewerkers en coaches.
2. Voor observatie van kinderen ten behoeve van gedrag en veiligheid.

Voor de 1e categorie is geen toestemming nodig van de betrokkene (ouders van kinderen), dit valt onder gerechtvaardigd belang.
Voor de 2e categorie is wel toestemming nodig van de betrokkene.

Bewustwording
Medewerkers worden regelmatig geschoold m.b.t. het veilig omgaan met persoonsgegevens. Ook worden zij middels een online nieuwsbrief met tips, nieuws en tools t.b.v. bewustwording regelmatig geïnformeerd over ontwikkelingen op het gebied van privacybescherming.
Systemen worden regelmatig getest.

Audits
Jaarlijks wordt er een interne audit uitgevoerd en wordt aan de bestuurder gerapporteerd.
In het jaarverslag wordt een samenvatting van de incidenten, resultaten van interne audits en een advies voor komend jaar opgenomen. Ook spreekt de accountant jaarlijks een oordeel uit over de mate van privacybescherming bij SKOP.

8. Technische Maatregelen

SKOP heeft de volgende maatregelen genomen ter beveiliging van de persoonsgegevens.

- logische toegangsbeveiliging;
- beveiligde datacenters;
- beveiligde toegangsdeuren voorzien van code voor entree en archief;
- videocamera’s ten behoeve van inbraakbeveiliging;
- logging van de bewerkingshandelingen in de systemen;
- goede firewalls;
- up-to-date virusscanners;
- pseudonimisering en versleuteling van bijzondere persoonsgegevens;
- software tegen malware-aanvallen;
- back-ups.