



Protocol Privacy /Algemene Verordening Gegevensbescherming

Vanaf 25 mei 2018 zijn alle organisatie verplicht te houden aan de Algemene Verordening Gegevensbescherming. Praktisch voor op de groep gelden daarom de volgende regels:

- Blokkeer altijd je beeldscherm bij het verlaten van je werkplek (of als je pauzeert achter een werkplek).
- Laat documenten met persoonsgegevens (bijv kindlijsten) nooit onbeheerd achter op je bureau of bij de printer.
- Kies nooit voor automatisch opslaan van inloggegevens op de computer.
- Besef dat openbare netwerken niet veilig zijn.
- Let op wat je deelt via sociale media. Alleen Chantal kan foto's delen op de facebookpagina van De Toverdroom. Bij voorkeur plaatsen we alleen foto's waarop de kinderen onherkenbaar zijn of met nadrukkelijke toestemming van de ouders/verzorgers.
- Maak alleen foto's met de telefoon van de groep. Of wanneer je foto's met je eigen telefoon maakt, stuur deze dan door naar de groepstelefoon en verwijder ze meteen op je eigen telefoon.
- Bedek altijd de webcam om 'meekijken' te voorkomen. Tip: plak er een leuk stickertje overheen.
- Laat inlogcodes niet slingeren bij de computer. Mocht je ze niet kunnen onthouden, zorg dan dat ze in een (afgesloten) kast liggen en laat collega's weten waar dit is.
- Zorg ervoor dat de mobiele telefoon van de locatie beveiligd is met een wachtwoord of patroon. Zet dit ook op het lijstje voor je collega's die komen invallen.
- Gebruik bij notulen (van kindbesprekingen) en formulier ongevallenregistratie alleen de eerste letters van voor- en eventueel achternaam.
- Verstuur foto's via Whatsapp niet via groepen, maar per ouder of per verzendlijst (dan zien ouders elkaars nummer niet) of via Kindplanner.
- Verstuur mailtjes naar ouders (indien je vanaf de locatie mailt) altijd met de adressen in de BCC en niet in AAN. Straks kan het ook via Kindplanner.
- Geef nooit ouders de telefoonnummers of emailadressen van andere ouders. Vraag altijd eerst aan de ouder van wie men het wil hebben of je dit mag doorgeven. Of je vraagt bij speelafspraken

Wat als je je per ongeluk niet aan de bovenstaande regels hebt gehouden?

Dan is er sprake van een datalek. Een datalek is een beveiligingsincident waarbij persoonsgegevens gelekt zijn. Dit kan gaan om een ongeoorloofde toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens. Van een datalek is alleen sprake als er persoonsgegevens zijn gelekt!

Enkele voorbeelden van datalekken om dit wat duidelijker te maken:

- USB-stick met daarop persoonsgegevens is kwijtgeraakt



- Er is een laptop gestolen met daarop persoonsgegevens
- Er is door een hacker ingebroken in een databestand of systeem (met daarop persoonsgegevens)
- Er is een mailing verstuurd met alle e-mailadressen in de Aan of CC in plaats van BCC
- Uit een tas zijn papieren gestolen met daarop persoonsgegevens
- Door een crash van een harddisk of door brand zijn persoonsgegevens verloren gegaan en er is geen back-up

In bepaalde gevallen zijn wij verplicht melding te doen van een datalek bij de Autoriteit Persoonsgegevens (www.autoriteitpersoonsgegevens.nl). Meld het daarom altijd aan Chantal als er sprake is geweest van een datalek. Zij neemt actie of vertelt wat je zelf moet doen. Zij is ook de aandachtsfunctionaris persoonsgegevens. Deze moeten we hebben omdat we met bijzondere persoonlijke gegevens werken.

Ook kan het zo zijn dat we de betrokkenen moet informeren over het datalek. Dit zijn de personen van wie de gegevens zijn verwerkt.

Wanneer een datalek niet gemeld wordt, kan de Autoriteit Persoonsgegevens je een (flinke) boete geven. Ook is het belangrijk dat alle datalekken vastgelegd worden. Met deze documentatie moet de Autoriteit Persoonsgegevens kan gecontroleerd worden of we aan de meldplicht hebben voldaan.