AVG - do's & dont's

November 2018

Algemeen

- Het juist omgaan met persoonsgegevens is een integraal onderdeel van veiligheid en respect op school. Neem je verantwoordelijkheid daarin.
- Neem bij vragen over privacy contact op met de Functionaris Gegevensbescherming (FG) via fg@cvog.nl
- Houd je aan de geheimhoudingsbepaling die behoort bij je functie in het onderwijs (zie CAO).
- Clean Desk Policy – Laat geen lijsten, aantekeningen, sollicitatiebrieven, gespreksverslagen of andersoortige documenten met persoonsgegevens op je bureau of in de klas liggen wanneer je niet aanwezig bent. Berg deze op in een af te sluiten lade of kast.
- Hang geen lijsten met persoonsgegevens op tenzij dit strikt noodzakelijk is.
- Deel bij communicatie over personen zo weinig mogelijk gegevens, bijv. alleen voornaam en leerlingnummer.
- Werk zoveel mogelijk in de daarvoor bestemde applicaties (zoals SOMtoday, Raet) en bewaar daarin persoonsgegevens. Zodoende zijn persoonsgegevens goed beveiligd en centraal terug te vinden voor jezelf maar ook wanneer de betrokkenen zijn/haar gegevens wil inzien of verwijderen.
- Check voorafgaand aan het gebruik van een (nieuwe) applicatie of leverancier waarin persoonsgegevens worden verwerkt of dat vanuit AVG mag en of daar alles voor geregeld is (bv verwerkersovereenkomst). Check dit bij twijfel altijd bij de FG (fg@cvog.nl).
- Verwijder persoonsgegevens wanneer deze niet meer noodzakelijk zijn.
- Stuur verzoeken of klachten van betrokkenen t.a.v. persoonsgegevens altijd door naar de FG.

ICT veiligheidsmaatregelen

- Clean Screen Policy - Beveilig persoonsgegevens op je scherm door bij (kortstondige) afwezigheid je computer altijd te vergrendelen (Windows toets + L en via Ctrl+Alt+Del op een remote desktop).
- Deel bestanden met persoonsgegevens die naar externen gaan altijd in PDF én op een beveiligde manier. Gebruik 7Zip met encryptie d.m.v. een wachtwoord. Verstuur dit wachtwoord via een ander kanaal (bijvoorbeeld telefonisch doorgeven via sms).
- Beveilig bestanden met bijzondere persoonsgegevens (bv. medisch, BSN, geloofsovertuiging) altijd met een wachtwoord (bv met 7Zip); ook op het interne netwerk, op google drive of Office 365.
- Beveilig eigen apparaten en thuisnetwerk goed (up-to-date antivirus-/beveiligingssoftware, firewall, inloggen met complex wachtwoord op computer, tablet en telefoon).
- Vermijd het gebruik van USB sticks om persoonsgegevens op te slaan. Gebruik altijd wachtwoord en encryptie (bv Bitlocker for Windows en Filevault voor Apple). Verlies van USB stick komt zeer vaak voor!
- Het is niet toegestaan om de cloudomgeving van je schoolaccount te synchroniseren naar privé-apparatuur, bijvoorbeeld via OneDrive en Google Sync.
- Het gebruik van e-mail en agenda apps op telefoons is alleen toegestaan wanneer de telefoon automatisch wordt vergrendeld na max 1 minuut. Laat geen devices onbeheerd achter.

E-mail

- Wees zeer voorzichtig met het (snel) versturen van e-mails met persoonsgegevens. NB: Het versturen van e-mails met persoonsgegevens aan onbedoelde personen of personen die de mail niet noodzakelijkerwijs hoeven te zien was in 2017 met bijna 50% de grootste bron van gemelde datalekken in Nederland!

- Gebruik geen eigen mailprogramma's maar alleen het e-mailadres en -programma dat de school beschikbaar stelt.
- Stuur geen hele mailwisselingen door waar persoonsgegevens van derden in worden genoemd die niets met het onderwerp van de e-mail te maken hebben (verwijder bijv. een deel van de mailwisseling).
- Verwijder ontvangen e-mails met persoonsgegevens na gebruik zo snel mogelijk. Stel je e-mailprogramma zo in dat e-mails na 1 maand worden verwijderd. Verwerk noodzakelijk te bewaren informatie in andere systemen (bv SOMtoday). Sla e-mails die bewaard moeten worden op in een aparte map in outlook.
- Deel geen persoonsgegevens in agenda afspraken die voor iedereen zichtbaar zijn. Gebruik algemene, anonieme omschrijvingen of afkortingen. Gebruik zo nodig de privé functie.

Exporteren en prints

- Vermijd het exporteren van persoonsgegevens (uit bv SOMtoday) tot alleen wanneer het strikt noodzakelijk is voor de uitvoering van je taak en exporteer dan ook alleen de persoonsgegevens die nodig zijn.
- Vermijd het uitprinten van persoonsgegevens (bv klaslijsten) tot alleen wanneer strikt noodzakelijk en er geen andere manier is om de lijst mee te nemen.
- Sla exports op een veilige plek op, bij voorkeur met een wachtwoord om het weer te openen.
- Verwijder exports en andere lijstjes direct na bereiken van het doel waarvoor je het geëxporteerd hebt. Later opnieuw dezelfde nodig? Maak dan opnieuw een export aan.
- Vernietig lijsten, printjes e.d. met persoonsgegevens op een veilige manier, bijv. papierversnipperaar; gooi het nooit bij het oud papier en laat printjes nergens achter.

SOMtoday

- Realiseer je bij het maken van notities en verslagen (bv in SOMtoday) dat de betrokkene inzage hierin kan vragen. Houdt het feitelijk en objectief.
- SOMtoday bevat veel bijzondere (en gevoelige) persoonsgegevens. Wees extra alert op het naleven van de beveiligingsmaatregelen. Vergrendel altijd je scherm bij (kortstondige) afwezigheid. Deel nooit wachtwoorden.
- Communiceer bij voorkeur zoveel mogelijk via SOMtoday. Dit is een afgeschermde beveiligde omgeving. Ook draagt dit bij aan het beheersen (bv. toepassen bewaartermijnen) van persoonsgegevens van leerlingen door het centraal in de applicatie te bewaren.

Excursies

- Bij verplichte excursies kunnen zonder toestemming noodzakelijke persoonsgegevens worden gedeeld met derden (bv. met vervoersbedrijf, hotels e.d.).
- Check vooraf of er een verwerkersovereenkomst nodig is bij de Functionaris Gegevensbescherming.
- Laat leerlingen een foto of digitale kopie van hun zorgpas op hun eigen mobiele telefoon meenemen.
- Maak bij Whatsapp geen groep aan maar een verzendlijst. Hierdoor zijn niet alle berichten (incl. mogelijke persoonsgegevens) voor iedereen zichtbaar maar kan er wel gecommuniceerd worden. Stel dit niet verplicht maar doe dit obv vrijwilligheid (toestemming door deelname). Let op: dit kan alleen bij leerlingen >16 jaar (personen onder de 16 mogen volgens gebruiksvoorwaarden van Whatsapp de applicatie niet gebruiken).
- Bijzondere persoonsgegevens (bv. dieet) mogen alleen gedeeld worden met schriftelijke toestemming.

Foto's en video's

- Herkenbare personen op foto's/video's zijn persoonsgegevens. Dus foto's maken en publiceren is niet zondermeer toegestaan.
- Wat mag wel:
    - foto's en video's die noodzakelijk/onmisbaar zijn bij het primaire onderwijsproces (bv pasfoto voor in SOMtoday / video opname voor opleidingsschool). Toestemming dus niet nodig.
    - onder voorwaarden mogen ook foto's en video's van direct aan school gerelateerde activiteiten zoals open dagen of musicals. Hierbij moet er een afweging gemaakt worden tussen het belang van school en die van leerling/medewerker waarbij het belang van kinderen zwaar weegt. Het zonder restricties publiceren van deze foto's is niet toegestaan. Lees de richtlijn AVG en foto's/video's hoe hier mee om te gaan.
    - Foto's/video's bij andere situaties (bv. klassenfoto's) mogen alleen gemaakt worden met schriftelijke toestemming (van ouders bij <16jr).
- Raadpleeg vooraf de richtlijn 'AVG en foto's/video's' en vraag om advies bij de FG (fg@cvog.nl).

Sollicitatiebrieven en CV's

- Verwijder en vernietig digitale én uitgeprinte sollicitatiebrieven, CV's en overige documenten (ook uit e-mail!) uiterlijk 4 weken na afronden van het sollicitatieproces.
- Uitzonderingen: CV/brief van nieuwe werknemer mogen bewaard blijven in personeelsdossier. Bij schriftelijke toestemming mogen CV's van sollicitanten max 1 jaar bewaard worden.
- Deel sollicitatiebrieven en CV's op een veilige manier en alleen met medewerkers die bij het sollicitatieproces betrokken zijn. Print sollicitatiebrieven en CV's alleen uit als het noodzakelijk is en er geen andere manier is om ze mee te nemen.
- Vernietig uitgeprinte sollicitatiebrieven en CV's, lijsten e.d. met persoonsgegevens op een veilige manier, bijv. een versnipperaar; gooi het nooit bij het oud papier en laat printjes nergens achter.
- Wanneer je dienstverband eindigt zorg je ervoor dat je alle werk-gerelateerde persoonsgegevens inlevert dan wel vernietigd, mochten deze niet meer bewaard hoeven te worden.
- Gespreksnotities, klachten e.d. bevatten vaak gevoelige of bijzondere persoonsgegevens. Wanneer het noodzakelijk is om deze te bewaren, doe dit dan op een centrale en voldoende beveiligde locatie (bv. personeelsdossier). Hierdoor worden o.a. datalekken voorkomen, kunnen betrokkenen hun rechten uitoefenen (bv inzage) en kunnen de persoonsgegevens worden verwijderd na afloop van de bewaartermijn.

Datalekken

- Een datalek is iedere inbreuk op de beveiliging die kan leiden tot inzicht in, misbruik van of verlies van persoonsgegevens.
- Een datalek kan bv. ontstaan als een laptop, usb stick of telefoon wordt verloren of gestolen, een lijst met aanmelders voor een bijeenkomst ergens blijft liggen, een e-mail over een persoon naar een verkeerd e-mailadres wordt gemaild of wanneer iemand ongeautoriseerd toegang heeft tot SOMtoday.
- Bij (het vermoeden van) een datalek, hoe klein ook, moet er **direct** contact opgenomen worden met de Functionaris Gegevensbescherming (FG) via fg@cvog.nl
- Het is aan het Emergency Response Team (FG / CvB / ICT) om te besluiten of het datalek gemeld moet worden aan de Autoriteit Persoonsgegevens en de betrokkenen. Meldt nooit zelf een datalek extern.