Protocol Voorkomen en melden van datalekken

Wat is een datalek?
Een datalek is een ruim begrip. Er wordt gesproken over een datalek als iemand toegang heeft of kan krijgen tot persoonsgegevens terwijl dat niet mag. Bekende voorbeelden hiervan zijn het verkrijgen van persoonsgegevens door hackers of het verliezen van een USB-stick met deze gegevens. Ook het kwijtraken van een laptop met persoonsgegevens kan een datalek zijn.

Het bevoegd gezag van Samenwerkingsverband (SWV) Driegang is verantwoordelijk voor de bescherming van persoonsgegevens van leerlingen, ouders/verzorgers en personeel.

Vanaf 1 januari 2016 is de meldplicht datalekken van kracht. Die wet geeft de privacytoezichthouder College Bescherming Persoonsgegevens (CBP) een verzwaarde boetebevoegdheid. Dat wil zeggen dat deze privacytoezichthouder het niet tijdig melden van een datalek kan bestraffen met een boete tot maximaal € 810.000,00 of een boete tot 10% van de omzet van een organisatie. SWV Driegang is verplicht om datalekken te voorkomen en datalekken zo snel mogelijk te melden. Hiervoor zijn afspraken gemaakt met het personeel en met leveranciers van administratie- en ICT-systemen.

De Personeels-Medezeggenschapsraad (PMR) van SWV Driegang heeft instemmingsrecht m.b.t. dit protocol. De PMR kan ook advies geven aan SWV Driegang n.a.v. adviezen of klachten van ouders/verzorgers of medewerkers. Bij veranderingen in dit protocol wordt de PMR altijd om toestemming gevraagd. Dit protocol wordt na vaststelling geplaatst op de website van SWV Driegang en is zodoende openbaar voor ouders/verzorgers, leerlingen en medewerkers. Hiermee garandeert SWV Driegang dat zorgvuldig en transparant met persoonsgegevens wordt omgegaan. Het protocol verplicht de medewerkers ook om op de juiste wijze met persoonsgegevens om te gaan.

Het voorkomen van datalekken:
Het volgende is geregeld om datalekken te voorkomen:

- Met alle medewerkers is afgesproken waar de persoonsgegevens opgeslagen mogen worden en er zijn afspraken gemaakt hoe om te gaan met persoonsgegevens.
- Persoonsgegevens zijn beveiligd.
- Er zijn bewerkersafspraken gemaakt.
- Alle medewerkers zijn op de hoogte hoe zij datalekken kunnen voorkomen en hoe en bij wie zij datalekken moeten melden.

Welke datalekken moeten gemeld worden:
De meldplicht geldt voor alle persoonlijke gegevensbestanden, waarvoor SWV Driegang verantwoordelijk is.
De volgende datalekken moeten gemeld worden:

- Verlies of inbreuk van leerlinggegevens.
- Verlies of inbreuk van persoonsgegevens personeel.
- Hacken of lekken van bijzondere persoonsgegevens, zoals medische gegevens.
- Datalekken bij de leverancier van leerlingvolgsystemen of administratiesystemen, server of cloudoplossing van loon- of persoonsadministratie.

Melden van datalekken:
In eerste instantie dient degene die het datalek veroorzaakt of ontdekt heeft dit te melden aan de coördinator/adjunct-coördinator van de kamer. Indien er ongunstige gevolgen voor betrokkenen kunnen veroorzaakt worden door het datalek, dient ook de betrokkene op de hoogte gesteld te worden.
Indien het datalek veroorzaakt wordt door de leverancier dient de verantwoordelijke (coördinator) een melding te doen aan de leverancier m.b.t. het lek.
Datalekken waarbij persoonlijke ongunstige gevolgen voor betrokkenen of een hele groep van betrokkenen zijn veroorzaakt moeten binnen twee dagen gemeld worden bij het CBP (College Bescherming Persoonsgegevens).

De plaatsen waar persoonsgegevens opgeslagen mogen worden:
SWV Driegang heeft de volgende afspraken gemaakt om persoonsgegevens op te slaan:

- Personeelsgegevens worden opgeslagen in TAS (digitaal systeem van administratiekantoor Dyade). Daarnaast is er nog een afsluitbare kast met gegevens over het personeel. Alle personeelsgegevens worden in 2017 gedigitaliseerd en opgeslagen in TAS. Vanaf 01-01-2018 wordt er geen papieren dossier van personeelsleden meer bewaard.
- Leerlinggegevens worden door alle medewerkers opgeslagen en uitgewisseld in Grippa of een aan de school gerelateerd administratiesysteem. Er worden geen papieren dossiers van leerlingen meer opgebouwd.
- De medewerkers (met uitzondering van de onderwijsassistenten) van kamer EC Rotonde werken op de eigen server:
    - Outlook (agenda's van de medewerkers).
    - Mail via de server.
    - Een beschermde omgeving voor opslag (eigen ruimte en een gedeelde ruimte).
- De medewerkers van kamer Rivierengebied Midden Nederland werken in G Suite for Education (Google).
- De medewerkers van kamer Alblasserwaard-West werken op een eigen laptop in afwachting van een besluit over een gezamenlijk ICT-systeem.
- Er wordt naar gestreefd dat alle medewerkers van SWV Driegang met hetzelfde systeem gaan werken (ambitie voor 2018).

Bewerkersafspraken:
SWV Driegang heeft bewerkersovereenkomsten afgesloten met Grippa en de leverancier van de server van EC Rotonde. Deze leveranciers geven in deze bewerkersovereenkomsten aan, dat hun product veilig is op het gebied van datalekken.

Hoe omgaan met persoonsgegevens:
Persoonsgegevens mogen door SWV Driegang alleen worden verwerkt om een vooraf vastgesteld doel te bereiken. Gegevens die hiermee niet in verband staan, mogen niet worden verzameld of bewaard. Hiervoor zijn de juiste, afgesproken beveiligingsmaatregelen uitgevoerd, zodat de gegevens niet voor een verkeerd doel gebruikt kunnen worden.

Deze persoonsgegevens mogen alleen verwerkt worden als de Wet bescherming persoonsgegevens

(Wbp) hier een grond voor noemt. Voor SWV Driegang gelden de onderstaande relevante gronden:

- De betrokkene heeft toestemming geven.
- De gegevens zijn noodzakelijk voor de uitvoering van de overeenkomst met de betrokkene.
- De wetgeving eist dat persoonsgegevens verwerkt worden.
- Op basis van een opgedragen publiekrechtelijk taak is gegevensbewerking noodzakelijk, bijvoorbeeld bij de aanvraag toelaatbaarheidsverklaring (TLV).
- De verwerking van persoonsgegevens is noodzakelijk om een ernstige bedreiging (van de gezondheid) van de betrokkene te voorkomen.
- Als er sprake is van gerechtvaardigd belang (indien het verzamelen van persoonsgegevens belangrijker is dan het privacybelang van de betrokkene).

Bij het verwerken van persoonsgegevens moet de volgende beveiliging uitgevoerd worden:

- Dataminimalisatie.
- Transparantie.
- Rechten van de betrokkene.

Beveiliging van persoonsgegevens:
Zorgvuldig omgaan met persoonsgegevens vraagt om een goede beveiliging. SWV Driegang is verplicht om deze gegevens te beveiligen volgens de “stand van de techniek”.

Realisatie beveiliging :

- Kamer ECR:
  De medewerkers van kamer ECR werken met een server voor de medewerkers. Er wordt gewerkt met Outlook en gemeenschappelijke mail.
- Kamer RMNL:
  De medewerkers van kamer Rivierengebied Midden Nederland werken in G Suite for Education (Google).
- Kamer AWW:
  De medewerkers van kamer Alblasserwaard-West werken op een eigen laptop in afwachting van een besluit over een gezamenlijk ICT-systeem.
- Intentie:
  Er wordt naar gestreefd dat alle medewerkers van SWV Driegang met hetzelfde systeem gaan werken (ambitie voor 2018).
- Alle kamers van SWV Driegang werken met Grippa.

Bij deze beveiliging wordt gebruikgemaakt van zogenaamde dataminimalisatie.
Er krijgen niet meer mensen toegang tot de gegevens of programma’s dan strikt noodzakelijk en er wordt alleen opgeslagen wat noodzakelijk is of mag.

Bij de beveiliging van persoonsgegevens wordt ook rekening gehouden met het type persoonsgegevens:

- Publieke informatie: deze informatie mag met iedereen gedeeld worden.
- Gevoelige informatie: deze informatie is bestemd voor een specifiek publiek; deze informatie wordt afgeschermd.
- Zeer gevoelige informatie: deze informatie is bestemd voor een zeer beperkt publiek en

absoluut niet voor derden; hiervoor worden veiligheidsmaatregelen getroffen.

Bewaartermijnen:
Een standaard bewaartermijn van leerlinggegevens is twee jaar na afloop van het traject of verlaten van de school. De bewaartermijn van het overstapdossier (naar een andere school of ander arrangement) is drie jaar.

Groeidocument:
Dit protocol is een groeidocument. Medewerkers worden verzocht om verbeteringen en aanvullingen m.b.t. dit Protocol Voorkomen en melden datalekken te melden bij de kamercoördinator.

Informeer ouders/verzorgers, medewerkers en wees transparant:
Personeelsleden hebben inzicht in hun personeelsdossier.
De medewerkers van SWV Driegang zijn naar ouders/verzorgers transparant over het gebruik van persoonsgegevens. Ouders/verzorgers hebben te allen tijde inzicht in de persoonsgegevens van hun kind. Aan ouders/verzorgers moet altijd toestemming worden gevraagd om persoonsgegevens van hun kind toe te voegen aan het leerlingdossier. Ook bij overdracht moeten ouders/verzorgers toestemmen welke gegevens overgedragen mogen worden.

Toestemming en rechten ouders/verzorgers:
De medewerkers van SWV Driegang moeten rekening houden met de rechten van de betrokkenen, als zij persoonsgegevens verzamelen en gebruiken. De rechten van een betrokkene moeten zonder belemmering of opgaaf van reden uitgevoerd kunnen worden. Het gaat hierbij om de volgende rechten:

- Ouders/verzorgers of medewerkers worden in begrijpelijke taal geïnformeerd over het gebruik van de persoonsgegevens.
- Ouders/verzorgers of medewerkers hebben inzage in alle verwerkte persoonsgegevens. Ook hebben zij recht op informatie van het doel van de verwerking.
- Ouders/verzorgers en medewerkers kunnen ontbrekende of verkeerd vastgelegde gegevens corrigeren.
- Ouders/verzorgers en medewerkers mogen opdracht geven om gegevens te verwijderen, die niet (langer) nodig zijn om de vastgelegde doelen te bereiken.
- Ouders/verzorgers mogen verzet instellen tegen een verwerking van persoonsgegevens (bijvoorbeeld bij registratie van het burgerservicenummer).

Deze aanpassingen van persoonsgegevens dienen binnen vier weken uitgevoerd te worden. SWV Driegang kan met opgaaf van redenen de termijn eenmaal verlengen met nogmaals vier weken.

Het gebruik van Grippa:
Voor het bovenschoolse leerlingdossier gebruikt SWV Driegang Grippa.
Grippa heeft de volgende mogelijkheden:

- Beschrijving arrangementen en voorzieningen.
- Bijhouden van toegekende arrangementen en voorzieningen en toegekende middelen hiervoor.
- Aanvraag ondersteuningstraject door intern begeleiders.

- Toekenning arrangementen en voorzieningen.
- Bovenschools dossier voor ambulant begeleiders, behandelaars en onderwijsassistenten.
- Aanvraag toelaatbaarheidsverklaringen.
- Administratie van toelaatbaarheidsverklaringen.
- Administratie thuiszitters.
- Communicatie (mail) over ondersteuningstrajecten.

Per kamer van SWV Driegang is afgesproken welke mogelijkheden van Grippa gebruikt worden. Gebruikers krijgen binnen Grippa rechten, die bij hun functie of deelname aan ondersteuningsarrangementen behoren.

Het is niet toegestaan om “voor eigen” gebruik persoonsgegevens te printen en zelf een papieren dossier van een leerling of persoon op te bouwen. Ook mogen persoonsgegevens niet opgeslagen worden op een privé-computer of -laptop.

Het gebruik van de beschermde, gedeelde omgeving:
De server van kamer ECR heeft een aantal mogelijkheden:

- Een algemeen beschermde omgeving, waar informatie opgeslagen wordt, die een doelgroep kan delen.
- Een eigen beschermde omgeving, waarop een personeelslid zijn of haar eigen zakelijk gegevens kan opslaan.
- Afgeschermde mail via Outlook.
- Afgeschermde agenda via Outlook.

Kamer RMNL werkt in de beschermde G Suite for Education (Google)-omgeving.
De medewerkers van kamer Alblasserwaard-West werken op een eigen laptop in afwachting van een besluit over een gezamenlijk ICT-systeem. Er wordt naar gestreefd dat alle medewerkers van SWV Driegang met hetzelfde systeem gaan werken (ambitie voor 2018).

Iedere kamer heeft zijn eigen indeling van de algemene, gedeelde omgeving. De toegang tot de mappen is bepaald per doelgroep. Een doelgroep krijgt dus toegang tot de mappen die bij die doelgroep behoren. Deze gegevens mogen gedeeld worden met de doelgroep.

Het gebruik van de beschermde eigen omgeving van de server/G Suite for Education (Google)-omgeving:
Iedere werknemer (behalve onderwijsassistenten) van SWV Driegang heeft op de server of G Suite for Education (Google)-omgeving een eigen beschermde omgeving. Op deze omgeving mag een werknemer zijn persoonlijke zakelijke gegevens opslaan. Voor zakelijke administratie moet de werknemer de server of **G Suite for Education (Google)-omgeving** gebruiken. Opslag op een eigen laptop of computer wordt afgeraden.

Het gebruik van Outlook:
Alle werknemers (behalve onderwijsassistenten) van kamer ECR maken gebruik van Outlook in de afgeschermde omgeving van de server voor:

1. Het bijhouden van de agenda.
2. Onderling mailcontact.

Per kamer zijn afspraken gemaakt over het gebruik van de agenda en de mail. Gevoelige en zeer gevoelige informatie mag niet per mail gedeeld worden. Gevoelige en zeer gevoelige informatie moet in agenda's afgeschermd opgeslagen worden.

Het gebruik van mail, internet en sociale media:
Veel informatie wordt tegenwoordig uitgewisseld door gebruik van mail, internet en sociale media. Medewerkers van SWV Driegang wordt geadviseerd om voor zakelijke mail en het internet het afgeschermde account van de server of de G Suite for Education (Google)-omgeving te gebruiken. Bij het gebruik van sociale media adviseert SWV Driegang om alleen publieke informatie te delen. Gevoelige en zeer gevoelige informatie mag niet gedeeld worden via sociale media.

Het gebruik van beeldmateriaal:
Het gebruik van een foto of video (beeldmateriaal) wordt gezien als een persoonsgegeven. Hierop is de Wbp van toepassing. Indien er beeldmateriaal publiekelijk gedeeld wordt, is hiervoor toestemming van de betrokkene nodig. Voor het gebruik van foto's of andere beeldmateriaal op sociale media kan het beste vooraf aparte toestemming gevraagd worden.

Vastgesteld door het bestuur op 8 mei 2018.
Instemming PMR op 10 januari 2018.