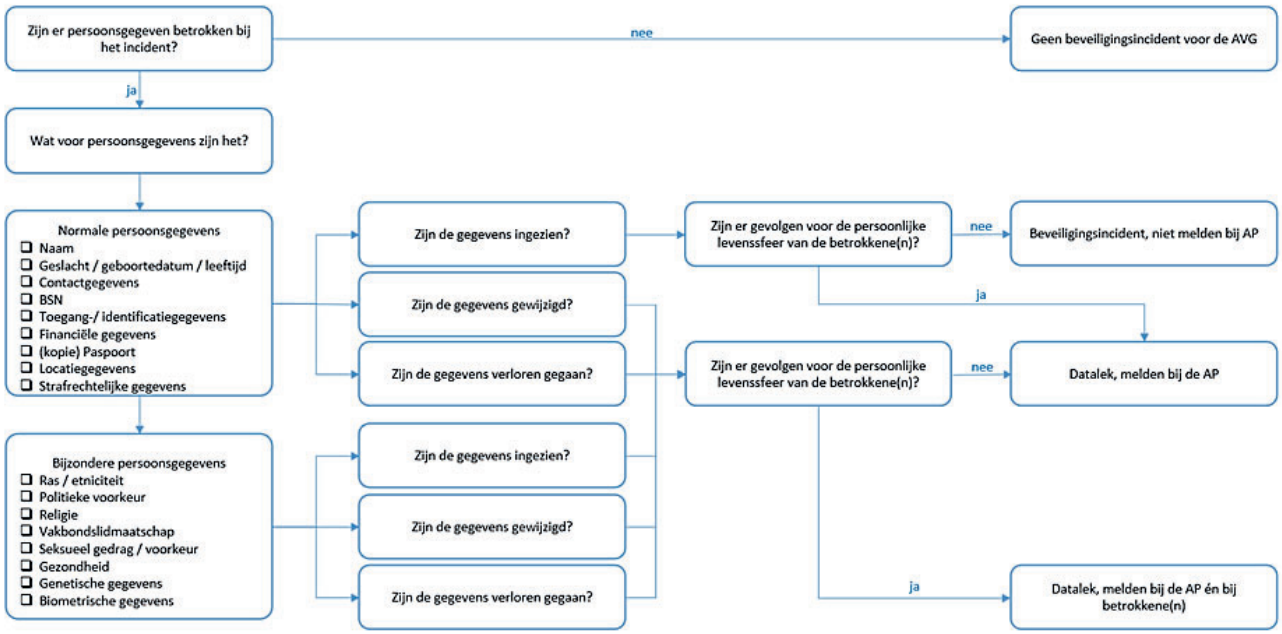
Datalekprotocol

De AVG geeft in artikel 4 de volgende definitie van een inbreuk in verband met persoonsgegevens: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.

Vrij vertaald betekent dit dat als er sprake is van het verkrijgen van toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van deze organisatie, of zonder dat dit wettelijk is toegestaan, sprake is van een beveiligingsincident, dan wel datalek. Dit kan zowel opzettelijk als onopzettelijk gebeuren.

Er zit een verschil in gradatie tussen een beveiligingsincident en een datalek. Een beveiligingsincident is een gebeurtenis waarbij de mogelijkheid bestaat dat de vertrouwelijkheid, integriteit of beschikbaarheid van informatie of informatieverwerkende systemen in gevaar is of kan komen. Een datalek is een beveiligingsincident, waarbij persoonsgegevens verloren raken of onrechtmatig worden verwerkt (opgeslagen, aangepast, verzonden, enz.). Alle datalekken zijn dus beveiligingsincidenten, maar niet alle beveiligingsincidenten zijn datalekken. Datalekken moeten binnen 72 uur gemeld worden bij de Autoriteit Persoonsgegevens (AP), terwijl beveiligingsincidenten alleen opgenomen hoeven te worden in het interne register van incidenten.

Om te bepalen of een beveiligingsincident een datalek is, is onderstaand stroomschema ontwikkeld. Naast de meldplicht voor datalekken is er ook de verplichting om alle beveiligingsincidenten registreren. Dat geldt óók voor alle incidenten die niet gemeld hoeven te worden aan de AP. Deze kan altijd om inzage hiervan vragen.



Een beveiligingsincident of datalek meld je zo spoedig mogelijk bij je direct leidinggevende en de privacyverantwoordelijke op school en Functionaris Gegevensbescherming (FG) via m.schoonus@vocampus.nl of 06 – 13 68 32 83.

Stappenplan datalekken

Stap 1 Zorg voor overzicht
Analyseer de situatie. Zorg dat je weet wat er is gebeurd en wat de omvang van het lek is. Gaat het om een inbreuk op de privacy door gelekte, vernietigde of gewijzigde gegevens? Wie heeft er mogelijk toegang (gehad) tot welke persoonsgegevens? Deze informatie wordt vastgelegd met daarin in ieder geval:

- Datum / periode van het beveiligingsincident
- Aard van het beveiligingsincident
- Omschrijving van de groep betrokkenen
- Aantal betrokkenen
- Type persoonsgegevens in kwestie
- Worden de gegevens binnen de keten gedeeld?

Stap 2 Beperk de schade
Op basis van de uitkomst van de gegevensverzameling in stap 1 wordt bepaalt of en zo ja welke maatregelen direct getroffen moeten worden. Om het lek te beëindigen en de schade te beperken. Schakel hiervoor zo nodig de juiste hulp in, bijvoorbeeld van de ICT-dienst.

Stap 3 Meld het datalek
De functionaris gegevensbescherming maakt de afweging of een datalek gemeld dient te worden bij de Autoriteit Persoonsgegevens (AP). Deze melding dient binnen 72 uur na ontdekking van het datalek plaats te vinden. In sommige gevallen moet een datalek ook aan betrokken personen gemeld worden. Dit is het geval als er sprake is van een verhoogd risico voor de rechten en vrijheden van betrokken personen.

Stap 4 Registreer
Tenslotte registreert de FG het datalek of beveiligingsincident in het datalekregister. Dit is een register, waar alle incidenten in worden bijgehouden en wat zo nodig ter beschikking van de AP gesteld moet worden. Het register dient ook als handvat om te kijken wat voor datalekken voorkomen, zodat training op dit onderdeel mogelijk wordt.

Belangrijk om te weten
Een datalek melden is niet erg. Het geeft aan dat je je bewust bent van de regels rondom privacy op school en een juiste inschatting gemaakt hebt wat betreft de mogelijke gevolgen van een datalek. Een tijdig gemeld datalek vormt ook een verkleining van het risico voor de organisatie. Je zult er dan ook nooit persoonlijk op worden afgerekend.

Een bewust niet gemeld datalek vormt juist een groot risico voor de organisatie en zal als het via een andere weg bij de AP terecht komt, vaak leiden tot een onderzoek met een mogelijke geldboete en imageschade als gevolg.