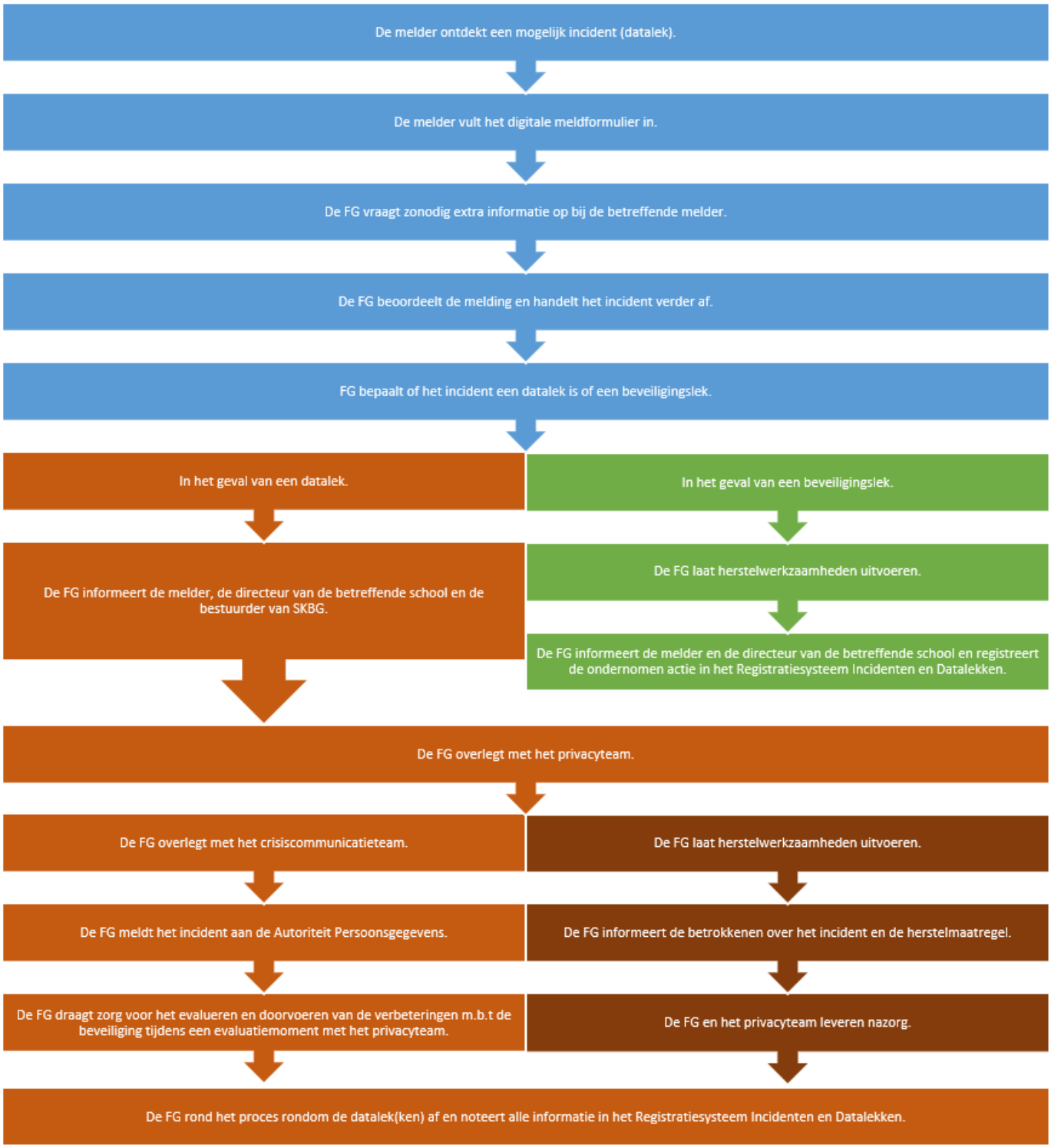
Protocol Meldplicht Datalekken

Schematische voorstelling proces datalekken.



1. Doel van dit protocol

Doel van dit protocol is medewerkers informeren over de wijze van handelen op het moment dat persoonsgegevens mogelijk of zeker in bezit zijn gekomen van personen die geen toegang tot die gegevens zouden mogen hebben. Het niet nakomen van de meldplicht kan leiden tot boetes die kunnen oplopen tot €820.000,- en imagoschade voor SKBG. Daarom dient een beveiligingsincident altijd serieus te worden genomen en zorgvuldig te worden afgehandeld.

2. Oppakken en afhandelen van de acute situatie

Om goed te kunnen handelen is het belangrijk om te weten wat onder een datalek verstaan wordt: Een datalek is een gevolg van een beveiligingsprobleem, echter is niet ieder beveiligingsincident een datalek. Wanneer er alleen sprake is van een zwakke plek in de beveiliging, spreken we van een beveiligingslek en niet van een datalek. Er is sprake van een datalek:

- Wanneer bij het beveiligingsincident persoonsgegevens verloren zijn gegaan,
- Wanneer er een aanzienlijke kans is dat persoonsgegevens verloren gaan of zijn gegaan,
- Wanneer we onrechtmatige verwerking van de persoonsgegevens niet redelijkerwijs kunnen uitsluiten.

Voorbeelden van beveiligingsincidenten zijn:

- Het kwijtraken van een USB-stick;
- Diefstal van een laptop, tablet of smartphone;
- Het verliezen van persoonsgegevens op papier (leerlingdossier);
- Onbevoegde toegang tot een gebouw/locaties/ruimten/kasten;
- Inbraak in het computersysteem van de school door een hacker;
- Het verlies van gegevens ten gevolge van een virus of *ransomware*[1];
- Het verlies van gegevens ten gevolge van een verwijdering van informatie;
- Het doorgeven van persoonsgegevens aan iemand die het niet had moeten ontvangen (bijvoorbeeld het sturen van gegevens aan de verkeerde externen of ouder(s));
- Het kwijtraken van wachtwoorden die toegang geven tot een gegevensbestand;
- Het kwijtraken van (papieren) gegevens door water- of brandschade.

3. Werkwijze

Criteria op basis waarvan je nagaat of je moet melden aan de Interne Functionaris Gegevensbescherming:

- Het datalek leidt tot een aanmerkelijke kans op nadelige gevolgen voor de bescherming van persoonsgegevens,
- De inbreuk heeft waarschijnlijk nadelige gevolgen voor de persoonlijke levenssfeer van de betrokkenen,
- De gevoeligheid van de gegevens; hoe gevoeliger de gegevens, hoe eerder er meldplicht is,
- Het aantal getroffen personen; hoe groter het aantal getroffen personen is, hoe eerder er moet worden gemeld.

Criterium dat aangeeft dat op basis van een veiligheidslek in het systeem niet hoeft te worden gemeld aan de betrokken personen:

- Wanneer de gegevens voldoende beschermd zijn (bijvoorbeeld versleuteld) zodat niet te achterhalen is om wiens gegevens het gaat.

[1] een type malware, ofwel kwaadaardige software, die een computer blokkeert of bestanden versleutelt. Pas als je losgeld (ransom) betaalt zou je de computer of de bestanden weer kunnen gebruiken.

Stap	Actie	Wie
1.	Bij het signaleren van een beveiligingsincident: Informeer direct de Functionaris Gegevensbescherming en leidinggevende van de school. Functionaris Gegevensbescherming: • Lars Timmermans | ✆ [redacted]	De ontdekker van het beveiligingsincident.
2.	Vul het digitale datalekformulier in en deze wordt automatisch gemaild deze naar de Functionaris Gegevensbescherming.	De ontdekker van het beveiligingsincident.
3.	Neem contact op met melder en leidinggevende voor het verkrijgen van een totaalbeeld van het beveiligingsincident.	Functionaris Gegevensbescherming
4.	Inventariseer of er acute maatregelen genomen moeten worden om het beveiligingsincident te dichten of dat er maatregelen genomen moeten worden om de gevolgen van het beveiligingsincident te beperken.	Functionaris Gegevensbescherming
5.	Beoordeel of er daadwerkelijk sprake is van een datalek aan de hand van de beleidsregels voor toepassing van *artikel 34a Wbp*. Bespreek dit met Externe Functionaris Gegevensbescherming. • André Jonker | ✆ [redacted]	Functionaris Gegevensbescherming
6a.	**Indien geen Datalek**; Beëindig de procedure en tref maatregelen. Registreer de melding in het meldingenregister met status Geen Datalek.	Functionaris Gegevensbescherming
6b.	**Indien wel Datalek**; Afhankelijk van de impact van het Datalek: 1. Overleg met het Privacyteam. 2. Overleg met het crisiscommunicatie team: a. Informeer de organisatie. b. Informeer Externe Functionaris Gegevensbescherming André Jonker | ✆ [redacted]	Functionaris Gegevensbescherming, directeur betreffende school, bestuurder SKBG
7.	Meld het datalek binnen 72 uur digitaal via het meldloket van de Autoriteit Persoonsgegevens.	Functionaris Gegevensbescherming
8.	Bepaal de te nemen maatregelen	Functionaris Gegevensbescherming
9.	Overweeg wie op welke wijze geïnformeerd moet worden over het datalek en genomen maatregelen: • In geval van leerlinggegevens; • In geval van personeelsgegevens; • In geval van organisatiegegevens.	Functionaris Gegevensbescherming, directeur betreffende school, bestuurder SKBG
10.	Indien er sprake is van een voorlopige melding bij de Autoriteit Persoonsgegevens, de melding aanvullen zodra bekend is welke maatregelen genomen zijn en welke personen geïnformeerd zijn	Functionaris Gegevensbescherming
11.	Uitvoering van maatregelen	Directeur betreffende school
12.	Monitoring van uitvoering maatregelen	Functionaris Gegevensbescherming
13.	Informeer alle betrokkenen (melder, directie, bestuurder en slachtoffer(s)) over uitgevoerde maatregelen en afhandeling datalek.	Functionaris Gegevensbescherming
14.	Evalueer het incident: Welke verbetermaatregelen zijn nodig om een volgend beveiligingsincident te voorkomen.	Functionaris Gegevensbescherming, directeur betreffende school, bestuurder SKBG
15.	Registreren van de melding in het meldingenregister	Functionaris Gegevensbescherming
16.	Afsluiten proces melding datalek.	Functionaris Gegevensbescherming

4. Taken en verantwoordelijkheden binnen SKBG onderwijs:

Bestuurder SKBG	Is eindverantwoordelijk voor het de uitvoering en monitoring van het proces datalekken.
Functionaris Gegevensbescherming	Plant, coördineert en evalueert het proces.
Medewerkers:	Zijn verantwoordelijk voor het direct melden van signalen/incidenten aan de Functionaris Gegevensbescherming en eigen leidinggevende.

5. Achtergrondinformatie en methodieken

Begrip	**Definitie**
Beveiligingsincident	Er is sprake van een zwakke plek in de beveiliging.
Datalek	Bij het beveiligingsincident zijn persoonsgegevens verloren gegaan of op een onbedoelde manier openbaar gemaakt, we kunnen onrechtmatige verwerking van de persoonsgegevens niet redelijkerwijs uitsluiten of op een onbedoelde manier openbaar gemaakt. .
Privacyteam	Bestaat uit de Functionaris Gegevensbescherming, de directeur van de school waar het beveiligingsincident voorvalt en de bestuurder van SKBG.

Opbouw van veiligheids- naar datalek