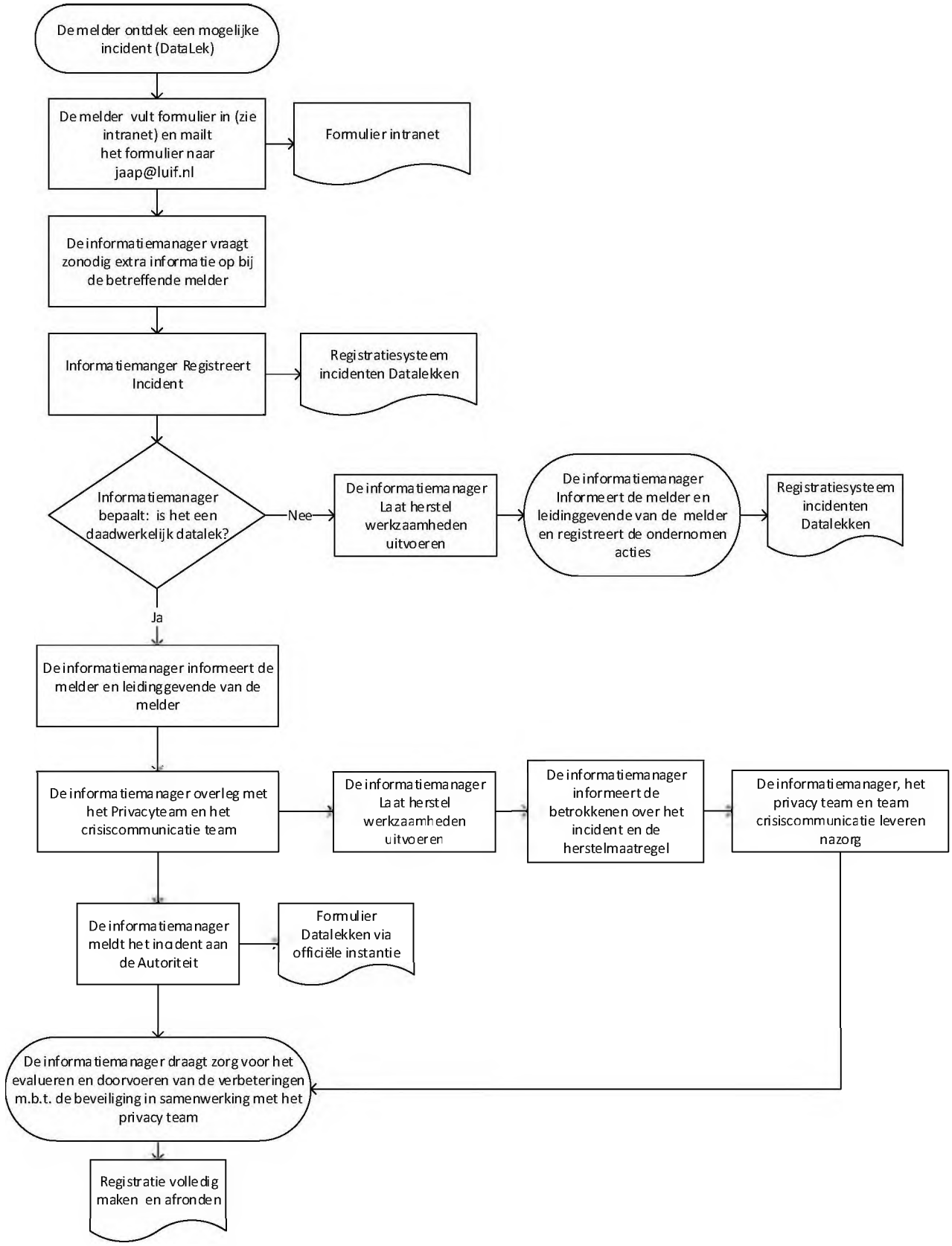
Protocol Meldplicht Datalekken

Schematische voorstelling Datalek Proces.



1. Doel van dit protocol

Doel van dit protocol is dat medewerkers weten hoe ze moeten handelen op het moment dat persoonsgegevens (cliëntgegevens, pleeggezingegevens, medewerkergegevens) 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,- [1]en imagoschade voor de organisatie. 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 moet worden.
Een datalek is een gevolg van een beveiligingsprobleem. Niet ieder beveiligingsincident is een Datalek. Als 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:

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

Voorbeelden van beveiligingsincidenten zijn:

- Het kwijtraken van een USB-stick;
- Diefstal van een laptop of telefoon;
- Het verliezen van cliëntengegevens op papier;
- Onbevoegde toegang tot een gebouw/locaties/ruimten/kasten;
- Inbraak in het computersysteem van (naam instelling) door een hacker;
- Het verlies van gegevens ten gevolge van een virus;
- 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 patiënt);
- 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 informatiemanager:

- 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 een 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:

- Als de gegevens voldoende beschermd zijn (bijvoorbeeld versleuteld) zodat niet te achterhalen is om wiens gegevens het gaat dan hoeft dit niet aan de betrokkene te worden gemeld.

[1] De maximumboete is gekoppeld aan de boete in het Wetboek van Strafrecht (artikel 23 vierde lid, zesde categorie).

Stap	Actie	Wie
	Acties door medewerker	
1	Bij het signaleren van een beveiligingsincident: Informeer **direct** de Informatiemanager. **Jaap Luif (020-4103920)**	Degene die het beveiligingsincident ontdekt.
2	Mail de details van de datalek naar info@luif.nl	Degene die het beveiligingsincident ontdekt.

Stap	Actie	Wie
	Actie door Informatiemanager / Privacyteam	
3	Neem contact op met melder en leidinggevende voor het verkrijgen van een totaalbeeld van het beveiligingsincident.	Informatiemanager
4	Inventariseer of er acute maatregelen genomen moeten worden om het Datalek te dichten of dat er maatregelen genomen moeten worden om de gevolgen van het beveiligingsincident of Datalek te beperken.	Informatiemanager
5	Beoordeel of er daadwerkelijk sprake is van een Datalek aan de hand van de Beleidsregels voor toepassing van artikel 34a Wbp.	Informatiemanager
6	Indien geen Datalek; Beëindig de procedure en tref maatregelen. Registreer de melding in het meldingenregister met status **geen Datalek**.	Informatiemanager in overleg met externe adviseurs
7	Indien wel Datalek; Afhankelijk van de impact van het Datalek: Overleg met het Privacyteam. Overleg met het crisiscommunicatie team: • Informeer in overleg met het crisiscommunicatie team de organisatie.	Informatiemanager
8	Meldt het Datalek **Binnen 72 uur** digitaal via het meldloket van de Autoriteit Persoonsgegevens	Informatiemanager
9	Bepaal de te nemen maatregelen	Informatiemanager in overleg met externe adviseurs

10	Overweeg wie op welke wijze geïnformeerd moet worden over het Datalek en genomen maatregelen: • In geval van cliëntgegevens; • In geval van personeelsgegevens; • In geval van organisatiegegevens.	Informatiemanager
11	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	
12	Uitvoering van maatregelen	Betrokken managers
13	Monitoring van uitvoering maatregelen	Informatiemanager
14	Informeer over uitgevoerde maatregelen en afhandeling Datalek • Lijnorganisatie (indien geïnformeerd, zie stap 9); • Betrokkenen (zie stap 12).	Informatiemanager
	Evaluatie/Onderzoek/Sluiting	
15	Evalueer het incident: Welke verbetermaatregelen zijn nodig om een volgend beveiligingsincident te voorkomen.	Informatiemanager, mensen die betrokken zijn geweest bij invoeren maatregelen en degene die het Datalek heeft ontdekt.
Stap	**Actie**	**Wie**
16	registreren van de melding in het meldingenregister (bewaartermijn van de melding: 3 jaar).	Informatiemanager
17	Afsluiten proces melding Datalek	Informatiemanager

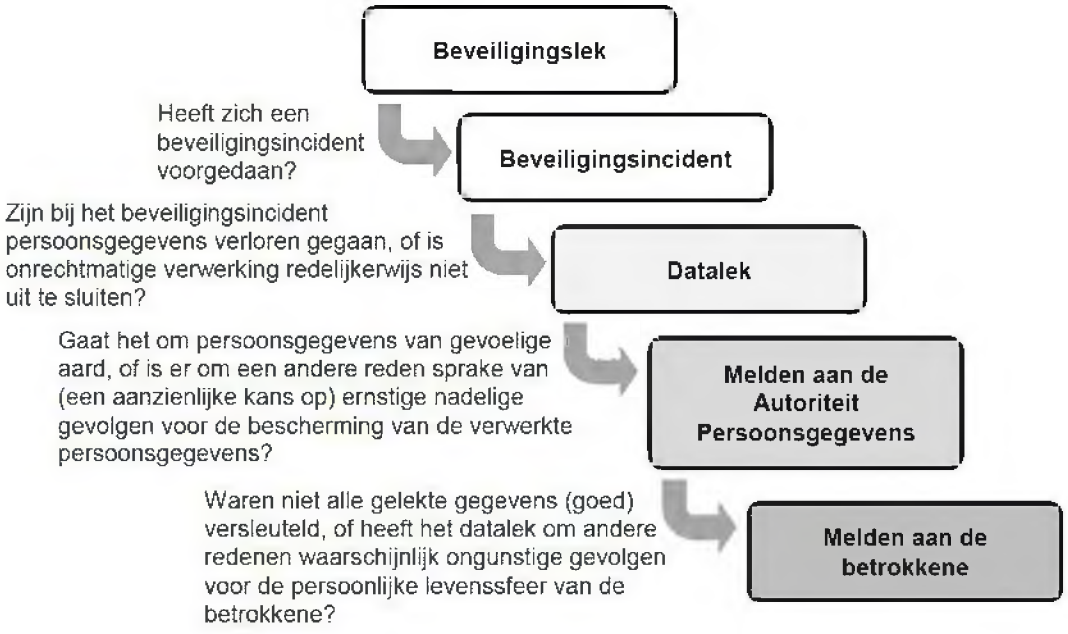
4. Taken en verantwoordelijkheden binnen Luif

Alle taken en verantwoordelijkheden liggen bij Jaap Luif

5. Achtergrondinformatie en methodieken
Definities

Begrip	Definitie
Beveiligingsincident	Er is alleen 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 Jaap Luif en eventueel externe adviseurs. A.h.v. deze analyse wordt bepaald of werkelijk een Datalek is en of het moet worden doorgezet naar Autoriteit Persoonsgegevens .

Opbouw van veiligheids- naar Datalek



Het proces van de Autoriteit Persoonsgegevens na binnenkomst van een melding