Protocol melden datalekken

Scholengroep Holland

Versie 1: opgesteld juli 2018
Evaluatie: december 2019

Protocol melden datalekken

1. Doel

Eenduidige werkwijze voor het melden van beveiligingsincidenten ter voorkoming van een boete op datalekken.

Elke organisatie wordt weleens geconfronteerd met een inbraak, fysiek op een locatie of op de digitale snelweg. Uiteraard hebben wij als organisatie onze scholen beveiligd en de digitale snelweg zo goed als mogelijk beveiligd tegen inbraak.
In een organisatie waar mensen werken worden fouten gemaakt. Je raakt weleens iets kwijt of je vergeet je laptop of smartphone goed op te bergen. Het hebben van sterke wachtwoorden, per applicatie, is iets wat uit praktisch oogpunt niet zo gauw wordt gedaan, maar waar grote beveiligingsrisico's aan kleven.

Iedereen maakt fouten en iedereen mag een fout maken, daar zijn wij mensen voor. Vaak maken wij fouten maar één keer, want we leren van onze fouten. Wat van fundamenteel belang is, is dat fouten (beveiligingsincidenten) gemeld worden als die gevolgen hebben voor onze belanghebbenden en organisatie.

2. Verantwoordelijkheden en bevoegdheden

Iedere medewerker:
Verantwoordelijk voor het melden van een beveiligingsincident
Schooldirecteur:
Verantwoordelijk voor het uitwerken van een incident en voor de afhandeling van de afgesproken verbetermaatregelen
Functionaris gegevensbescherming:
Verantwoordelijk voor het registreren, wegen en evt. melden van beveiligingsincidenten.
Privacyteam:
Verantwoordelijk voor het wegen van beveiligingsincidenten.
Bestuur:
Verantwoordelijk voor het bepalen of een incident gemeld wordt bij de Autoriteit Persoonsgegevens.

Functionaris gegevensbescherming en Privacy team

Naam/Functionaris	Telefoon	Emailadres
Dolf Dubois	06-14729330	Privacyteam@scholengroepholland.nl

3. Norm

Elk (beveiligings)incident moet binnen 24 uur gemeld zijn bij het privacyteam.
De functionaris gegevensbescherming dient een daaruit voortkomend datalek binnen 72 uur te melden bij de Autoriteit Persoonsgegevens.

4. Prestatie indicator

Register beveiligingsincidenten

5. Inhoud van procedure

Voorbereiden

Bij (ten minste) welke beveiligingsincident moet je altijd een interne melding doen?

- Bij het kwijtraken van een USB-stick;
- Bij diefstal van een laptop/smartphone/tablet;
- Bij het verliezen van papier waar klantgegevens op staan;
- Bij het signaleren van onbevoegden die zichzelf toegang verschaffen tot een gebouw, een locatie, een ruimte, kasten of computersystemen;
- Bij ongebruikelijke reacties van het computersysteem, zoals bijvoorbeeld een bewegende muis terwijl je zelf de muis niet aanraakt. Dit kan mogelijk wijzen op inbraak in het computersysteem door een hacker;
- Bij een virus;
- Bij het doorgeven van persoonsgegevens aan iemand die het niet had moeten ontvangen (bijvoorbeeld het sturen van gegevens aan de verkeerde ontvanger);
- Bij het kwijtraken van wachtwoorden die toegang geven tot een gegevensbestand;
- Bij het kwijtraken van (papieren) gegevens door water- of brandschade.

Bij twijfel moet je altijd een melding doen. Iedere melding wordt vastgelegd in een register. Het register wordt bijgehouden en beheerd door het privacyteam.

Wat is een datalek?
We spreken van een datalek als bijzondere persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens zouden mogen hebben.

Wat zijn bijzondere persoonsgegevens waarbij een melding noodzakelijk is:

1. Bijzondere persoonsgegevens als bedoeld in artikel 16 Wbp.
   Het gaat hierbij om persoonsgegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en om strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.
2. Gegevens over de financiële of economische situatie van de betrokkene.
   Hieronder vallen bijvoorbeeld gegevens over (problematische) schulden, salarissen en betalingsgegevens.
3. Andere gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene.
   Denk hierbij aan bijvoorbeeld gegevens over gokverslaving, prestaties op school of werk of relatieproblemen.
4. Gebruikersnamen, wachtwoorden en andere inloggegevens.
   Denk hierbij aan bijvoorbeeld de inloggegevens voor Parnassys, Basispoort, YouForce of welke software dan ook wordt gebruikt voor het vastleggen van kind- of personeelsgegevens.
5. Gegevens die kunnen worden misbruikt voor (identiteits)fraude.
   Het gaat hierbij onder meer om biometrische gegevens, kopieën van identiteitsbewijzen en om het Burgerservicenummer (bsn).

Uitvoeren

stap	Actie	Wie	
	Actie door medewerker		
1	Wanneer je een beveiligingsincident signaleert informeer direct je leidinggevende en het privacyteam.	Degene die het beveiligingsincident ontdekt	

2	Melding d.m.v. 'Formulier melden bveiligingsincident/datalekken' naar de schooldirecteur en naar privacyteam@scholengroepholland.nl	Degene die het beveiligingsincident ontdekt.	
	Actie door de schooldirecteur		
3	Schakel direct direct één van de privacy functionarissen in.	Schooldirecteur en bij diens afwezigheid degene die het beveiligingsincident heeft ontdekt.	
	Actie door funcionaris gegevensbescherming/privacyteam		
4	Contact met melder en schooldirecteur voor het verkrijgen van een totaalbeeld van het beveiligingsincident	Functionaris gegevensbescherming	
5	Inventariseren of er acute maatregelen genomen moeten worden om het datalek te dichten of maatregelen te nemen om de gevolgen van het beveiligingsincident of datalek te beperken	Functionaris gegevensbescherming	
6	Beoordelen of er werkelijk sprake is van een datalek aan de hand van de beleidsregels voor toepassing artikel 34a Wbp.	Functionaris gegevensbescherming	
7	Indien geen datalek, beëindigen procedure, melding opnemen in het meldingenregister (bewaartermijn 3 jaar) en maatregelen treffen	Functionaris gegevensbescherming, evt. in overleg met betrokken lijnorganisatie	
8	Indien wel datalek, afhankelijk van de bevindingen van het privacyteam en de impact van het datalek informeren van Bestuur	Privacyteam	
9	Binnen 72 uur wordt, op verzoek van de Bestuurder het datalek digitaal gemeld via het meldloket van de Autoriteit Persoonsgegevens	Functionaris gegevensbescherming	
10	Overwegen wie op welke wijze geïnformeerd moet worden over het datalek en de genomen maatregelen: * in geval van kindgegevens * in geval van personeelsgegevens * in geval van organisatiegegevens	Functionaris gegevensbescherming in overleg met Bestuurder en communicatie adviseur De betrokkenen	
11	In geval van voorlopige melding bij de Autoriteit Persoonsgegevens, de melding aanvullen zodra bekend is welke maatregelen genomen zijn en welke personen geïnformeerd zijn	Functionaris gegevensbescherming	
12	Uitvoering van maatregelen	Schooldirecteur	
13	Monitoring van uitvoering maatregelen	Functionaris gegevensbescherming	
14	Informeren over uitgevoerde maatregelen en afhandeling datalek aan betrokkene	Functionaris gegevensbescherming	

Controleren

	Evaluatie/onderzoek/sluiting		
15	Evaluatie van het incident, welke verbetermaatregelen zijn nodig om een volgend beveiligingsincident te voorkomen	Degene die het incident heeft ontdekt schooldirecteur Privacyteam	
16	Controle op de afhandeling van de verbetermaatregelen: Hebben de maatregelen geleid tot het gewenste resultaat?	Schooldirecteur Privacyteam	
17	Afsluiten melding in meldingenregister en aanvullen met de genomen stappen	Functionaris gegevensbescherming	
18	Afsluiten proces melding beveiligingsincident	Functionaris gegevensbescherming	
19	Jaarlijkse analyse van de incidenten en verbetermaatregelen	Functionaris gegevensbescherming	

Bijstellen/herstellen

20	Doorvoeren van verbetermaatregelen n.a.v. de jaarlijkse analyse van beveiligingsincidenten	Privacyteam	

6. Risico inventarisatie

Datalek wordt niet gemeld of datalek wordt te laat gemeld. In beide gevallen is een boete het gevolg.
Het niet melden van het datalek aan de betrokkenen.

7. Beheersmaatregel

Bewustzijn creëren bij medewerkers dat privacy voor een ieder een groot goed is, dat fouten maken menselijk is, maar dat je deze fouten moet melden.
Jaarlijks evalueren of het protocol voldoet.

8. Registratie / Documentatie

Documentatie	**Wie**	**Waar**	**Hoe lang**	**Vernietigen**
Ingevuld formulier Melden beveiligingsincidenten/datalekken	Privacyteam		3 jaar	Verwijderen
Register beveiligingsincidenten	Privacyteam		3 jaar	Verwijderen
Analyse beveiligingsincidenten	directeurenoverleg		3 jaar	Verwijderen