Protocol informatiebeveiligingsincident en en datalekken

Scholengroep OPRON

Preambule

Dit protocol geldt voor de onder Scholengroep OPRON ressorterende scholen:

Obs De Mieden	Meeden
Obs Inspecteur Amerikaschool	Noordbroek
Obs Burgemeester Verkruisenschool	Muntendam
Obs De Tandem	Zuidbroek
Obs De Viermaster	Veendam
Obs De Braskörf	Veendam
Obs Noorderbreedte	Veendam
Obs Hagenhofschool	Stadskanaal
Odbs Westerschool	Wildervank
Obs De Sleutel	Wildervank
Obs Meester Neuteboomschool	Stadskanaal
Obs De Oleander	Stadskanaal
Ojbs De Ommewending	Veendam
Obs De Badde	Musselkanaal
Obs De Musselhorst	Stadskanaal
Wim Monnereau-school	Veendam
Margaretha Hardenbergschool	Veendam

scholengroep opron

Inhoud

Inleiding

Het Protocol informatiebeveiligingsincidenten en datalekken sluit aan bij de uitgangspunten in het Privacybeleid van SCHOLENGROEP OPRON

Dit protocol biedt een handleiding voor de professionele melding, beoordeling en afhandeling van beveiligingsincidenten en datalekken. Het doel hiervan is het voorkomen van beveiligingsincidenten en datalekken.

Dit protocol is van toepassing op de gehele organisatie van SCHOLENGROEP OPRON en al haar medewerkers.

Gebruikte termen:

- **Beveiligingsincident**; een beveiligingsincident is een gebeurtenis die er voor zorgt of zou kunnen zorgen dat de beschikbaarheid, integriteit en/of vertrouwelijkheid van de informatievoorziening wordt aangetast.
- **Informatievoorziening**; het geheel van mensen, middelen en maatregelen, gericht op de informatiebehoefte van de organisatie.
- **Datalek**; een beveiligingsincident waarbij persoonsgegevens verloren raken of onrechtmatig worden bewerkt (opgeslagen, aangepast, verzonden, et cetera). Alle datalekken zijn beveiligingsincidenten, maar niet alle beveiligingsincidenten zijn datalekken.
- **Betrokkene**; de persoon van wie de persoonsgegevens zijn gelekt.

Wet- en regelgeving datalekken

Op 1 januari 2016 is de Wet meldplicht datalekken ingevoerd. Door deze meldplicht zijn ook scholen verplicht melding te maken van ernstige datalekken bij de Autoriteit Persoonsgegevens. Het nalaten van deze melding kan leiden tot een fikse boete.

Meldplicht datalekken onder de AVG
Onder de nieuwe Europese privacywet die sinds 25 mei 2018 geldt, de Algemene verordening gegevensbescherming (AVG), blijft de meldplicht datalekken bestaan.

De AVG stelt strenge eisen aan de registratie van de datalekken in een organisatie. Organisaties moeten alle datalekken documenteren. Met deze documentatie moet de AP kunnen controleren of zij aan de meldplicht datalekken hebben voldaan.

De meldplicht is alleen van toepassing wanneer persoonsgegevens worden verwerkt. Als de school gebruik maakt van leveranciers, zoals uitgevers of distributeurs, die persoonsgegevens ontvangen van de school, dan moet de school met deze verwerkers aanvullende afspraken maken over het melden van datalekken.

Er is sprake van een datalek als er bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, óf waarbij het niet valt uit te sluiten is dat persoonsgegevens verloren zijn gegaan. Er is persoonlijke informatie 'gelekt'. Dit kan zijn een hack, het verliezen van een usb-stick of de diefstal van een laptop. Maar ook een verkeerd verzonden email of een verkeerd ingestelde autorisatie.

De meldplicht geldt voor de verantwoordelijke voor de persoonsgegevens, dat is dus het schoolbestuur. Als er een datalek is, moet daar binnen 72 uur na ontdekking van het lek melding van worden gedaan bij de Autoriteit Persoonsgegevens.

Afspraken met scholen en leveranciers

Het schoolbestuur maakt als verantwoordelijke voor de persoonsgegevens de onderstaande datalek-afspraken met de scholen en de leveranciers die persoonsgegevens ontvangen en verwerken:

- De ontdekker van een datalek meldt dit binnen 24 uur bij de directeur van de school of de zaakgelastigde of contactpersoon van een leverancier.
- De directeur of de zaakgelastigde of contactpersoon meldt binnen 24 uur het datalek bij de Functionaris Gegevensbescherming via het mailadres: fg@opron.nl
- De FG neemt de melding op in het Register Datalekken en doet, na een positieve weging, de melding bij de Autoriteit Persoonsgegevens. Ook informeert hij de bestuurder bij een ernstige datalek.

SCHOLENGROEP OPRON heeft schriftelijke afspraken met verwerker(s) over datalekken gemaakt d.m.v. de model bewerkersovereenkomst die hoort bij het convenant “Digitale onderwijsmiddelen en privacy” (www.privacyconvenant.nl).

Werkwijze

De vier rollen

Er zijn tenminste vier rollen die onderscheiden moeten worden om een beveiligingsincident en/of datalek succesvol af te handelen:

1. **Ontdekker (medewerker of leerling)**; degene die het beveiligingsincident of datalek op het spoor komt.

2. **Meldpunt (directeur)**; een aanspreekpunt per school waar alle beveiligingsincidenten worden gemeld.

3. **Melder (Functionaris Gegevensbescherming)**; degene die verantwoordelijk is voor het melden van een datalek bij de Autoriteit Persoonsgegevens en een incidentenregister bijhoudt.

4. **Technicus**; degene die de oorzaak van het datalek kan vinden en kan (laten) repareren.

De 7 stappen

1. Ontdekken

De Ontdekker merkt een beveiligingsincident op. Via eigen waarneming of via waarneming van een derde. De Ontdekker verzamelt zoveel mogelijk informatie over het beveiligingsincident en meldt dit bij de eigen directeur van de school of de zaakgelastigde of contactpersoon van een leverancier van de school.

2. Inventariseren

De directeur zal samen met de melder de vragenlijst in de bijlage zo compleet mogelijk.

3. Beoordelen

Wanneer de vragenlijst is ingevuld, stuurt de directeur deze binnen 24 uur naar de FG fg@opron.nl met het verzoek het datalek te beoordelen. De FG beoordeelt de informatie om te bepalen of een melding aan de Autoriteit persoonsgegevens en de bestuurder vereist is.
De volgende informatie over het datalek wordt vastgelegd door de FG:

- De feiten rondom het datalek en de mogelijke gevolgen van het datalek (de ingevulde vragenlijst).
- Is het datalek gemeld aan de bestuurder? Waarom niet?
- Is het datalek gemeld aan de Autoriteit Persoonsgegevens? Waarom niet?
- De inhoud van de melding.
- Is het datalek gemeld aan de betrokkenen? Waarom niet?

Bij de beoordeling of er sprake is van een 'meldingsplichtig datalek', houdt de FG rekening met het type gegevens, en met de hoeveelheid gegevens. Indien het datalek een risico inhoudt voor de rechten en vrijheden van de betrokkenen wordt er gemeld bij de Autoriteit Persoonsgegevens. De onderstaande beslisboom wordt gebruikt:

4. Beperken gevolgen

De gevolgen worden zoveel mogelijk beperkt. Er wordt gekeken wat de oorzaak van het beveiligingsincident is. De nodige acties voor de aanpak en het verhelpen van de oorzaak worden uitgevoerd.

5. Melden

Indien de conclusie bij stap 3 is dat er melding gedaan moet worden bij de Autoriteit Persoonsgegevens, dan zal de FG dit binnen één werkdag doen. De melding bevat alle verzamelde informatie en de getroffen incidentele en structurele technische en organisatorische maatregelen. Het lek wordt gemeld bij het meldloket datalekken: https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0.

6. Vastleggen

Alle informatie, die in de voorafgaande stappen is ingewonnen of ontstaan, wordt gearchiveerd door de FG waarmee het incident is afgesloten. De FG informeert de directeur van de school over de genomen (te nemen) maatregelen om herhaling te voorkomen.

7. Informeren betrokkene: leerling en/of zijn ouders

Wanneer het datalek waarschijnlijk een hoog risico inhoudt voor de betrokkene(n), dan wordt het datalek ook aan de betrokkene(n) zelf gemeld. Dat zijn medewerkers, leerlingen, of hun ouders als zij jonger zijn dan 16 jaar.

In principe wordt ervan uitgegaan dat het lekken van persoonsgegevens van kinderen altijd van gevoelige aard is en gemeld moet worden bij de betrokkenen.

Als er persoonsgegevens zijn gelekt maar die zijn beveiligd of versleuteld, en de gelekte data zijn volledig onbegrijpelijk of ontoegankelijk voor anderen, dan hoeft dat niet aan betrokkenen te worden gemeld.

Monitoring beveiligingsincidenten en datalekken

De FG maakt twee keer per jaar een analyse van de meldingen van de beveiligingsincidenten en de datalekken. In de analyse wordt ingegaan op eventuele structurele ontwikkelingen, en of de noodzaak bestaat om maatregelen te nemen om herhaling te voorkomen.
De bestuurder wordt door de FG geïnformeerd over de uitkomsten van de analyse.

Aanpassen

Wij behouden ons het recht voor dit protocol aan te passen. Wijzigingen zullen op de website worden gepubliceerd.

Formulier melding datalek

Voor het melden van een datalek vult u onderstaand formulier in. Na invulling kunt u dit formulier als PDF opslaan en als bijlage digitaal zenden naar: fg@opron.nl

Of sturen per gewone post naar:
Scholengroep OPRON
t.a.v. FG
Postbus 138
9640 AC Veendam

0. Over deze melding

Gaat het om een nieuwe of bestaande melding?

0 Nieuw
0 Bestaand, het meldingsnummer is: ……

1. Contactgegevens en overige algemene informatie

Over welke school van de organisatie gaat het?
Naam …….
Adres …….

Wie meldt het datalek?
Naam …….
Functie ……..
E-mailadres ……
Telefoonnummer ……..
Met wie kan de FG contact opnemen voor nadere informatie over de melding?
0 De melder is contactpersoon
0 Er is een andere contactpersoon, te weten:
Naam contactpersoon ……
Functie contactpersoon ……. E-mailadres contactpersoon …….. Telefoonnummer contactpersoon ……..

Was er een andere organisatie betrokken bij de inbreuk?
0 nee
0 ja, namelijk ……

In welke hoedanigheid was de andere organisatie betrokken bij de inbreuk?

……

2. Tijdlijn

Exacte datum waarop de inbreuk was, indien bekend

……

Startdatum van de periode waarbinnen de inbreuk was

……

Einddatum van de periode waarbinnen de inbreuk was

……

Duurt de inbreuk op dit moment nog voort?
0 ja
0 nee

Wanneer werd de inbreuk ontdekt?

…….

Als u de inbreuk later meldt dan 72 uur na de ontdekking, wat is daarvan dan de reden?

……

3. Gegevens over het datalek

Aard van de inbreuk

0 Inbreuk op de vertrouwelijkheid van de gegevens
0 Inbreuk op de integriteit van de gegevens
0 Inbreuk op de beschikbaarheid van de gegevens

Aard van het incident

Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest?
0 Apparaat, gegevensdrager (bijv. USB-stick) en/of papier met persoonsgegevens kwijtgeraakt of gestolen
0 Brief of postpakket met persoonsgegevens kwijtgeraakt of geopend retour ontvangen
0 Hacking, malware (bijv. ransomware) en/of phishing
0 Persoonsgegevens bij oud papier gezet Persoonsgegevens mondeling gedeeld met onbevoegde ontvanger
0 Persoonsgegevens nog aanwezig op afgedankt apparaat of op afgedankte gegevensdrager (bijv. USBstick)
0 Persoonsgegevens per ongeluk gepubliceerd
0 Persoonsgegevens van verkeerde klant getoond in klantportaal
0 Persoonsgegevens verstuurd of afgegeven aan verkeerde ontvanger
0 Anders, namelijk: ……

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest:

4. Persoonsgegevens die betrokken zijn bij het datalek

Persoonsgegevens in het algemeen
0 Naam
0 Geslacht, geboortedatum en/of leeftijd
0 Contactgegevens
0 Toegangs- of identificatiegegevens (bijv. inlognaam, wachtwoord, zaaknummer)
0 Locatiegegevens
0 Onbekend / anders, namelijk: ……

Bijzondere categorieën van persoonsgegevens
0 Persoonsgegevens waaruit iemands ras of etnische afkomst blijkt
0 Persoonsgegevens waaruit iemands politieke opvattingen blijken
0 Persoonsgegevens waaruit iemands religieuze of levensbeschouwelijke overtuigingen blijken
0 Persoonsgegevens waaruit iemands lidmaatschap van een vakbond blijkt
0 Gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid
0 Gegevens over iemands gezondheid
0 Financiële gegevens (bijv. rekeningnummer, creditcardnummer)
0 (Kopieën van) paspoorten of andere legitimatiebewijzen
0 Burgerservicenummer (BSN)
0 Genetische gegevens
0 Biometrische gegevens (vingerafdruk, irisscan, stemherkenning, gezichtsscan)
0 Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen

Hoeveelheid persoonsgegevens
Geef (eventueel bij benadering) aan hoeveel gegevensrecords ("gegevensregisters") zijn getroffen door de inbreuk

……

5. De groep mensen van wie persoonsgegevens betrokken zijn bij het datalek

0 Werknemers
0 Leerlingen
0 Minderjarigen
0 Personen uit kwetsbare groepen

Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk.

……

Van minimaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?

……
Van maximaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?

……

6. Maatregelen die zijn getroffen voordat het datalek plaatsvond

Waren de persoonsgegevens op het moment dat de inbreuk zich voordeed versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk voor onbevoegden?
0 ja
0 nee
0 deels, namelijk:…….

Als de persoonsgegevens deels onbegrijpelijk of ontoegankelijk waren, om welk deel gaat dat dan?

……

Als de persoonsgegevens geheel of deels onbegrijpelijk of ontoegankelijk waren gemaakt, op welke manier is dit dan gebeurd? Geef een zo uitgebreid mogelijke toelichting. Indien u gebruik heeft gemaakt van encryptie, licht dan ook de wijze van versleutelen toe.

……

7. Gevolgen van het datalek

Gevolgen van de inbreuk op de vertrouwelijkheid, de integriteit en/of de beschikbaarheid van de gegevens.
0 Onbevoegden hebben kennis kunnen nemen van de gegevens
0 De gegevens kunnen op een onbehoorlijke of onrechtmatige manier worden gebruikt 0
Er worden binnen uw eigen organisatie mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens gebruikt
0 Er worden mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens hergebruikt voor andere doeleinden of doorgegeven aan andere organisaties
0 Een essentiële dienst kan tijdelijk niet meer worden verleend aan de betrokkenen 0
Een essentiële dienst kan permanent niet meer worden verleend aan de betrokkenen
0 Anders, namelijk ……

Lichamelijke, materiële en immateriële schade voor de betrokkenen
Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkenen?
0 Discriminatie
0 Identiteitsdiefstal of -fraude
0 Financiële verliezen
0 Reputatieschade
0 Verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens
0 Ongeoorloofde ongedaanmaking van pseudonimisering
0 Betrokkenen kunnen hun rechten en vrijheden niet uitoefenen
0 Betrokkenen worden verhinderd controle over hun persoonsgegevens uit te oefenen 0
Andere gevolgen, namelijk: ……..

Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkenen
0 Verwaarloosbaar 0 Beperkt 0 Aanzienlijk 0 Zeer groot

8. Vervolgacties naar aanleiding van het datalek

Informeren van de betrokkenen
Heeft u het datalek gemeld aan de betrokkenen of bent u van plan dat te gaan doen?
0 Ja
0 Nee
0 Nog niet bekend

Wanneer heeft u het datalek gemeld aan de betrokkenen?

……..

Wanneer gaat u het datalek melden aan de betrokkenen?

……..

Wat is de inhoud van de melding aan de betrokkenen? Geef een letterlijke weergave van het bericht aan betrokkenen

……

Hoeveel betrokkenen heeft u geïnformeerd of gaat u informeren?

……

Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken om de betrokkenen te informeren?

……

Waarom ziet u af van het melden van het datalek aan de betrokkenen?
0 De maatregelen die ik heb getroffen voordat het datalek plaatsvond bieden voldoende bescherming om de melding aan de betrokkene achterwege te kunnen laten.
0 Het zou een onevenredige inspanning vergen om iedere betrokkene op individuele basis te informeren.
0 Ik heb na het datalek maatregelen getroffen waardoor het niet langer waarschijnlijk is dat zich daadwerkelijk een hoog risico voor zal doen voor de rechten en vrijheden van de betrokkenen.
0 Anders, namelijk: ……

Licht uw keuze toe

Als het informeren van alle betrokkenen een onevenredige inspanning zou vergen, licht dan toe hoe u door een openbare mededeling of een soortgelijke maatregel de betrokkenen gaat informeren.

……

Welke maatregelen heeft u getroffen waardoor het niet nodig is om de betrokkenen te informeren?

……

Welke andere redenen heeft u om de betrokkenen niet te informeren?

……

Maatregelen om de inbreuk aan te pakken

Welke technische en organisatorische maatregelen heeft uw organisatie getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?

…….

Internationale aspecten

Heeft de inbreuk zich voorgedaan in een grensoverschrijdende gegevensverwerking?
0 Ja
0 Nee

Als er sprake is van een grensoverschrijdende gegevensverwerking, om welke landen gaat het dan?
…….

Heeft uw organisatie of bedrijf, het datalek gemeld bij privacytoezichthouders in een of meer andere EU-landen, of gaat u dat nog doen?
0 Ja, namelijk……
0 Nee

Heeft uw organisatie het datalek gemeld bij Europese toezichthouders op andere meldplichten, of gaat u dat nog doen?
0 Ja, namelijk …….
0 Nee

9. Overig

Is naar uw mening deze melding compleet?
0 Ja, de vereiste informatie is verstrekt en er is geen vervolgmelding nodig
0 Nee, er komt later een vervolgmelding met aanvullende informatie over deze inbreuk **Ondertekening**

Met de ondertekening verklaart u bevoegd te zijn deze melding te doen en dat de in de melding verstrekte informatie juist is.

Handtekening: Datum: