Procedure melden beveiligingsincidenten en datalekken



©Panta Rhei, stichting voor r.k., openbaar en algemeen bijzonder primair onderwijs



Bestuursbureau Panta Rhei
Bezoekadres: Overgoo 13, 2266 JZ Leidschendam
Postadres: Postbus 103, 2270 AC Voorburg
info@stichtingpantarhei.nl
www.stichtingpantarhei.nl

Inhoudsopgave

Inleiding	2
Definities	3
Deel A. Personeelsleden en leerlingen	4
Deel B. ICT Coördinator	6
Deel C. IBP-functionaris	8
Deel D. Communicatiemedewerker	10
Bijlage 1. Meldingsformulier Autoriteit Persoonsgegevens (oktober 2016)	11

1. Inleiding

Deze procedure maakt integraal onderdeel uit van het privacybeleid van de Panta Rhei en is vastgesteld door het college van bestuur.

De procedure bestaat uit 4 onderdelen voor afzonderlijke doelgroepen, te weten:

A. Personeelsleden en leerlingen (meldingen aan ICT-coördinator)

B. ICT-coördinatoren (meldingen aan bovenschoolse IBP-functionaris)

C. IBP-functionaris[1] (meldingen aan Autoriteit Persoonsgegevens)

D. Communicatiemedewerkers (informeren betrokkenen)

Er wordt periodiek (minstens een keer per jaar) gecontroleerd of deze procedure inclusief de onderstaande beschreven stappen adequaat zijn geïmplementeerd.

Waarom deze procedure?

Beveiligingsincidenten kunnen leiden tot informatie en/of gegevens die verloren gaan of onbedoeld gewijzigd worden. Dit kan gevolgen hebben voor de kwaliteit en continuïteit van het onderwijs.

Daarnaast kunnen vertrouwelijke gegevens door beveiligingsincidenten op straat komen te liggen of in verkeerde handen vallen. Voor de verwerking van persoonsgegevens zijn regels vastgelegd in de Wet bescherming persoonsgegevens (Wbp). Het niet zorgvuldig omgaan met vertrouwelijke gegevens kan leiden tot boetes en imagoschade.

Als een beveiligingsincident betrekking heeft op persoonsgegevens, moet er mogelijk binnen 72 uur melding worden gemaakt aan de Autoriteit Persoonsgegevens (voorheen College Bescherming Persoonsgegevens).

Deze procedure is bedoeld voor het snel oplossen van beveiligingsincidenten en, indien nodig, het tijdig melden van datalekken.

[1] Dit is een rol die bovenschools belegd wordt. IBP staat voor informatiebeveiliging en privacy.

2. Definities

Wat is een beveiligingsincident?

Een beveiligingsincident is een gebeurtenis waarbij gegevens:

1. verloren zijn geraakt
2. gestolen zijn
3. beschadigd zijn
4. onbedoeld gewijzigd zijn
5. onrechtmatig toegankelijk zijn voor derden

Wat is een datalek?

Er is sprake van een datalek als er bij een opgetreden beveiligingsincident (verlies of diefstal) persoonsgegevens betrokken zijn.

Wat zijn persoonsgegevens?

Alle gegevens die (evt. gecombineerd met andere gegevens) tot een persoon herleid kunnen worden.

Voorbeelden persoonsgegevens

- Naam
- BSN
- Pasfoto
- Geboortedatum
- Adres
- IP-adres
- Etc.

Deel A. Personeelsleden en leerlingen

Onderstaande teksten zijn opgenomen op de website en intranet van de scholen binnen Panta Rhei en worden regelmatig besproken.

Voor het personeel kan onderstaande tekst worden gebruikt hoe zij om moeten gaan bij computerproblemen.

Computerproblemen? Meld ze direct!

Als er problemen zijn met een computer, software of de website van *<naam school>* dan moet je dit zo snel mogelijk melden bij de ICT-coördinator.

Bij problemen moet je bijvoorbeeld denken aan een pc die niet opstart, een softwareprogramma die je niet kunt gebruiken, maar ook gestolen computers of opslagmedia, virussen en kwijtgeraakte logingegevens (zie kader belangrijke tips). Zeker wanneer je eigen gegevens of die van andere leerlingen of personeelsleden zijn kwijtgeraakt of toegankelijk zijn voor anderen, moet dit zo snel mogelijk worden gemeld!

Wanneer je merkt dat computers of smartphones op school voor de verkeerde zaken gebruikt worden. Of je ziet informatie of gegevens die je niet mag zien, meld dit dan zo snel mogelijk bij de ICT-coördinator.

Op deze manier hopen we op *<naam school>* veilig en probleemloos met ICT te kunnen werken. Klik hier voor meer informatie *<hyperlink>* over hoe wij omgaan met privacy en zorgen voor een veilig schoolklimaat.

Onderstaande informatie wordt gebruikt voor de leerlingen en wordt regelmatig onder de aandacht gebracht.

Computerproblemen? Meld ze direct!

Als er problemen zijn met een computer, software of de website van *<naam school>* dan moet je dit zo snel mogelijk melden bij je meester of juf.

Bij problemen moet je bijvoorbeeld denken aan een pc die niet opstart, een softwareprogramma die je niet kunt gebruiken, maar ook gestolen computers of opslagmedia, virussen en kwijtgeraakte logingegevens. Zeker wanneer je eigen gegevens of die van andere leerlingen zijn kwijtgeraakt of toegankelijk zijn voor anderen, moet dit zo snel mogelijk worden gemeld!

Wanneer je merkt dat computers of smartphones op school voor de verkeerde zaken gebruikt worden. Of je ziet informatie of gegevens die je niet mag zien, meld dit dan zo snel mogelijk bij je meester of juf.

Op deze manier hopen we op *<naam school>* veilig en probleemloos met ICT te kunnen werken.

Onderstaand een aantal voorbeelden en tips die gecommuniceerd worden binnen de school.

Voorbeelden incidenten

- computer of software die niet werkt of bruikbaar is
- kwijtgeraakte USB-stick
- gestolen laptop
- inbraak door een hacker
- DDOS aanval
- malware- of virusbesmetting
- gestolen logingegevens
- onbeveiligde serverruimte.

Nog 3 belangrijke tips:

1. Deel je logingegevens nooit met anderen en laat ze niet meekijken.
2. Als je een link in je mail niet vertrouwt, klik er dan niet op.
3. Mocht je computer besmet zijn met een virus, sluit de computer dan zo snel mogelijk af en verbreek de internet- of netwerkverbinding, om besmetting te voorkomen.

Deel B. ICT-coördinator

Dit onderdeel is ook opgenomen is in het ICT-beleidsplan voor de ICT-coördinator op scholen.

Stap 1 - Inventariseer en registreer

Indien er een melding wordt gedaan van een beveiligingsincident, dan worden de volgende gegevens geregistreerd:

- Naam:
- Datum:
- Tijdstip:
- Omschrijving incident:
- Soort gegevens:
- Omvang gegevens: (aantal personen)
- Betrokkenen:
- Locatie:
- Type hardware (tagcode):
- Naam software:
- Prioriteit: (indien datalek: hoog)
- Backup aanwezig?: ja/nee
- Zijn de gegevens geëncrypt?: ja/nee

Stap 2 - Analyseer en beoordeel (binnen 8 uur na melding)

Heeft de melding betrekking op persoonsgegevens?
Meld dit direct via privacy@stichtingpantarhei.nl

Is er sprake van opzettelijk misbruik of strafbare feiten, zoals diefstal, hacken of DDOS?
Neem (ook) contact op met de schooldirecteur in verband met te nemen sancties en/of het doen van aangifte.

Stap 3 – Neem herstelmaatregelen

Is er sprake van diefstal, verlies of beschadiging?
Dan moet het systeem vervangen worden en/of de backup teruggeplaatst worden (indien aanwezig). Neem hiervoor contact op met de ICT-leverancier van de school.

Is er sprake van onrechtmatige toegang?
Dan dient de toegang afgesloten te worden door fysieke beveiliging, een wijziging in de configuratie van het netwerk of in de accounts van computers, netwerkapparatuur of applicaties, zoals wachtwoorden. Pas dit zelf aan de software of neem hiervoor contact op met de ICT-leverancier en/of ICT-netwerkbeheerder van de school.

Is er sprake van DDOS aanval op servers die in beheer zijn van de school?
Dan dient relevante netwerkapparatuur afgesloten of opnieuw geconfigureerd te worden, eventueel in overleg met leveranciers of externe beheerders. Neem hiervoor contact op met de ICT-leverancier van de school of de leverancier van het betreffende softwarepakket.

Is er sprake van malware of anti-virus aanvallen?
Dan dient de computer of apparatuur uit het netwerk genomen, opgeschoond en hersteld te worden. Indien nodig dienen backups teruggeplaatst te worden. Neem hiervoor contact op met de ICT-leverancier van de school.

Stap 4 – Neem preventieve maatregelen en registreer deze bij de melding

De melding kan pas afgesloten worden als de herstelmaatregelen zijn uitgevoerd en er preventieve maatregelen zijn genomen en beschreven om het risico op toekomstige incidenten te vermijden of te verkleinen.

De herstelmaatregelen en preventieve maatregelen worden geregistreerd bij de melding.

N.B. De registratie van meldingen wordt meegenomen in de periodieke evaluatie van het privacy beleid van Panta Rhei. In de evaluatie wordt ingegaan op eventuele structurele ontwikkelingen, en of de noodzaak bestaat om maatregelen te nemen om herhaling te voorkomen.

Deel C. IBP-functionaris

De IBP-functionaris is een rol die op bovenschools niveau is belegd en belast is met onder andere de volgende taken en verantwoordelijkheden:

- (Laten) uitvoeren risicoanalyses.
- (Laten) opstellen / bijwerken beleidsplan.
- (Laten) opstellen, evalueren en controleren jaarplan.
- Rapporteren (relevante) incidenten en datalekken aan College van Bestuur.

Stap 1 - Controleer en registreer

Controleer of al gegevens zijn geregistreerd over het beveiligingsincident. Vul deze registratie aan met de informatie die uit de volgende stappen naar voren komt.

Stap 2 – Bepaal of er sprake is van een datalek (binnen 8 uur na melding)

Zijn er bij het incident persoonsgegevens verloren gegaan?
Er is geen kopie of backup aanwezig van de persoonsgegevens.

Is er bij het incident sprake van onrechtmatige verwerking van persoonsgegevens? En kan dit niet uitgesloten worden?
Onbevoegden hebben onrechtmatig toegang kunnen krijgen tot de persoonsgegevens.

Indien Ja op één beide → Ga naar stap 3.
Indien Nee op beide → Er is geen sprake van een datalek, overleg met systeembeheer over preventieve maatregelen.

N.B. Schakel indien nodig een externe deskundige in en informeer de betrokken leverancier(s)! Zie bewerkersovereenkomst voor de afspraken in het kader van datalekken met leveranciers.

Stap 3 – Bepaal of er sprake is van meldplicht

Zijn er persoonsgegevens van gevoelige aard gelekt of leidt de aard en omvang van de inbreuk tot (een aanzienlijke kans op) ernstige nadelige gevolgen?

Indien Ja → Ga naar stap 4.
Indien Nee → Er is geen sprake van meldplicht, overleg met systeembeheer over preventieve maatregelen.

Gegevens van gevoelige aard:
Godsdienst of levensovertuiging, ras, politieke gezindheid, ras, gezondheid, seksuele leven, lidmaatschap vakvereniging, strafrechtelijke gegevens of over onrechtmatig of hinderlijk gedrag, financiële gegevens of over de economische situatie, gegevens die kunnen leiden tot stigmatisering (schoolprestaties, relatieproblemen), gebruikersnamen en wachtwoorden, gegevens die kunnen worden gebruikt bij identiteitsfraude (BSN)

Nadelige gevolgen:
Misbruik in het criminele circuit van grote databestanden, ingrijpende beslissingen die op basis van (gewijzigde) gegevens worden genomen, gevolgen die binnen ketens van gegevensverwerking kunnen optreden.

Stap 4 – Informeer het college van bestuur en bepaal of betrokkenen ook geïnformeerd dienen te worden.

Ontbreken er technische beschermingsmaatregelen waardoor het datalek (waarschijnlijk) nadelige gevolgen kan hebben voor leerlingen, ouders of personeel?
De gegevens zijn niet voorzien van encryptie of de encryptie is verouderd.

Indien Ja → Ga naar de volgende vraag.
Indien Nee → Ga naar stap 5 en informeer het college van bestuur.

Zijn er zwaarwegende redenen om de melding aan leerlingen, ouders of personeel achterwege te laten?
Het informeren van de leerlingen, ouders of personeel kan negatieve gevolgen hebben voor de veiligheid van anderen.

Indien Ja → Ga naar stap 5 en informeer het college van bestuur.
Indien Nee → Ga naar stap 5 en informeer het college van bestuur en de communicatiemedewerker. (Zie deel D procedure Melden beveiligingsincidenten en datalekken.)

Stap 5 – Meld het datalek bij de Autoriteit (binnen 72 uur na melding)

Verzamel alle benodigde informatie (zie bijlage 1 voor vragenlijst).

Na toestemming van het college van bestuur wordt door de IBP-functionaris een melding gedaan via http://datalekken.autoriteitpersoonsgegevens.nl of (indien de website niet beschikbaar is) via faxnummer 070 - 888 85 01.

De melding wordt minimaal 3 jaar bewaard. Informeer indien nodig de leverancier over de melding.

Deel D. Communicatiemedewerker

Dit onderdeel is opgenomen in het procedurehandboek van de communicatiemedewerker.

Informeer de betrokkenen (binnen 1 week na melding) via de daarvoor vastgestelde communicatiemiddelen indien er sprake is van een datalek.

De communicatiemedewerker wordt van een datalek op de hoogte gesteld door de IBP-functionaris. Deze verstrekt ook de benodigde gegevens ten behoeve van de communicatie.

In de kennisgeving aan de betrokkene wordt in ieder geval vermeldt:

> Een algemene omschrijving van de aard van de incident, de contactgegevens om meer informatie over de inbreuk te verkrijgen, en de maatregelen die genomen zijn en/of door betrokkene genomen moeten worden om negatieve gevolgen te beperken.

Bij grootschalige datalekken dient er ook een persbericht in overleg met het college van bestuur opgesteld te worden.

Bijlage 1 – Meldingsformulier Autoriteit Persoonsgegevens (oktober 2016)

1. Is dit een vervolg op een eerdere melding? Zo ja, Wat is het nummer van de oorspronkelijke melding?
2. Wat is de strekking van de vervolgmelding? Zo ja, Wat is daar de reden voor?
3. Op grond van welke wettelijke bepaling doet u deze melding?
4. Naam van het bedrijf of de organisatie
5. Adres locatie
6. Postcode
7. Plaats
8. KvK-nummer
9. Naam van de persoon die meldt
10. Functie van de persoon die meldt
11. E-mailadres van de persoon die meldt
12. Telefoonnummer van de persoon die meldt
13. Alternatief telefoonnummer van de persoon die meldt
14. In welke sector is het bedrijf of de organisatie actief?
15. Geef een samenvatting van het incident waarbij de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan.
16. Van hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?
17. Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk.
18. Wanneer vond de inbreuk plaats? (Kies een van de volgende opties en vul waar nodig aan.)
19. Wat is de aard van de inbreuk? (U kunt meerdere mogelijkheden aankruisen.)
20. Om welk type persoonsgegevens gaat het? (U kunt meerdere mogelijkheden aankruisen.)
21. Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkenen? (U kunt meerdere mogelijkheden aankruisen.)
22. Welke technische en organisatorische maatregelen heeft uw organisatie getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?
23. Heeft u het datalek gemeld aan de betrokkenen of bent u van plan dat te gaan doen?
24. Wanneer heeft u het datalek gemeld aan de betrokkenen, of wanneer gaat u dit doen?
25. Wat is de inhoud van de melding aan de betrokkenen? (Letterlijke weergave, beantwoord deze vraag als de eerste vraag met “ja” is beantwoord.)
26. Hoeveel betrokkenen heeft u in kennis gesteld of gaat u in kennis stellen? (Beantwoord deze vraag als de 1e vraag met “ja” is beantwoord.)
27. Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken bij het in kennis stellen van de betrokkenen? (Beantwoord deze vraag als de 1e vraag met “ja” is beantwoord.)
28. Waarom ziet u af van het melden van het datalek aan de betrokkenen? (Beantwoord deze vraag als de 1e vraag met “nee” is beantwoord.)
29. Zijn de persoonsgegevens versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden?

30. Als de persoonsgegevens geheel of deels onbegrijpelijk of ontoegankelijk zijn gemaakt, op welke manier is dit dan gebeurd? (Beantwoord deze vraag als de vorige vraag beantwoord is met “ja” of “deels”. Als u gebruik heeft gemaakt van encryptie, licht dan ook de wijze van versleutelen toe.)
31. Heeft de inbreuk betrekking op personen in andere EU-landen?
32. Heeft uw bedrijf of organisatie het datalek gemeld bij toezichthouders in een of meer andere EU-landen?
33. Is naar uw mening deze melding compleet?