Procedure datalekken

NoorderBasis

noorder Basis
scholen met de bijbel

Inleiding

Deze procedure maakt integraal onderdeel uit van het privacy beleid van NoorderBasis en is vastgesteld door het bestuur.

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

E1. Medewerkers en leerlingen
E2. Schoolse ICT-coördinator of schoolleider
E3. Functionaris Gegevensbescherming (FG) / Privacy Officer
E4. Communicatie

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 Algemene Verordening Persoonsgegevens (AVG). 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.

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 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 E1.
Medewerkers en leerlingen

Persoonsgegevens gelekt? Meld ze direct!
Als er sprake is van gestolen computers of opslagmedia, virussen of kwijtgeraakte logingegevens waardoor persoonsgegevens toegankelijk zijn voor anderen, meld dit dan zo snel mogelijk bij de directie van de school.

Voorbeelden
- 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:
- Deel je logingegevens nooit met anderen en laat ze niet meekijken.
- Als je een link in je mail niet vertrouwt, klik er dan niet op.
- 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 E2.
Schoolse ICT-coördinator of schoolleider

Stap 1 - Analyseer en beoordeel (binnen 8 uur na melding)
Heeft de melding betrekking op persoonsgegevens?
Meld dit direct via privacy@noorderbasis.nl .
Is er sprake van opzettelijk misbruik of strafbare feiten, zoals diefstal, hacken of DDOS?
Denk ook na over evt. uit te voeren sancties en/of het doen van aangifte.

Stap 2 - 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 vermoeden van datalek: hoog)
Back-up aanwezig?: ja/nee
Zijn de gegevens geëncrypt?: ja/nee

Stap 3 - Neem herstelmaatregelen (door de bovenschoolse ICT-er!)
Is er sprake van diefstal, verlies of beschadiging?
Dan moet het systeem vervangen worden en/of de back-up teruggeplaatst worden (indien aanwezig). Neem hiervoor contact op met de ICT van NoorderBasis.

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 in de software of neem hiervoor als ICT-coördinator contact op met de ICT-leverancier van de school.

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

Is er sprake van malware of antivirus aanvallen?
Dan dient de computer of apparatuur uit het netwerk genomen, opgeschoond en hersteld te worden. Indien nodig dienen back-ups teruggeplaatst te worden. Neem hiervoor contact op met de ICT van NoorderBasis.

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.
De registratie van meldingen wordt meegenomen in de periodieke evaluatie van hetprivacy beleid van NoorderBasis. In de evaluatie wordt ingegaan op eventuele structurele ontwikkelingen en of de noodzaak bestaat om maatregelen te nemen om herhaling te voorkomen.

Deel E3.
Functionaris Gegevensbescherming (FG)

Dit onderdeel is opgenomen in het handboek van de bovenschoolse Functionaris Gegevensbescherming (FG). Dit betreft 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 directeur/bestuurder.

Binnen NoorderBasis is afgesproken dat de Functionaris Gegevensbescherming hierin samenwerkt met de Privacy Officer.

Stap 1 - Controleer en registreer
Controleer of alle 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)
Vraag 1
Zijn er bij het incident persoonsgegevens verloren gegaan?
Is er een kopie of back-up aanwezig van de persoonsgegevens?

Vraag 2
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 van beide, ga naar stap 3
Indien Nee op beide: er is geen sprake van een datalek, er wordt nagedacht over preventieve maatregelen.

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

Stap 3 - Bepaal of er sprake is van meldplicht
Vraag 3
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 en er is geen sprake van meldplicht, overleg met systeembeheer over preventieve maatregelen

Gegevens van gevoelige aard:
Godsdienst of levensovertuiging, ras, politieke gezindheid, 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 bestuur en bepaal of betrokkenen ook geïnformeerd dienen te worden.
Vraag 4
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.

Vraag 5
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 bestuur.
Indien Nee, ga naar stap 5 en informeer het bestuur.
(zie deel D procedure Melden beveiligingsincidenten en datalekken).

Stap 5 - Meld het datalek bij de Autoriteit Persoonsgegevens (binnen 72 uur na melding)
Verzamel alle benodigde informatie (zie bijlage A voor vragenlijst).

Na toestemming van het bestuur wordt door de Functionaris Gegevensbescherming een melding gedaan bij de Autoriteit Persoonsgegevens.

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

Deel E4.
Communicatie

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

In de kennisgeving aan de betrokkene wordt in ieder geval vermeld:
Een algemene omschrijving van de aard van het 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 door de bestuurder opgesteld te worden.