Notitie Informatiebeveiliging en Privacy

10 november 2016

Van: Arnold Dik, bovenschools ICT-coördinator
Aan: bestuur en leden RvT OPRON

1 Inleiding

Binnen het primair onderwijs wordt steeds vaker en intensiever gebruik gemaakt van digitale informatie. Binnen deze informatie is ook sprake van vertrouwelijke gegevens, zoals persoonsgegevens. Het is van groot belang dat er met vertrouwelijke gegevens zorgvuldig wordt omgegaan, om privacy van kinderen, ouders, verzorgers, en medewerkers te waarborgen.

Hiervoor zijn regels vastgelegd in de Wet Bescherming Persoonsgegevens (Wbp). In deze wet staat o.a. dat organisaties de persoonsgegevens die het verwerkt moet beveiligen tegen verlies en tegen onrechtmatige verwerking (artikel 13, Wbp). Één specifiek onderdeel van deze wet is de Meldplicht Datalekken (artikel 34a, Wbp). Op 1 januari 2016 is deze meldplicht ingegaan.

Deze meldplicht houdt in dat organisaties (zowel bedrijven als overheden) direct een melding moeten doen bij de Autoriteit Persoonsgegevens, zodra zij een ernstig datalek hebben. En in een aantal gevallen moeten zij het datalek ook melden aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt).

In deze notitie staat welke acties we als OPRON ondernemen om invulling te geven aan Informatiebeveiliging en Privacy, en de meldplicht datalekken in het bijzonder.

2 Soorten gegevens en informatie

In de Wbp gaat het over persoonsgegevens. Dat zijn alle gegevens waarmee direct of indirect een natuurlijk persoon (mens) kan worden geïdentificeerd. Het kan dan bijvoorbeeld gaan om een naam, BSN, geboortedatum of telefoonnummer.
Leerlinggegevens zijn ook persoonsgegevens, waarop de Wbp van toepassing is. Leerlinggegevens kunnen gevoelige informatie bevatten, zoals informatie over gedragsproblemen, gezondheid, levensbeschouwing, geaardheid of thuissituatie. Deze gevoelige persoonsgegevens worden bijzondere persoonsgegevens genoemd. Deze mogen alleen worden vastgelegd als hiervoor een noodzaak bestaat.
Scholen en besturen zijn verantwoordelijk voor het vaststellen van welke (persoons)gegevens gebruikt worden en wat het doel daarvan is. De Wbp heeft als uitgangspunt dat “het bevoegd gezag” eindverantwoordelijk is voor de privacy van leerlingen.

Alle betrokkenen binnen OPRON en onze scholen dienen te weten waar privacy over gaat en wat onze uitgangspunten hierin zijn. We stellen een privacyreglement op dat gebaseerd is op de wettelijke kaders van de Wbp.

Leerlinggegevens worden in toenemende mate gebruikt in combinatie met informatiesystemen die "buiten de school" staan. Denk hierbij aan:

- Leerlingvolgsystemen;
- Basispoort;
- Digitaal (adaptief) lesmateriaal;
- Toets- en oefenprogramma's.

Dit is toegestaan mits dit aantoonbaar bijdraagt aan de onderwijs- en ontwikkeldoelen en de juridische spelregels worden vastgelegd in een bewerkersovereenkomst tussen school / bestuur en leverancier.

We stellen bewerkersovereenkomsten op met alle externe partijen die gebruik maken van leerlinggegevens.

We moeten ouders en verzorgers op de hoogte brengen van:

- waar leerlinggegevens voor gebruikt worden;
- om welke soorten gegevens het gaat;
- Wat wij doen om privacy van leerlinggegevens te waarborgen;
- Wat ouders / verzorgers zelf kunnen doen om de privacy van hun kinderen te beschermen.

Hier zullen we transparant en actief de ouders over informeren. Op de onderdelen waar toestemming nodig is van ouders, zullen we periodiek de ouders hier om vragen.

Dit betreft niet alleen gegevens in de vorm van data, maar ook films en foto's (portretrecht en auteursrecht, schoolfoto's, films van een schoolreisje) en de relatie met social media.

We maken afspraken met ouders en verzorgers over het gebruik van leerlinggegevens

Privacy en bescherming van de persoonlijke sfeer geldt uiteraard ook in het klaslokaal. De aanwezigheid van social media, de laagdrempeligheid hiervan en het belang is sterk toegenomen. Vaak hebben scholen hiervoor al een initiatief opgestart (mediawijsheid). Dit gaan we toetsen in het licht van de Wbp. Daar waar nodig is, zal het bestaande protocol van de school aangevuld worden.

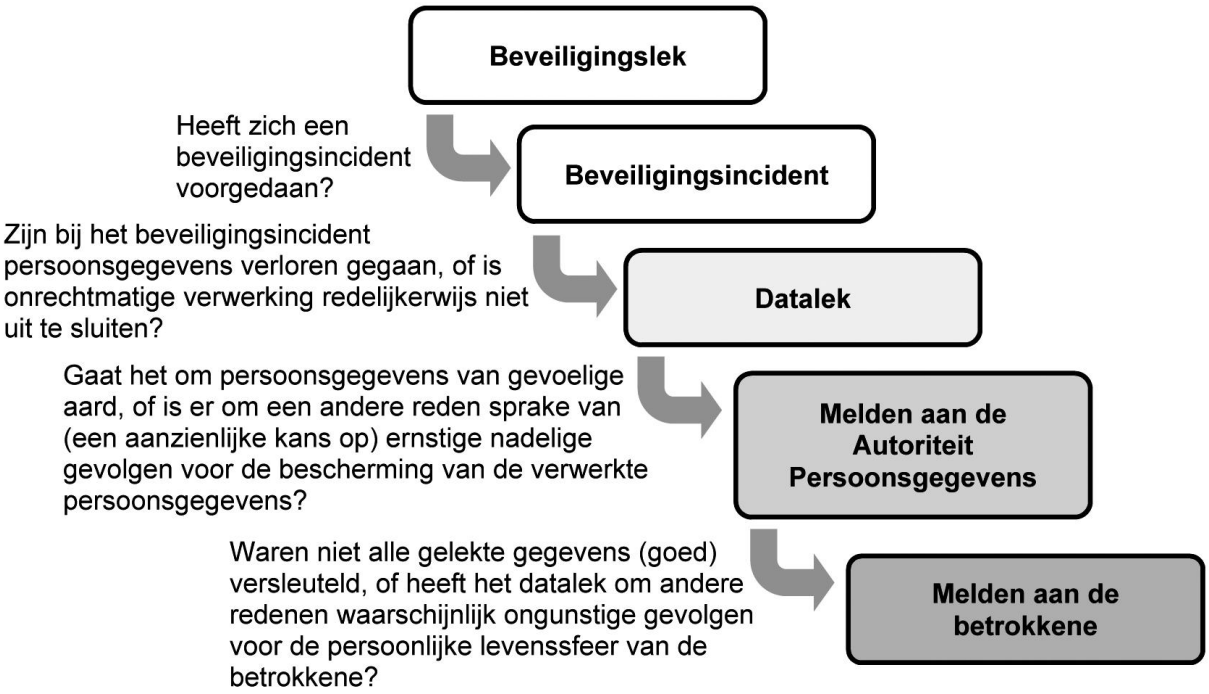
We informeren leerlingen over het belang van privacy en maken afspraken hierover (voor zover dat nog niet gedaan is)

3 Datalekken

Vanwege het belang van de bescherming van de persoonlijke levenssfeer is de Wbp en de meldplicht datalekken in het leven geroepen.

> *Bij een datalek gaat het om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van deze organisatie. Onder een datalek valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook onrechtmatige verwerking van gegevens.*
>
> *We spreken van een datalek als er een inbreuk is op de beveiliging van persoonsgegevens (zoals bedoeld in artikel 13 van de Wet bescherming persoonsgegevens). Bij een datalek zijn de persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking – dus aan datgene waartegen de beveiligingsmaatregelen bescherming moeten bieden.*

Er is een verschil tussen een beveiligingslek (een zwakke plek in de informatiebeveiliging) en een datalek. Of er daadwerkelijk sprake is van een datalek, is afhankelijk van een aantal afwegingen:



Een *beveiligingslek*, zoals de post-it naast de monitor met daarop gebruikersnaam en wachtwoord voor ESIS, kan leiden tot een *beveiligingsincident*.

Enkele voorbeelden van beveiligingsincidenten die tot datalekken kunnen leiden:

- Het kwijtraken van een USB-stick;
- Verlies of diefstal van een laptop;
- Inbraak door een hacker

Niet ieder beveiligingsincident is een datalek. Er is sprake van een datalek als er bij het beveiligingsincident persoonsgegevens verloren zijn gegaan, of als onrechtmatige verwerking van persoonsgegevens niet uitgesloten kan worden.

Niet elk datalek hoeft gemeld te worden. Dit is alleen nodig als er ernstige nadelige gevolgen voor de bescherming van persoonsgegevens (kunnen) optreden. Dit is afhankelijk van meerdere factoren:

- Aard van de persoonsgegevens (gevoeligheid)
- De hoeveelheid gelekte persoonsgegevens
- Aantal betrokkenen

3.1 Sancties

Bij overtreding van de meldplicht datalekken uit de Wbp kan de Autoriteit Persoonsgegevens een bestuurlijke boete opleggen. Deze bestuurlijke boete bedraagt ten hoogste het bedrag van de zesde categorie van artikel 23, vierde lid, van het Wetboek van Strafrecht. Dat is per 1 januari 2016 maximaal 820.000 euro. Indien de overtreding niet opzettelijk is gepleegd en er geen sprake is van ernstig verwijtbare nalatigheid, dan zal de Autoriteit Persoonsgegevens eerst een bindende aanwijzing opleggen voorafgaand aan eventuele oplegging van een bestuurlijke boete. Bij het opleggen van een bestuurlijke boete houdt de Autoriteit Persoonsgegevens rekening met alle omstandigheden van het geval. Een omstandigheid van het geval kan bestaan uit het feit dat de gegevens waarover het gaat niet door derden zijn ingezien.

3.2 Maatregelen

Binnen OPRON worden, naast de eerder genoemde acties rondom privacy, de volgende maatregelen uitgevoerd om te voldoen aan de meldplicht datalekken en de eisen die de wet ons stelt:

- Er komt een bij OPRON passende “gegevensbeveiligingsorganisatie” inclusief de daarbij horende rollen. Dit houden we compact. Van belang is dat bij een beveiligingsincident het helder is wie welke rol op zich neemt;
- De beveiligingsrisico’s worden in kaart gebracht, inclusief impact. Op basis daarvan worden passende (organisatorische en technische) maatregelen genomen;
- Er wordt een procedure opgesteld voor het behandelen van gegevensbeveiligingsincidenten. Hierin staat hoe we de incidenten beoordelen, welke gradaties we hanteren en hoe we dit melden aan de Autoriteit persoonsgegevens en de betrokkene;
- Alle medewerkers worden geïnformeerd over de meldplicht datalekken en de opgestelde werkwijze en maatregelen.

3.3 Tijdpad

Nov 2016	Bespreken notitie in RvT
Dec 2016	Vaststellen notitie door het bestuur, kennisstellen in RvT en GMR. Bespreken notitie in GMR en directieberaad
Jan 2017	Inrichten actieteam
Vanaf Jan 2017	Gezamenlijke uitrol van de maatregelen

Bronnen:

- “Omgaan met data in het onderwijs”, Kennisnet, januari 2016
- PO raad, website
- www.autoriteitpersoonsgegevens.nl
    - Richtsnoer meldplicht datalekken in de Wbp
- “portretrecht en auteursrecht”, Kennisnet, website