



Deel 3: Hoe voorkom je een datalek?



De AVG, informatiebeveiliging en privacy (IBP) - veelgehoorde termen, maar wat moet en kun je er eigenlijk mee op het Nuborgh College? In acht IBP-berichten met animatiefilmpjes ben je helemaal up-to-date! In deel 3: datalekken.

Klik op het puzzelstukje voor een korte introductie!

Waarom moet ik iets weten over datalekken?

In de vorige IBP-berichten heb je ontdekt wat de AVG en IBP inhouden en dat we persoonsgegevens goed moeten beschermen. Dat betekent ook dat we ervoor zorgen dat deze niet in verkeerde handen vallen.

Wanneer dat wel gebeurt, dan spreken we van het 'lekken' van persoonsgegevens. In dat geval hebben we de verplichting om een datalek te melden bij de Autoriteit Persoonsgegevens (AP) - deze meldplicht datalekken geldt voor alle organisaties, dus ook voor het Nuborgh College.

In sommige gevallen moet het datalek ook gemeld worden bij de betrokkenen - degenen van wie de persoonsgegevens zijn 'gelekt'.

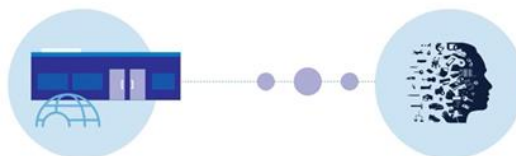
Een datalek, wat is dat eigenlijk?

Een datalek is een inbreuk op de informatiebeveiliging waarbij persoonsgegevens verloren gaan of in handen komen van derden die geen toegang tot die gegevens mogen hebben.

Dat is soms lastig vast te stellen, daarom is de bewijslast omgedraaid. Het is dus een datalek als toegang door onbevoegden niet uitgesloten kan worden.

Datalek ontdekt? Meld het!

Je ontdekt, veroorzaakt of vermoed een datalek - waar moet je dit melden? Dit kan bijvoorbeeld via het daarvoor bestemde e-mailadres privacy@nuborgh.nl of bij je directe leidinggevende. In de gedragscode van de school staat dit precies beschreven. Maak altijd melding van een (mogelijk) datalek! We gaan dan kijken hoe het lek is ontstaan en hoe we het in toekomst kunnen voorkomen. Met de juiste maatregelen kunnen we daarna (verdere) schade beperken. Als schoolbestuur moeten we een datalek direct (liefst binnen 72 uur) melden aan de Autoriteit Persoonsgegevens.



Wat is bijvoorbeeld een datalek?

- Het verlies van een usb-stick of laptop met daarop persoonsgegevens van leerlingen of medewerkers.
- Het verlies van een smartphone. Deze kan mogelijk toegang geven tot veel informatie, zoals de gesynchroniseerde e-mail van school, notities of een automatische inlog in schoolsystemen.
- 'Offline' datalekken zoals documenten met persoonsgegevens in de papierbak, leerlingverslagen op het bureau of meegenomen dossiers uit een kwijtgeraakte tas.
- Een computer thuis, die gehackt of gestolen wordt waarop bijvoorbeeld een Excelbestand met leerlinggegevens staat. Gehackte bestanden, een DDoS-aanval of inbraak in een databestand.
- Een e-mail met persoonsgegevens verstuurd naar de verkeerde persoon of personen.

Meer weten over hoe een DDoS-aanval werkt en wat je er tegen kunt doen? Bekijk het dossier '[DDoS-aanval op school](#)' van Kennisnet.

De AVG en datalekken in de praktijk

Het is niet de vraag of wij te maken krijgen met een datalek, maar eerder wanneer. Met technische maatregelen kunnen we veel datalekken voorkomen, maar de menselijke factor blijft altijd belangrijk. Iedereen heeft de verantwoordelijkheid om bewust en zorgvuldig met persoonsgegevens om te gaan.

We hebben afspraken over het veilig werken met persoonsgegevens, vastgelegd in een gedragscode. Hiermee kunnen we samen het risico op datalekken beperken. Waar moet je bijvoorbeeld op letten?

- Verstuur geen persoonsgegevens per e-mail, WhatsApp of andere sociale media. Niet mailen, maar delen!
- Beveilig apparatuur met een wachtwoord en vergrendel je pc als je even weg gaat.
- Vraag geen toegang tot meer gegevens dan je voor je werk nodig hebt.
- Laat je devices buiten de school nooit onbeheerd achter, ook niet in een auto die op slot zit.
- Sla persoonsgegevens niet op op je eigen pc, laptop of telefoon.
- Houd je school-mail en privé-mail gescheiden.

Dat klinkt allemaal logisch, maar vraagt wel om meer alertheid. Help elkaar om hier aan te denken. Zo kunnen we er samen voor zorgen dat persoonsgegevens veilig blijven - zowel van leerlingen, ouders, medewerkers als directieleden en bestuurder.

[Klik hier voor '6x zorgvuldig'](#)

Ieder datalek kan grote nadelige gevolgen hebben voor leerlingen (en hun ouders), medewerkers, maar ook voor onze school. Datalekken kunnen rekenen op flinke (negatieve) media-aandacht en veroorzaken imagoschade. Daarnaast staan er hoge boetes op datalekken of het niet tijdig melden ervan.



Als medewerker van het Nuborgh College vraagt dit van ons dat we weten:

- Wat een datalek is en welke afspraken er binnen het Nuborgh College zijn om het risico daarop te verkleinen.
- Dat we een (mogelijk) datalek altijd moeten melden via het afgesproken e-mailadres privacy@nuborgh.nl of aan de directe leidinggevende.
- Wat de gevolgen kunnen zijn als we bijvoorbeeld onze school-mail synchroniseren met een ander apparaat. We weten welke stappen we moeten en kunnen nemen bij het verlies van het device.

Sleutelwoorden deel 3: Meldplicht, datalek, afspraken e-mail en gebruik persoonsgegevens

Vragen? Stel ze via privacy@nuborgh.nl.

[De volgende keer: sociale media](#)



Informatiebeveiliging en privacy goed geregeld op het Nuborgh College