

## Gebruikersvoorwaarden-privacybijlage

Per 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. Deze wet heeft als doel gebruikers meer controle te geven over zijn of haar persoonsgegevens.

*Onderwijsinstellingen maken in toenemende mate gebruik van digitale toepassingen binnen het onderwijs. Bij het gebruik en levering van deze producten en diensten zijn gegevens nodig die te herleiden zijn tot personen (zoals leerlingen). Scholen moeten met Verwerkers afspraken maken over het gebruik van die Persoonsgegevens. Deze gebruikersvoorwaarden geven scholen informatie over de dienstverlening die Verwerker verleent en welke persoonsgegevens de Verwerker daarbij verwerkt. Alles bij elkaar eigenlijk over de vraag "wie, wat, waar, waarom en hoe" wordt omgegaan met de privacy van de betrokken personen wiens gegevens worden uitgewisseld. Het gebruik van deze Privacy Bijsluiter helpt Onderwijsinstellingen en gebruikers om beter te begrijpen wat de werking van het product en/of dienst is en welke gegevens daarvoor worden uitgewisseld.*

**VO-next werkt met persoonsgegevens en verwerkt ook persoonsgegevens van gebruikers (zoals naam, e-mailadres en naam school). Deze gegevens zijn noodzakelijk om gebruik te maken van de producten en diensten van VO-next. In deze gebruikersvoorwaarden leest u wat we doen om uw gegevens te beschermen.**

### A. Algemene informatie

Naam product en/of dienst : VO-next platform  
Naam Verwerker en vestigingsgegevens : VO-next  
Coehoornsingel 6  
7201 AB ZUTPHEN

Beknorte uitleg en werking product en dienst:

**VO-next platform** levert een online leeromgeving.

De leeromgeving biedt de mogelijkheid om leertrajecten (taken-toetsen) uit te zetten en vorderingen van leerlingen hierop te volgen. De basis voor de leertrajecten kunnen de Stercollecties van VO-content zijn, maar ook zelfontworpen leermateriaal of materiaal van derden.

Links naar website VO-next:

VO-next algemeen : <https://www.vo-next.nl>  
VO-next dashboard : <https://www.vo-next.nl/dashboard>

Via het dashboard van VO-next wordt er ook gelinkt naar websites van VO-content:

Eindexamensite, Rekenite, Oefenprogramma Engels en Portfolio-site. Dit zijn webapplicaties waarmee leerlingen zich respectievelijk kunnen voorbereiden op het eindexamen en om rekenen en Engels te oefenen op eigen tempo. Met portfolio-site.nl laat de leerling zien welke producten en opdrachten gemaakt zijn.

Links naar websites derden (VO-content):

Rekenite : <https://www.rekenite.nl/rekenen/>  
Oefenprogramma Engels : <https://www.oefenprogrammaengels.nl/read-and-listen/>  
Portfolio : <https://www.portfolio-site.nl>  
Eindexamensite : <https://www.eindexamensite.nl>  
Docentenmateriaal : <https://vo-content.azurewebsites.net/docent-vo-content/set/docentenmateriaal-vo-content/8356>

Doelgroep : voortgezet onderwijs  
Gebruikers : leerlingen/docenten

## B. De specifieke diensten

Omschrijving van de specifiek verleende diensten en bijbehorende Verwerkingen van Persoonsgegevens:

1. Opslag van leer- en toetsresultaten
  2. Het terugontvangen door gebruikers Onderwijsinstelling van leer- en toetsresultaten.
  3. Beoordeling van leer- en toetsresultaten om leerstof af te stemmen op specifieke leerbehoefte van leerlingen Onderwijsinstelling.
  4. Analyse en interpretatie van leerresultaten.
- 
1. Verwerkingen die een onlosmakelijk onderdeel vormen van de aangeboden dienst.
    - a. Inloggen met Kennisnet Federatie Entree account: standaard attributenset wordt meegegeven.
    - b. Persoonlijke gegevens: naam school, naam gebruiker, e-mailadres gebruiker en eventueel door gebruiker zelf wordt geüpload.
    - c. Door leerlingen in het profiel in te voeren gegevens t.b.v. juiste werking van dienst, zoals opleidingsniveau, leerjaar, examenjaar, klas.
    - d. Door leerling ingevoerde antwoorden op vragen, opdrachten en toetsen (leerresultaten).
    - e. Feedback en beoordelingen van leerlingen door docenten.
    - f. Door docenten of mentor ingevoerde namen van klassen en/of mentorklassen.

## C. Doeleinden voor het verwerken van gegevens

De Verwerker is leverancier van een digitaal product en/of digitale dienst bestaande uit Leermiddelen en/of toetsen. De mogelijke doelstellingen van deze producten en diensten zijn omschreven in het daarop betrekking hebbende onderdeel van artikel 5 van de Verwerkersovereenkomst. Doelen verwerken personeelsgegevens:

1. Het geleverd krijgen/ in gebruik nemen van VO-next conform afspraken die zijn gemaakt tussen Onderwijsinstelling en VO-next.
2. De verwerking van Persoonsgegevens bevat naast een koppeling van de leerling of docent aan de school (identificatie via Entree) ook de opslag van leer- en toetsresultaten van leerlingen met als doel;
  - Begeleiden volgen van leeractiviteiten leerlingen door docenten;
  - door docenten terugontvangen van leer- en toetsresultaten;
  - de beoordeling van leer- en toetsresultaten om leerstof en toets- of oefenmateriaal te kunnen verkrijgen dat is afgestemd op de specifieke leerbehoefte van een leerling;
  - analyse en interpretatie van leerresultaten;

## D. Categorieën en soorten persoonsgegevens

### Inloggen met Kennisnet Entree Federatie

Inloggen wordt geregeld met een Kennisnet Entree account. Dit zorgt ervoor dat Onderwijsinstellingen toegang hebben tot verschillende educatieve diensten met slechts een login (Single Sign On – SSO). Tijdens het authenticatieproces ontvangt de applicatie van de Service Provider persoonsgegevens van de gebruiker in de vorm van attributen. Dit heeft als doel het identificeren en autoriseren van de persoon die gebruik wil maken van VO-next. VO-next gebruikt hiervoor alleen de Standaard attributen: deze attributen worden door alle Service Providers ontvangen (hiervoor is geen expliciete toestemming van de onderwijsinstellingen nodig, Attribute Release Policy).

**Standaard attributenset Kennisnet Entree Federatie**

Attribuutnaam	Beschrijving
uid	Versleutelde gebruikersnaam
nIEduPersonHomeOrganization	Naam instelling
nIEduPersonHomeOrganizationId	BRIN-nummer
givenName	Voornaam
eduPersonAffiliation	Rol

Omschrijving van de categorieën persoonsgegevens:

Van toepassing	Categorie	Toelichting
Ja	<b>1. Contactgegevens</b>	naam, e-mail, opleiding, geslacht, profielfoto;
Nee	2. Onderwijs-deelnemer-nummer	een administratienummer dat onderwijsdeelnemers identificeert
Nee	3. Nationaliteit en geboorteplaats	
Nee	4. Ouders, voogd	gegevens als bedoeld onder 1, van de ouders/verzorgers van onderwijsdeelnemers
Nee	5. Medische gegevens	gegevens die noodzakelijk zijn met het oog op de gezondheid of het welzijn van de betrokkene of op eigen verzoek, een en ander voor zover noodzakelijk voor het onderwijs;
Nee	6. Godsdienst	gegevens betreffende de godsdienst of levensovertuiging van de betrokkene, voor zover die noodzakelijk zijn voor het onderwijs, of op eigen verzoek, een en ander voor zover noodzakelijk voor het onderwijs;
Ja, voor de niet doorgehaalde punten	7. Studievoortgang	gegevens betreffende de aard en het verloop van het onderwijs, alsmede de behaalde studieresultaten; te weten: - Klas / leerjaar /ILT code - <b>Examinering</b> - Studievoortgang en/of Studietraject - <b>Begeleiding</b> <del>onderwijsdeelnemers,</del> <del>inclusief handelingsplan</del> <del>-Aanwezigheidsregistratie</del>
Nee	8. Onderwijsorganisatie	gegevens met het oog op de <b>organisatie van het onderwijs</b> en het verstrekken of ter beschikking stellen van leermiddelen;
Nee	9. Financiën	gegevens met het oog op het berekenen, vastleggen en innen van inschrijvingsgelden, school- en lesgelden en bijdragen of vergoedingen voor leermiddelen, alsmede bankrekeningnummer van betrokkene.

Ja	<b>10. Beeldmateriaal</b>	uitsluitend de door gebruiker zelf ingevoerde
----	---------------------------	---

		profielfoto. Deze is nuttig voor de docent voor snelle identificatie van een leerling bij het beoordelen van voortgang en resultaten.
Ja	<b>11. Docent, zorg-coördinator, intern begeleider, decaan, mentor</b>	koppeling door leerling aan door docent aangemaakte klas.
Ja	<b>12 Overige gegevens, te weten ....</b>	door leerling in te voeren gegevens t.b.v. juiste werking van de dienst, zoals opleidingsniveau, leerjaar, examenjaar, examenvakken en klas.
Nee	<b>13. BSN/PGN</b>	
Nee	<b>14. Keten-ID (ECK-ID)</b>	unieke ID voor de 'educatieve contentketen'. hiermee kunnen onderwijsinstellingen gegevens delen, zonder dat ze direct herleidbaar zijn naar onderwijsdeelnemers of docenten.

Na een jaar geen lid of een jaar geen activiteit door de gebruiker worden persoonsgegevens verwijderd en gebruiksgegevens die gebruikt worden als input voor geaggregeerde gegevens geanonimiseerd. Bij demo-accounts wordt het mailadres niet verwijderd, maar blijft dit ge-encrypt bestaan. De reden hiervoor is dat er per mailadres maar één keer een gratis demo aangevraagd mag worden.

### **E. Opslag Verwerking Persoonsgegevens:**

VO-next is ingericht op het Microsoft Azure Platform, <https://azure.microsoft.com/nl-nl/support/trust-center/>  
Opslag en verwerking vindt plaats in Amsterdam, Nederland.

### **F. Subverwerkers**

Onderwijsinstelling geeft Verwerker door ondertekening van de Verwerkersovereenkomst een algemene schriftelijke toestemming voor het inschakelen van een Subverwerker. Verwerker heeft het recht gebruik te gaan maken van andere Subverwerkers, mits daarvan voorafgaand mededeling wordt gedaan aan Onderwijsinstelling, en Onderwijsinstelling daartegen bezwaar kan maken binnen een redelijke periode.

Verwerker maakt ten tijde van het afsluiten van de Verwerkersovereenkomst gebruik van de volgende Subverwerkers (functioneel en technisch beheer):

- StudioVO, Coehoornsingel 6, 7201 AB ZUTPHEN, Rekensite.nl, Oefenprogrammaengels.nl en Portfolio-site.nl
- SubVerwerker voor Eindexamensite.nl is Eduspot Stormeer 9, 3446 JM Woerden

## Definities

In deze gebruikersvoorwaarden wordt verstaan onder:

- a. AVG: de Algemene Verordening Gegevensbescherming (Verordening 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG);
- b. Betrokkene, Verwerker, Derde, Persoonsgegevens, Verwerking van Persoonsgegevens, en Verantwoordelijke: de begrippen zoals gedefinieerd in de AVG;
- c. Bijlage: een bijlage bij deze Verwerkersovereenkomst, welke daarvan een onlosmakelijk deel uitmaakt;
- d. Convenant: het *Convenant Digitale Onderwijsmiddelen en Privacy*;
- e. Datalek: een inbreuk in verband met persoonsgegevens, zoals bedoeld in artikel 4, sub 12 AVG, die leidt tot de aanzienlijke kans op ernstig nadelige gevolgen
- f. Digitaal Onderwijsmiddel: Leermiddelen en Toetsen, en School- en Leerlinginformatiemiddelen;
- g. Kennisnet Keten iD (ECK ID): een keten pseudoniem van een aan een onderwijsinstelling persoonsgebonden nummer van een Onderwijsdeelnemer dat de Onderwijsdeelnemer niet langer direct identificeerbaar maakt. Hierna wordt dat pseudoniem opnieuw versleuteld tot het Keten iD, dat voor identificatiedoeleinden gebruikt wordt voor de toegang tot en het gebruik van Digitale Onderwijsmiddelen;
- h. Leermiddelen en Toetsen: digitaal product en/of digitale dienst bestaande uit leerstof en/of toetsen en de daarmee samenhangende digitale diensten, gericht op onderwijsleersituaties, ten behoeve van het geven van onderwijs door of namens Onderwijsinstelling;
- i. Privacy Bijsluiter: de privacy bijsluiter zoals opgenomen in Bijlage 1;
- j. Product- en Dienstenovereenkomst: de overeenkomst tussen Onderwijsinstelling en Verwerker, zoals omschreven in overweging a;
- k. School- en Leerlinginformatiemiddelen: een digitaal product en/of digitale dienst ten behoeve van het onderwijs(proces), zoals een leerling administratiesysteem, roostersysteem, ouderportaal, leerling- en oudercommunicatiesysteem, een elektronische leeromgeving en een leerlingvolgsysteem;
- l. Standaardattributenset: de door Kennisnet Entree Federatie vastgestelde aanvullende gestandaardiseerde Persoonsgegevens van Onderwijsdeelnemers die naast het Keten iD gebruikt kunnen worden voor de toegang tot en het gebruik van Digitale Onderwijsmiddelen;
- m. SubVerwerker: de partij die door Verwerker wordt ingeschakeld als Verwerker ten behoeve van de Verwerking van de Persoonsgegevens in het kader van deze Verwerkersovereenkomst en de Product- en Dienstenovereenkomst;
- n. Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens: de toepasselijke (Unierechtelijke en lidstaatrechtelijke) wet- en regelgeving en/of (nadere) verdragen, verordeningen, richtlijnen, besluiten, beleidsregels, instructies en/of aanbevelingen van een bevoegde overheidsinstantie betreffende de Verwerking van Persoonsgegevens, tevens omvattende toekomstige wijziging hiervan en/of aanvulling hierop, inclusief lidstaatrechtelijke uitvoeringswetten van de AVG en de Telecommunicatiewet.
- o. Verwerker: VO-next BV

## BIJLAGE: INFORMATIE BEVEILIGING EN PRIVACY (IBP)

Vanuit het IBP-beleid zijn er een aantal onderwerpen die we op basis van de wetgeving op orde moeten hebben. Vanaf 25 mei 2018 wordt de huidige Wet bescherming persoonsgegevens vervangen door de Algemene Verordening Gegevensbescherming (AVG).

De Verwerker is overeenkomstig de AVG en artikel 7 en 8 Model Verwerkersovereenkomst verplicht passende technische en organisatorische maatregelen te nemen ter beveiliging van de Verwerking van Persoonsgegevens, en om die maatregelen aan te tonen. Deze bijlage geeft een beknopte beschrijving en opsomming van die maatregelen.

### Classificeren

Elk proces, elk systeem en alle gegevens zijn in bepaalde mate belangrijk.

Maar hoe belangrijk, hoe essentieel zijn ze? En welke gegevens gebruiken we eigenlijk in welke systemen? Tot welke hoogte moet de informatie beveiligd worden?

Dit ligt aan: **Beschikbaarheid, Integriteit en Vertrouwelijkheid.**

VO-next platform wordt zowel op het gebied van beschikbaarheid, integriteit als vertrouwelijkheid geclassificeerd in de categorie midden.

Dit betekent:

1. Beschikbaarheid is belangrijk.

Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende een dag brengt merkbare schade toe aan de belangen van de instelling, haar medewerkers of haar studenten of klanten.

2. Integriteit is beschermd.

Blijvende juistheid van informatie moet gewaarborgd zijn. Sommige toleranties zijn toelaatbaar. Juistheid van informatie is belangrijk, maar niet kritisch. Het is niet noodzakelijk dat correctheid onbetwistbaar aangetoond kan worden. Indien informatie niet correct is kan de organisatie substantiële schade lijden.

3. Informatie is vertrouwelijk.

De organisatie, instelling of betrokkene kan substantiële schade lijden indien informatie toegankelijk is voor ongeautoriseerde personen. Informatie mag alleen toegankelijk zijn voor personen die hier vanuit hun functie toegang toe moeten hebben (need-to-know basis). Hieronder vallen onder andere persoonsgegevens.

b. Beschrijving in welke mate aan de hieronder genoemde minimale beveiligingsmaatregelen in het kader van artikel 32 AVG wordt voldaan.

- Verwerker maakt voor toegang tot de diensten gebruik van authenticatie via Kennisnet Entree Federatie en het daarmee verbonden wachtwoordbeleid.

<https://www.kennisnet.nl/artikel/privacy-leerlingen-bij-kennisnet-nog-beter-beschermd-dankzij-convenant/> Toegang is voor alle diensten alleen beschikbaar via een beveiligde verbinding (SSL).

- Verwerker heeft een InformatieBeleidsPlan waarin is vastgelegd welke medewerkers (rol en naam) toegang hebben tot welke gegevens en waarom.

- VO-next platform is ingericht op het Microsoft Azure Platform:

<https://azure.microsoft.com/nl-nl/support/trust-center/>.

Hierdoor worden beschikbaarheid, integriteit en vertrouwelijkheid afdoende gewaarborgd. <https://azure.microsoft.com/nl-nl/support/legal/sla/>

De wachtwoorden van gebruikers worden versleuteld opgeslagen in de SQL database.

*Fysieke beveiliging en beveiliging systemen voor opslag:*

- Het datacenter laat alleen mensen toe die door de webhoster toegang hebben tot de faciliteiten.
- Alle beveiligingsystemen worden continu getest en zijn gecertificeerd door een derde partij.
- Het beveiligingsteam staat in direct contact met relevante lokale instanties om de veiligheid van het datacenter te kunnen waarborgen.
- Er is sprake van een "authorized access list".
- Firewall: Sophos UTM firewall, beveiligd Wifi network, gescheiden netwerk voor gasten.
- N-Central software controleert of alle software applicaties up-to-date zijn.
- Alike backup

#### *Beveiliging verbindingen:*

VO-next platform is toegankelijk middels een encrypted HTTPS verbinding. Regular HTTP requests worden automatisch geredirect naar HTTPS. De web hosting provider staff krijgen toegang tot de hosting server middels encrypted SSH and HTTPS verbindingen.

#### *Maatregelen voor opsporen van zwakke plekken en incidentenbeheer:*

- N-Central software controleert of alle software applicaties up-to-date zijn.
- Sophos UTM monitort network actief op ongewenst/kwaadaardig data verkeer.
- Aanmelden op netwerk of server beveiligd met VPN Sophos UTM met SSL VPN.
- Gegevens en data gecategoriseerd en beschermd tegen ongeoorloofde toegang.
- Beleid voor het delen van bestanden via de cloud.

Een toetsing van getroffen maatregelen aan (inter)nationaal erkende normen en standaarden voor informatiebeveiliging: De genomen maatregelen zijn door <https://checkjedatalek.nl/> getoetst. Deze toetsing wordt periodiek herhaald.

#### **Beveiligingsincidenten en/of datalekken:**

In geval van een (vermoeden van) beveiligingsincident en/of datalek, kan Onderwijsinstelling contact opnemen met:

✉ [info@vo-next.nl](mailto:info@vo-next.nl)

☎ 0575-549681

#### **Informeren over Datalekken en/of incidenten met betrekking tot beveiliging**

StudioVO hanteert voor VO-content de volgende procedure:

##### **a) de 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 het bij het meldpunt via [info@vo-next.nl](mailto:info@vo-next.nl)

##### **2. Inventariseren**

Het Meldpunt bepaalt dan of er voldoende informatie omtrent het beveiligingsincident bekend is. Zo niet, dan zet hij aanvullende vragen uit bij de Ontdekker en/of de Technicus. De volgende informatie wordt daarna vastgelegd:

- Samenvatting van het beveiligingsincident, wat is er met de gegevens gebeurd, wat voor gegevens zijn het (bijzondere gegevens of van gevoelige aard)
- Datum/periode van het beveiligingsincident
- Aard van het beveiligingsincident
- Wanneer van toepassing (bij een datalek):
  - o Omschrijving van de groep betrokkenen
  - o Aantal betrokkenen
  - o Type persoonsgegevens in kwestie
  - o Worden de gegevens binnen een keten gedeeld

### 3. Beoordelen

Wanneer het Meldpunt voldoende informatie heeft verzameld, en een datalek vermoed, stuurt deze de Melder een verzoek om de verzamelde informatie te bekijken. De Melder beoordeelt de feiten om te bepalen of een melding aan de Autoriteit persoonsgegevens en/of betrokkenen vereist is.

De volgende informatie wordt vastgelegd door de Melder:

- Mogelijke gevolgen voor de persoonlijke levenssfeer van de betrokkenen
- Wordt het datalek gemeld aan de Autoriteit Persoonsgegevens? Waarom niet?
- Wordt het datalek aan betrokkenen gemeld? Waarom niet?
- Hoe worden meldingen gedaan? Wat is de inhoud van de melding?

Bij de beoordeling of er sprake is van een 'meldingsplichtig datalek', hou je rekening met het type gegevens, en met de hoeveelheid gegevens. Indien het datalek leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, of als het ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens, moet er gemeld worden.

Van die ernstige nadelige gevolgen of de kans op ernstige nadelige gevolgen is bijvoorbeeld sprake wanneer er heel veel gegevens van een betrokkene of gegevens van heel veel betrokkenen gelekt zijn maar ook wanneer de gelekte gegevens "gevoelig" zijn zoals bijvoorbeeld bijzondere persoonsgegevens over gezondheid, over de financiële of economische situatie van de betrokkene, of als de gegevens kunnen leiden tot stigmatisering van de betrokkene (denk aan het lekken van een leerling die vaak kinderen pest en daarmee gezien kan worden als notoire pester).

De onderstaande beslisboom wordt gebruikt:





#### 4. Repareren

De Technicus (Dave de Jong of Sander van der Laan) wordt gevraagd te achterhalen wat de oorzaak van het beveiligingsincident is en moet de oorzaak (laten) verhelpen. De technicus van Office in a box en/of Dnote leggen onderstaande vast:

- Technische en organisatorische maatregelen die genomen zijn om de inbreuk te verhelpen en verdere inbreuk te voorkomen.  
Voorgaande voor zover de oorzaak bekend is.
- Zijn de gelekke gegevens onbegrijpelijk voor degenen die er kennis van heeft kunnen nemen? Hoe zijn de gegevens onbegrijpelijk gemaakt (versleuteld)?

#### 5. Melden

Indien de conclusie bij stap 3 is dat er melding gedaan moet worden bij de Autoriteit Persoonsgegevens (en eventueel betrokkenen), dan zal de Melder dit binnen twee werkdagen 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 het Meldpunt waarmee het incident is afgesloten. Het Meldpunt verstuurt een samenvatting van de genomen maatregelen aan de Ontdekker.

#### 7. Informeren betrokkene(n): leerling/ouders, docenten

Heeft het datalek waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkene? Dan moet het datalek ook aan de betrokkenen zelf worden gemeld. Dat zijn medewerkers, leerlingen (of hun ouders als zij jonger zijn dan 16 jaar). In principe kan er van worden uitgaan dat het lekken van gevoelige aard gelek gemeld moet worden bij de betrokkenen en betrokken opdrachtgever.

Let op: als er persoonsgegevens zijn gelek maar die zijn beveiligd of versleuteld, en de gelekke data zijn onbegrijpelijk of ontoegankelijk voor anderen, dan hoeft dat toch niet aan betrokkenen te worden gemeld. Denk aan het lekken van een beveiligde én versleutelde database met gebruikersnamen en wachtwoorden.

#### b) Monitoring beveiligingsincidenten en datalekken

Het Meldpunt van VO-next maakt twee keer per jaar een analyse van de meldingen van beveiligingsincidenten en datalekken in samenwerking met de functionaris gegevensbescherming.

In de analyse wordt ingegaan op eventuele structurele ontwikkelingen, en of de noodzaak bestaat om maatregelen te nemen om herhaling te voorkomen.

Het schoolbestuur wordt geïnformeerd over de uitkomsten van de analyse.

#### Versie 1, 7 mei 2018

*Deze Beveiligingsbijlage maakt onderdeel uit van de afspraken die zijn gemaakt in het Convenant Digitale Onderwijsmiddelen en Privacy 3.0, een initiatief van de PO-Raad, VO-raad, MBO Raad de verschillende betrokken ketenpartijen (GEU, KBb-E en VDOD) en het ministerie van Onderwijs, Cultuur en Wetenschap. Meer informatie hierover vindt u hier: <http://www.privacyconvenant.nl>.*

## **Contactgegevens**

Voor vragen of opmerkingen over deze gebruikersvoorwaarden of de werking van dit product of deze dienst, kunt u terecht bij:

✉ [info@vo-next.nl](mailto:info@vo-next.nl)

☎ **0575-549681**