

## Bijlage 2: Beveiligingsbijlage

Behorende bij verwerkersovereenkomst Van Dale Online van Van Dale Uitgevers handelend onder de naam VBK|media B.V..

Versie: 7 december 2022

[Naam Uitgever] heeft, overeenkomstig de AVG en artikel 7 en 8 van de Model Verwerkersovereenkomst passende technische en organisatorische maatregelen genomen om de verwerking van persoonsgegevens aantoonbaar te beveiligen. Deze bijlage geeft een beknopte beschrijving en opsomming van die maatregelen.

### 1. Maatregelen die Van Dale Uitgevers heeft genomen om de Persoonsgegevens te beschermen tegen onopzettelijke of onrechtmatige vernietiging, wijziging, opslag, toegang of openbaarmaking.

- Een passend beleid voor de beveiliging van de Verwerking van de Persoonsgegevens, waarbij het beleid periodiek wordt geëvalueerd en – zo nodig – aangepast;
- Een systeem van autorisatie waardoor enkel geautoriseerde medewerkers toegang kunnen verkrijgen tot de Verwerking van Persoonsgegevens in het kader van de Verwerkersovereenkomst. Medewerkers hebben op grond van deze systematiek geen toegang tot meer data dan strikt noodzakelijk is voor hun functie;
- Er is een coördinator informatiebeveiliging die de risico's omtrent de verwerking van persoonsgegevens inventariseert, het beveiligingsbewustzijn stimuleert, voorzieningen controleert en maatregelen treft die zien op naleving van het informatiebeveiligingsbeleid. Deze coördinator is bereikbaar op het volgende emailadres: [klantgegevens@vandale.nl](mailto:klantgegevens@vandale.nl).
- Informatiebeveiligingsincidenten worden gedocumenteerd en worden benut voor optimalisatie van het informatiebeveiligingsbeleid;
- Er is een proces ingericht voor communicatie over informatiebeveiligingsincidenten;
- Met medewerkers worden geheimhoudingsverklaringen afgesloten en worden informatiebeveiligingsafspraken gemaakt;
- Het bewustzijn, opleiding en training ten aanzien van informatiebeveiliging wordt gestimuleerd.

## 2. Maatregelen om de Persoonsgegevens te beveiligen en continuïteit van de middelen, het netwerk, de server en de applicatie te waarborgen.

Hieronder staat de rapportage van de BIV-classificatie, de mate van compliance en de uitleg bij eventuele afwijkingen van de standaarden, zoals beschreven in het Certificeringsschema informatiebeveiliging en privacy ROSA. Zie: [https://www.edustandaard.nl/standaard\\_afspraken/certificeringsschema-informatiebeveiliging-en-privacy-rosa/certificeringsschema-informatiebeveiliging-en-privacy-rosa/](https://www.edustandaard.nl/standaard_afspraken/certificeringsschema-informatiebeveiliging-en-privacy-rosa/certificeringsschema-informatiebeveiliging-en-privacy-rosa/).

<b>Toetsvorm</b>	Self-assessment, uitgevoerd op 11-10-2022 op basis van het toetsingskader v3.0		
<b>Uitvoerder toets</b>	R. Vos, Software Architect, IO Digital		
<b>Inlogpagina</b>	www.dienst-x.nl		
<b>BIV-classificatie</b>	Beschikbaarheid=Hoog    Integriteit=Laag    Vertrouwelijkheid=Midden		
<b>Categorie</b>	<b>Maatregelen</b>	<b>Compliance</b>	<b>Uitleg</b>
<b>Beschikbaarheid</b>	Ontwerp	Niet voldaan	Van Dale Online is onafhankelijk van klantsystemen.
	Capaciteit beheer	Voldaan	
	Onderhoud	Voldaan	
	Testen	Niet voldaan	Testen worden handmatig gedaan
	Monitoring	Voldaan	
	Herstel	Voldaan	
<b>Integriteit</b>	Herleidbaarheid (gebruikers)	Voldaan	
	Backup	Niet voldaan	Er wordt dagelijks een snapshot gemaakt. Er wordt geen gebruikers content in de toepassing opgeslagen. Derhalve niet relevant.
	Application controls	Niet voldaan	Er is geen controle op invoervelden in het abonnementenbeheer. Dit abonnementenbeheer is echter alleen toegankelijk voor medewerkers van Van Dale.
	Onweerlegbaarheid	Voldaan	Inloggegevens worden 13 maanden bewaard.
	Herleidbaarheid (technisch beheer)	Niet voldaan	In het abonnementenbeheer (trails) wordt niet bijgehouden wie welke wijzigingen heeft gedaan. Dit abonnementenbeheer zit echter achter een firewall met ip-whitelisting.
	Controle integriteit	Voldaan	
	Onweerlegbaarheid (toepassing)	Niet voldaan	Activiteit in het abonnementenbeheer wordt niet gelogd
<b>Vertrouwelijkheid</b>	Levenscyclus gegevens	Niet voldaan	Wordt op korte termijn opgelost door data anonimisering. Een proces tot het verwijderen van persoonsgegevens is al ingeregeld.
	Logische toegang	Voldaan	

	Fysieke toegang	Voldaan	
	Netwerk toegang	Voldaan	
	Scheiding omgevingen	Voldaan	
	Transport en fysieke opslag	Voldaan	
	Logging	Voldaan	
	Omgaan met kwetsbaarheden	Niet voldaan	OWASP top 10 wordt aan voldaan, Zoek applicatie is ontworpen volgens privacy by design

### 3. Afspraken over het informeren over beveiligingsincidenten en/of Datalekken

Van Dale Uitgevers heeft een procedure voor de monitoring en identificatie van incidenten en het informeren in geval van Datalekken en/of incidenten met betrekking tot beveiliging. In zo'n geval zullen wij de verwerkingsverantwoordelijke de volgende informatie ter hand stellen:

- De kenmerken van de inbreuk, zoals: datum en tijdstip ontdekken en duur inbreuk, samenvatting van de inbreuk waaronder de aard van de inbreuk en de aard en beschrijving van het beveiligingsincident (op wat voor onderdeel van de beveiliging ziet het, hoe heeft het zich voorgedaan, heeft het betrekking op lezen, kopiëren, veranderen, verwijderen/vernietigen en/of diefstal van persoonsgegevens);
- De oorzaak van de inbreuk;
- Hoe de inbreuk is ontdekt;
- De maatregelen die getroffen zijn om de inbreuk aan te pakken en eventuele (verdere en toekomstige) schade te voorkomen;
- Of de bij de inbreuk betrokken gegevens versleuteld, gehasht etc. waren;
- Benoemen van groep(en) Betrokkenen die gevolgen kunnen ondervinden van het incident, en de aantallen en omvang van de groep Betrokkenen;
- Wat de mogelijke gevolgen zijn van de inbreuk voor de Onderwijsinstelling en de Betrokkene(n), waaronder indien mogelijk een inschatting van het risico van de gevolgen voor betrokkene(n);
- De hoeveelheid en soort Persoonsgegevens betrokken bij de inbreuk (met name bijzondere gegevens zoals gegevens over gezondheid of godsdienst, of gegevens van gevoelige aard, waaronder toegangs- of identificatiegegevens, financiële gegevens of leerprestaties).

In geval van een (vermoeden van) beveiligingsincident en/of Datalek zal onze coördinator informatiebeveiliging, in beginsel per email contact opnemen met de contactpersoon van de Onderwijsinstelling die is vermeld in bijlage 4. De coördinator informatiebeveiliging is tevens aanspreekpunt voor het geval de Onderwijsinstelling contact wil opnemen over een beveiligingsincident en/of Datalek. De coördinator informatiebeveiliging is bereikbaar op het volgende mailadres: [klantgegevens@vandale.nl](mailto:klantgegevens@vandale.nl).

#### Paraaf

Onderwijsinstelling

Verwerker

---

*Deze bijlage is opgezet volgens het branche-specifieke format van MEVW en vormt een integraal onderdeel van de bijbehorende verwerkersovereenkomst. Verwerkersovereenkomst en de bijlagen daarbij maken onderdeel uit van de afspraken die zijn gemaakt in het Convenant Digitale Onderwijsmiddelen en Privacy 4.0, een initiatief van de PO-Raad, VO-raad, MBO Raad de verschillende betrokken ketenpartijen (MEVW, KBB-e en VDOD) en het ministerie van Onderwijs, Cultuur en Wetenschap. Meer informatie hierover vindt u hier: <https://www.privacyconvenant.nl/>.*