

Bijlage 2: Beveiligingsbijlage methode Dubbelklik

Eduklik is overeenkomstig de AVG en artikel 7 en 8 Model Bewerkerovereenkomst 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.

Minimale beveiligingsmaatregelen en aantoonbaarheid

Eduklik treft passende technische maatregelen voor de beveiliging van de Verwerking van Persoonsgegevens.

- a. Eduklik hanteert een autorisatiebeleid om te bepalen wie toegang moet hebben tot welke gegevens. Medewerkers hebben op grond van deze systematiek geen toegang tot meer data dan noodzakelijk is voor hun functie.
- b. Een beschrijving in welke mate aan de hieronder genoemde minimale beveiligingsmaatregelen in het kader van artikel 32 AVG wordt voldaan;
 - i. Eduklik heeft een passend beleid voor de beveiliging van de Verwerking van de Persoonsgegevens, waarbij het beleid periodiek wordt geëvalueerd en – zo nodig – aangepast;
 - ii. Eduklik heeft de Persoonsgegevens die worden verwerkt geclassificeerd op het gebied van beschikbaarheid, integriteit en vertrouwelijkheid en heeft op basis van die classificatie beveiligingsmaatregelen genomen om de risico's voor de Verwerking van Persoonsgegevens te beperken;
 - iii. Eduklik neemt maatregelen zodat via een systeem van autorisatie enkel geautoriseerde medewerkers toegang kunnen verkrijgen tot de Verwerking van Persoonsgegevens in het kader van de Bewerkerovereenkomst. Hierbij heeft Eduklik procedures vastgesteld en gedeeld met de Onderwijsinstelling voor de identificatie, autorisatie en authenticatie van medewerkers alsmede rondom de registratie, aanmelding en afmelding van de medewerkers;
 - iv. Eduklik zorgt dat de toegang tot het product of de dienst beveiligd is door middel van een passend beleid voor wachtwoorden dat aansluit bij de stand van de techniek;
 - v. Eduklik heeft procedures voor het verlenen van toegang tot Persoonsgegevens (waaronder een registratie- en afmeldprocedure voor toewijzing van toegangsrechten), en het in logbestanden vastleggen van gebeurtenissen betreffende gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen;
 - vi. Eduklik heeft maatregelen genomen om de Persoonsgegevens te beschermen tegen verwerkingsrisico's, vooral als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig.
 - vii. Eduklik maakt bij de beveiliging van de Verwerking van Persoonsgegevens gebruik van een (inter)nationale beveiligingsnorm;
 - viii. Eduklik heeft maatregelen genomen om zwakke plekken te identificeren ten aanzien van de Verwerking van Persoonsgegevens in de systemen die worden ingezet voor het verlenen van diensten aan de Onderwijsinstelling.
- c. Een toetsing van getroffen maatregelen aan (inter)nationaal erkende normen en standaarden voor informatiebeveiliging.

Beveiligingsincidenten en/of datalekken:

In geval van een (vermoeden van) beveiligingsincident en/of datalek, kan Onderwijsinstelling contact opnemen met: helpdesk@dubbelklik.nu

De contactpersoon voor Eduklik is: A. Hoogenboom

Informereren over Datalekken en/of incidenten met betrekking tot beveiliging

Er is een procedure over het informeren in geval van datalekken en/of incidenten met betrekking tot beveiliging, en bevat ten minste te volgende punten:

- Eduklik monitort 24/7 haar dienstverlening en heeft maatregelen getroffen om ongeoorloofde of onrechtmatige toegang tot gegevens te voorkomen en te identificeren.
- Signalen die duiden op een Datalek worden beoordeeld door de contactpersoon van Eduklik, die analyseert of sprake kan zijn van een Datalek.
- Wanneer zich een Datalek voordoet, wordt de verantwoordelijke onderwijsinstelling door of namens Eduklik in beginsel binnen 24 uur na vaststelling dat sprake is van een Datalek per e-mail geïnformeerd.
- Voor vervolgvragen of vragen kan telefonisch of per e-mail contact worden opgenomen met onze helpdesk.
- Informatie die in ieder geval over een incident gedeeld moet worden:
 - De kenmerken van het incident, zoals: datum en tijdstip constatering, samenvatting incident, kenmerk en aard incident (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 het beveiligingsincident;
 - De maatregelen die getroffen zijn om eventuele/verdere schade te voorkomen;
 - Benoemen van betrokkenen die gevolgen kunnen ondervinden van het incident, en de mate waarin;
 - De omvang van de groep betrokkenen;
 - Het soort gegevens dat door het incident wordt getroffen (met name bijzondere gegevens, of gegevens van gevoelige aard, waaronder toegangs- of identificatiegegevens, financiële gegevens of leerprestaties).
- Eventuele afspraken of, en zo ja hoe, Eduklik een melding aan de Autoriteit Persoonsgegevens kan verrichten.

Versie

1.0 / 19-03-2018

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>.