PRIVACY COMPANY

Analyse online proctoring

SURF

9 april 2020

SURF onderzoek naar online proctoring

Introductie

Het online toetsen afnemen bij studenten, ook wel online proctoring genoemd, wordt steeds populairder. Dit is begrijpelijk. Op alle niveau's binnen het onderwijs zie je het digitaal lesgeven exponentieel groeien. Een logische vervolgstap lijkt dan ook het online toetsen van de lesstof.

Het online toetsen kent meerdere voordelen. Zo biedt het de mogelijkheid om studenten veelal tijd - en plaatsonafhankelijk op een veilige manier te toetsen en om grotere groepen studenten te examineren. Met online toetsing kan het onderwijs flexibeler worden in gevuld.

Er zijn echter ook nog veel (onbeantwoorde) vragen over het gebruik van online toetsen, waardoor vooralsnog onderwijsinstellingen terughoudendheid betrachten om naast het analoog toetsen ook online toetsing aan te bieden. Een van die vragen betreft de wijze waarop de aanbieders van online proctoring software de privacy van studenten waarborgen.

De privacy wetgeving, de Algemene Verordening Gegevensbescherming (AVG), stelt regels aan het monitoren van personen. Het online toetsen is een vorm van monitoren, namelijk bij online toetsing worden studenten bij het maken van een toets met behulp van software structureel online gecontroleerd of de student niet spiekt of fraudeert. De AVG is dan ook van toepassing op het gebruik van online proctoring software. De AVG vereist dat bij monitoring altijd een belangenafweging wordt gemaakt of de controle op een minder ingrijpende wijze kan plaatsvinden. Daarnaast zullen er altijd voldoende waarborgen moeten worden getroffen om de inbreuk op de privacy van de student zoveel mogelijk te beperken.

SURF heeft een juridisch analyse gevraagd van de beschikbare documentatie van drie online proctoring software aanbieders. Uit een korte rondgang blijkt dat hogescholen en universiteiten veelal met deze drie aanbieders in gesprek zijn. Het betreft de online proctoring software van de aanbieders Proctorio, ProctorExam en RPnow.

Het is belangrijk om te onderstrepen dat de focus ligt op de juridische analyse van documenten op basis van de volgende (beschikbare) documentatie: de privacyverklaring, de algemene voorwaarden en de verwerkersovereenkomst. Per online proctoring (aanbieder) kijken we naar de volgende AVG onderdelen:

1. De definitie en gebruik van persoonsgegevens
2. Versturen van persoonsgegevens naar landen buiten de Europese Economische Ruimte
3. Rol van aanbieder onder de AVG en doelbinding
4. Grondslagen
5. Procedure om datalekken te melden en aansprakelijkheid
6. Bewaartermijnen
7. Subverwerkers en derde partijen
8. Rechten van betrokkenen
9. Bijstand verlenen voor nakoming AVG compliance
10. Geautomatiseerde besluitvorming en profilering

Elk AVG onderdeel heeft de volgende opzet: introductie van het AVG beginsel, analyse van de (niet) AVG compliant onderdelen en aanbevelingen ten aanzien van de onderdelen die niet AVG compliant zijn. In de bijlage is nog een overzicht opgenomen waarin kort de bevindingen zijn weergegeven.

Proctorio

Proctorio, met haar hoofdvestiging in de Verenigde Staten, Arizona, biedt een '*Learning Integrity Platform*' met ID-verificatie, geautomatiseerde bewaking, inhoudsbescherming, veilige browserinstellingen, computervergrendeling, originaliteitsverificatie, administratieve en facultaire controles en diepgaande, onmiddellijke analyse. De dienstverlening van Proctorio houdt zowel 'live proctoring', 'opslag en controle achteraf' als volledig 'geautomatiseerd proctoring' in.[1] De website geeft een korte toelichting op de voor en nadelen hiervan.[2]

Proctorio biedt een service, waarbij het opnemen van video, audio en schermactiviteit of geen van vorenstaande mogelijk is. Er zijn verschillende instelbare parameters die door de onderwijsinstelling zelf ingesteld kunnen worden en de gevoeligheid bepalen waarmee frauduleus gedrag van studenten kan worden gedetecteerd.

De Proctorio software (een SaaS oplossing) kan door onderwijsinstelling in hun eigen leeromgeving (LMS) worden geïnstalleerd, studenten zelf dienen uitsluitend Google Chrome en de Proctorio extension te downloaden op hun computer.

Voor meer uitleg dan wel toelichting van de verschillende services die Proctorio biedt, wordt verwezen naar de website en de SaaS Agreement die een klant (i.c. onderwijsinstelling) kan afsluiten met Proctorio. Deze laatste is niet openbaar beschikbaar en dan ook niet meegenomen in deze risico-analyse. Navraag bij de leverancier leert dat Proctorio (vooralsnog) geen verwerkersovereenkomst-template hanteert. Het is aldus aan de verwerkingsverantwoordelijke (i.c. onderwijsinstelling) om deze zelf voor te leggen aan Proctorio indien zij de service wenst afnemen.

Bronnen die zijn gebruikt bij de juridische analyse:

- Proctorio website, geraadpleegd op 8 april 2020, https://proctorio.com/
- Proctorio Privacy Policy (versie 1 januari 2020), https://proctorio.com/privacy
- Proctorio GDPR, geraadpleegd op 8 april 2020, https://proctorio.com/gdpr
- Proctorio Terms of Service, geraadpleegd op 8 april 2020, https://proctorio.com/terms

1. Definitie en gebruik van persoonsgegevens

Introductie AVG beginsel

De Algemene Verordening Gegevensbescherming (AVG) definieert persoonsgegevens als alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.

Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is. Een persoonsgegeven is een stukje informatie dat direct naar een individu leidt (een geïdentificeerde persoon) of zonder al te veel moeite herleidbaar is tot een individu (een identificeerbare persoon). Dat kan een (persoons)naam zijn, maar ook een telefoonnummer, (e-mail)adres en zelfs het IP-adres van een computer. Ook camerabeelden, telefoongesprekken, cookies, persoonlijke verificatiecodes, paspoortgegevens, BSN en andere zaken vallen hier onder.

[1] Voor meer informatie over deze drie hoofdcategorieën van proctoring wordt verwezen naar de Whitepaper Online Proctoring van Surf https://www.surf.nl/files/2019-04/whitepaper-online-proctoring.pdf
[2] https://proctorio.com/platform/exam-monitoring, geraadpleegd op 8 april 2020.

Analyse van de (niet) AVG compliant onderdelen

Proctorio houdt in haar Privacy Policy de definitie van Personal Identifiable Information (PII) aan. Een gangbare term in de Verenigde Staten en in de informatiebeveiliging sector. PII wordt gedefinieerd als *alle informatie over een persoon die door een agentschap wordt onderhouden, waaronder (1) alle informatie die kan worden gebruikt om de identiteit van een persoon te onderscheiden of te achterhalen, zoals naam, burgerservicenummer, geboortedatum en geboorteplaats, naam van de moeder of biometrische gegevens; en (2) alle andere informatie die aan een persoon is gekoppeld of kan worden gekoppeld, zoals medische, educatieve, financiële en werkgelegenheidsinformatie.*[3]

PII wordt vaak als de equivalent van een persoonsgegeven uit de AVG gezien, maar is niet volledig hetzelfde. Onder de term PII vallen niet gegevens die niet op zichzelf kunnen worden gebruikt om een persoon te identificeren, te traceren of te lokaliseren. Denk hierbij aan een IP adres, een studenten ID of cookies. Deze informatie valt dus wel onder de term 'persoonsgegevens' uit de AVG (art. 4.1) maar niet onder de term PII.

Proctorio geeft dan ook in haar Privacy Policy weer dat het bij het gebruik maken van haar diensten student gegevens, '*such as your name, email address, phone number, and institution*' worden verwerkt. Een overzicht van (categorieën van) de persoonsgegevens zoals gedefinieerd onder de AVG die door Proctorio worden verwerkt mist.

Daarnaast stelt Proctorio dat het geanonimiseerde gegevens kan gebruiken, die zij verzamelt als gevolg van het gebruik van de Proctorio website of de services. Als voorbeeld geeft Proctorio het verwerken van geanonimiseerde gegevens over het gebruik van de service door studenten (van aangesloten onderwijsinstellingen) met als doel het identificeren van trends, statistieken, beveiliging, onderzoek of andere doeleinden. Proctorio anonimiseert de verzamelde gegevens *door alle directe en indirecte persoonlijke identificatiegegevens te verwijderen, inclusief maar niet beperkt tot naam- en locatiegegevens.* Opvallend is dat hier wel wordt aangegeven dat ook 'indirecte persoonlijke identificatiegegevens' worden verwijderd. Proctorio stelt geanonimiseerde gegevens niet te her-identificeren en niet geanonimiseerde gegevens over te dragen, tenzij die partij waarvan de gegevens afkomstig zijn ermee instemt.

Proctorio kan het totale aantal bezoekers (op elke pagina) van de website, browsertype en IP-adressen volgen. Hierbij anonimiseert Proctorio het IP-adres van de bezoeker in een zo vroeg mogelijk stadium van het verzamelnetwerk door het laatste octet van het IP adres te verwijderen. De bijgehouden gegevens worden in geaggregeerde vorm bewaard, gebruikt en mogelijk openbaar gemaakt voor het analyseren op trends en statistieken in totaal.

Proctorio verzamelt geen betalingsinformatie. Voor zover toepasselijk, wordt de betaal functionaliteit geleverd door een niet-gelieerde derde partij, onderhevig aan hun gebruiksvoorwaarden. Dit staat los van het facturen door Proctorio van klanten waarmee het een SaaS-overeenkomst heeft gesloten.

Een student zal bij gebruikmaking van Proctorio software moeten instemmen dat Proctorio je monitort:

> "... by webcam, microphone, browser, desktop, or any other means necessary to uphold integrity. At the discretion of the exam administrator, this may include a scan of your surroundings and computer display. This monitoring will be conducted by machine or by a live person. The information from the session may be recorded and provided to the institution, university, college, school, or organization and can be viewed by authorized

[3] NIST definitie voor PII

personnel thereof. It is important to note that this information is not sold, or given to any third parties."

Als uitleg bij 'or any other means necessary' wordt gegeven: tekst, grafieken, foto's, geluidopnames en documenten die geüpload, gedownload worden of in beeld verschijnen bij gebruik van de services[4]. Een recent verschenen artikel in de Washington Post stelt dat hieronder ook moet worden verstaan:

> "the system tracks their speech and eye movements, how long they took to complete the test and how many times they clicked the mouse. It then gives professors an automated report ranking test-takers by "suspicion level" and the number of testing "abnormalities."[5]

Proctorio verklaart onder de link "GDPR' op haar website dat zij de AVG verplichtingen erkent en de eisen ervan ondersteunt. Bovendien stelt Proctorio dat het toegewijd is om persoonlijke informatie te beschermen waarover zij beschikt en bij het ontwikkelen van haar diensten rekening houdt dat de aanpak van gegevensbescherming effectief is, geschikt is voor het doel en een begrip van en waardering voor GDPR toont.

Daarnaast wordt vermeld:

> "we provide easy to access information via our website of an individual's right to access any personal information that Proctorio processes about them and to request information about:
>
> - What personal data we hold about them
> - The purposes of the processing
> - The categories of personal data concerned
>
> (...)"

Deze informatie is echter niet te vinden op de website, anders dan de hierboven vermelde informatie over PII.

<u>Aanbevelingen</u>

Doordat Proctorio de – te beperkte- definitie van PII aanhoudt voldoet zij niet aan de vereisten zoals deze in de AVG zijn gesteld ten aanzien van de definitie van persoonsgegevens onder art. 4 AVG.

Mogelijk biedt de SaaS Agreement (welke niet is beoordeeld als onderdeel van deze analyse) meer duidelijkheid, maar in het algemeen kan worden gesteld dat de openbare informatie op de Proctorio website voor gebruikers en (onderwijs)instellingen onvoldoende duidelijk en concreet maakt welke persoonsgegevens worden verwerkt.

Proctorio zal de informatie over de (categorieën van) persoonsgegevens die zij verwerkt naar klanten en gebruikers toe moeten aanvullen en makkelijk toegankelijk maken wil zij voldoen aan de AVG en haar eigen toezegging op de website onder 'GDPR' nakomen.

[4] zie de definitie van Content in de Terms of Use te vinden op de Proctorio website
[5] Washington Post, 1 april 2020, *'Mass school closures in the wake of the coronavirus are driving a new wave of student surveillance'* van Drew Harwell

2. Versturen van persoonsgegevens naar landen buiten de Europese Economische Ruimte

Introductie AVG beginsel

Persoonsgegevens doorgeven vanuit Nederland naar het buitenland mag alleen als een land voldoende bescherming biedt. Binnen de Europese Economische Ruimte (EER) is dit gewaarborgd door de AVG. Voor doorgifte naar landen buiten de EER gelden aparte regels.

Als een land buiten de EER in de nationale wetgeving een passend niveau van gegevensbescherming biedt, kan de Europese Commissie (EC) een 'adequaatheidsbeslissing' nemen (artikel 45 van de AVG). De EC stelt dan vast dat de gegevensbescherming in dat land van een vergelijkbaar niveau is als de AVG.

Als er een adequaatheidsbeslissing is genomen, hoeft er voor doorgifte naar dat land of die sector geen aanvullende waarborg te worden getroffen.

Het EU-VS Privacy Shield is een voorbeeld van een adequaatheidsbeslissing, met het verschil dat de beslissing alleen geldt voor zover het ontvangende bedrijf zich heeft gecertificeerd en zich houdt aan de principes die zijn vastgelegd in het EU-V.S. Privacy Shield.

Als er geen sprake is van een adequaatheidsbeslissing, dan moet er een andere passende waarborg zijn als een organisatie persoonsgegevens wil doorgeven aan een land buiten de EU. Dat kan met een EU modelovereenkomst die door de Europese Commissie is vastgesteld (artikel 46 (2) onder c) of Bindende bedrijfsvoorschriften zijn (artikel 47). Dit laatste zijn 'global privacy policies' die gelden binnen organisaties voor doorgifte van persoonsgegevens naar landen zonder adequaat beschermingsniveau (derde landen) wereldwijd. Alle werknemers en entiteiten binnen het concern (ook de Nederlandse en Europese vestigingen) moeten zich houden aan deze interne global privacy policy.

Analyse van de (niet) AVG compliant onderdelen

Proctorio is gevestigd in de Verenigde Staten, Arizona en heeft twee vestigingen in de EER, namelijk München in Duitsland en Belgrado in Servië. Voor wat betreft de plaats van verwerking wordt uitsluitend het volgende gemeld in de Privacy Policy: (…) *if you use our services anywhere else [United States], Proctorio d.o.o. (a European corporation) is the data processor*. Of, en voor hoe ver, persoonsgegevens van EU ingezetenen worden verwerkt buiten de EU door Proctorio wordt niet toegelicht in de gereviewde documentatie.

Proctorio vermeldt in de Privacy Policy met betrekking tot de doorgifte van persoonlijke informatie van EU ingezetenen naar buiten de EU het volgende:

> "By using the Services you acknowledge and agree that: (i) your information will be processed as described in this Privacy Policy; and (ii) you consent to have your information transferred to us and our facilities in the United States or elsewhere, including those of third parties as described in this policy.
>
> European Economic Area (EEA) or Switzerland: If you are based in the EEA or Switzerland, you acknowledge and agree that we may transfer your information (including personal information) to us and our facilities in the United States or elsewhere, including those of third parties as described in this policy. Please review our Terms of Service and the applicable SaaS Agreement for more information regarding any other applicable data protections."

Ten aanzien van de bescherming van persoonlijke informatie buiten de EER verklaart Proctorio:

> "where Proctorio stores or transfers personal information outside the EU, we have robust procedures and safeguarding measures in place to secure, encrypt and maintain the integrity of the personal information. Our procedures include a continual review of the countries with sufficient adequacy decisions, as well as provisions for binding corporate rules; standard data protection clauses or approved codes of conduct for those countries without".[6]

Uit bovenstaande kan worden opgemaakt dat persoonsgegevens van EER ingezetenen worden verwerkt buiten de EER en meer specifiek in de Verenigde Staten. Per land wordt gekeken welke passende maatregelen genomen moeten worden. Proctorio is sinds december 2017 als actief EU-V.S. Privacy Shield bedrijf geregistreerd.[7] In oktober 2020 zal zelf-hercertificering moeten plaats vinden.

Tegelijkertijd blijkt uit de beschikbare documentatie niet waar persoonsgegevens van EER gebruikers worden opslagen en verwerkt, wordt er geen garantie of mogelijkheid gegeven om persoonsgegevens van EER ingezetenen uitsluitend binnen de EER te verwerken. De Terms of Service levert helaas niet meer relevante informatie op. Mondeling navraag leert dat Proctorio de persoonsgegevens van betrokkenen uit de EER die gebruik maken van de online proctoring software uitsluitend verwerkt worden in München. Hier kunnen echter geen rechten aan worden ontleend.

Aanbevelingen

Met de EU-VS Privacy Shield zelfcertificering bewijst Proctorio dat zij aan de eisen van het Privacy Shield voldoen. Een EU modelovereenkomst is dan dus niet meer nodig indien een onderwijsinstelling een SaaS-overeenkomst sluit met Proctorio. Dit betekent overigens niet dat een verwerkersovereenkomst overbodig is. Het is aan te bevelen hieraan de nodige aandacht te besteden. Het EU-V.S. Privacy Shield is al enkele jaren onderwerp van discussie. Privacy voorvechters stellen dat het regime onvoldoende de AVG standaarden waarborgt, het principe van '*je eigen vlees keuren*' (zelfcertificering) niet voldoet en een regelmatige controle door de Amerikaanse overheid of de bedrijven ook daadwerkelijk de regels naleven te wensen overlaat.

3. Rol van Proctorio onder de AVG en doelbinding

Introductie AVG beginsel

Rol van Proctorio: De wet maakt onderscheid tussen de verwerkingsverantwoordelijke (degene die verantwoordelijk is voor de verwerking van persoonsgegevens) en de verwerker (degene die in opdracht van de verwerkingsverantwoordelijke persoonsgegevens verwerkt).

Verwerkingsverantwoordelijke (ook wel verantwoordelijke): de verwerkingsverantwoordelijke is degene die (1) het doel en (2) de middelen van de verwerking vaststelt.

(1) Het gaat erom wie uiteindelijk bepaalt of er gegevens worden verwerkt en zo ja, welke verwerkingen er plaatsvinden, welke persoonsgegevens verwerkt worden en voor welk doel.

(2) Bij het bepalen van de middelen gaat het erom op welke wijze de verwerking van persoonsgegevens zal plaatsvinden, bijvoorbeeld met software.

Verwerker: de verwerker verwerkt de persoonsgegevens in opdracht van de verwerkingsverantwoordelijke. De verwerker verwerkt gegevens volgens de instructies van en onder de verantwoordelijkheid van de verwerkingsverantwoordelijke, maar staat wel buiten de organisatie. Verder heeft de verwerker geen zeggenschap over het doel en de middelen van de verwerking.

[6] zie GDPR, https://proctorio.com/gdpr, onder 'International Data Transfers & Third-Party Disclosures'
[7] zie ook Privacy Policy; https://proctorio.com/privacy, EU-U.S. and Swiss-U.S. Privacy Shield Framework

Beslissingen over het gebruik van de gegevens, de verstrekking aan derden, de duur van de opslag etc. worden genomen door de verwerkingsverantwoordelijke.

De verwerkingsverantwoordelijke is verplicht een overeenkomst aan te gaan met de verwerker, de zogenaamde verwerkersovereenkomst.

Subverwerker: een verwerker kan natuurlijk ook een ander inschakelen om werk voor hem uit te voeren. Deze onderaannemer noemen we dan een subverwerker. In de verwerkersovereenkomst is vaak bepaald dat een subverwerker alleen mag worden ingeschakeld na schriftelijk akkoord van de verwerkingsverantwoordelijke.

Doelbinding: een verwerking mag alleen plaatsvinden als er een duidelijk omschreven en gerechtvaardigd doel is. De persoonsgegevens die worden verzameld mogen vervolgens ook niet verder worden verwerkt op een manier die niet te verenigen is met dat doel.

Analyse van de (niet) AVG compliant onderdelen

In de Privacy Policy stelt Proctorio het volgende:

> "(..) If you use our services anywhere else [United States], Proctorio d.o.o. (a European corporation) is the data processor. This privacy Policy ("**Privacy Policy**") details Proctorio's use of Personally Identifiable Information (as defined below) about users of our Services."

Proctorio beschouwt zichzelf als verwerker als het gaat om het gebruik van de dienst. De software (SaaS service) van Proctorio wordt geïntegreerd in de LMS van de klant (i.c. onderwijsinstelling). Zodoende wordt de klant in staat gesteld zelf in de LMS de gewenste parameters in te stellen passende bij het af te nemen examen als ook de gevoeligheid te bepalen waarmee frauduleus gedrag van studenten kan worden gedetecteerd. Het doel en de middelen van de verwerking van persoonsgegevens wordt aldus bepaald door de onderwijsinstelling en vindt plaats in de LMS. Proctorio zegt hierover zelf:

> "Because we fully integrate with all learning management systems and test platforms, test taker data stays with the testing institution and not Proctorio.[8]"

De stelling dat Proctorio gezien kan worden als verwerker is juist. De klant (i.c. de onderwijsinstelling) zal een verwerkersovereenkomst met Proctorio moeten sluiten om de rollen en de bijbehorende verantwoordelijkheden vast te leggen .

Proctorio licht haar rol als verwerker van de Service toe, maar benoemt niet expliciet de rol van verwerkingsverantwoordelijk die zij (mogelijk) ook heeft. In haar Privacy Policy stelt Proctorio ten slotte dat zij ook persoonlijke gegevens (PII) verzamelt van gebruikers voor de volgende doeleinden:

> "(...) invite you to participate in surveys, questionnaires, contests, or to contact us with questions, comments, or to provide us with feedback, which due to the nature of some of these activities,...en gebruikt in geval: (...) to contact you to deliver certain services, news, or information related to the Services, verify your authority to use our Services, and improve the content and general administration of the Services."

In het algemeen geldt dat voor iedere verwerking van persoonsgegevens door de leverancier (i.c. Proctorio) buiten de overeengekomen doeleinden uit de verwerkersovereenkomst, de leverancier

[8] Integrity without barriers, https://proctorio.com/about/system-integration

zelfstandig verwerkingsverantwoordelijke is. Daarbij zal Proctorio zelfstandig een doel en rechtmatige grondslag moeten hebben.

Aanbevelingen

Als verwerker zal Proctorio toegang hebben – bijv. voor beheer en incidenten – tot de software en daarbij persoonsgegevens van studenten kunnen inzien en verwerken. Elke onderwijsinstelling zal als verwerkingsverantwoordelijke hiervoor een verwerkersovereenkomst met Proctorio moeten sluiten. In de verwerkersovereenkomst zal in ieder geval afspraken moeten worden gemaakt over welke gegevens worden verwerkt en voor hoe lang, wat de aard en het doel van de verwerking is en op welke manier de beveiliging van de gegevens is gewaarborgd.

Het is Proctorio niet toegestaan binnen de overeenkomst verkregen persoonsgegevens te gebruiken voor eigen doeleinden. Dit zal door de onderwijsinstelling moeten worden overeengekomen in de verwerkersovereenkomst.

4. Grondslagen

Introductie AVG beginsel

Bij het gebruik en de inzet van proctoring software bij toetsing en examinering worden persoonsgegevens van de student en de proctors (in geval van 'live proctoring' en 'record & review proctoring') verwerkt. Dit betekent dat er een juridische grondslag moet zijn om deze persoonsgegevens rechtmatig te verwerken.

De wet kent zes grondslagen. Het zijn de volgende:

1. Toestemming
2. Overeenkomst
3. Wettelijke verplichting
4. Bescherming van de vitale belangen van een betrokkene
5. Taak van algemeen belang
6. Gerechtvaardigd belang

Analyse van de (niet) AVG compliant onderdelen

In de Privacy Policy stelt Proctorio verschillende grondslagen te hebben om gegevens te verwerken welke afhankelijk zijn van de situatie. Zij noemt zowel toestemming, uitvoering van de overeenkomst als gerechtvaardigd belang. In specifieke situaties ook wettelijke verplichting.

> "Legal Basis for processing your information. If you are a user or located in the European Economic Area ("EEA"), our legal basis for collecting and using the personal information described above will depend on the personal information concerned and the specific context in which we collect it. We will normally collect personal information from you only where we have your consent to do so, where we need the personal information to perform a contract with you, or where the processing is in our legitimate business interests. In some cases, we may also have a legal obligation to collect personal information from you. If you have questions about or need further information concerning the legal basis on which we collect and use your personal information, please contact us using the contact details provided below."

Daarnaast geeft Proctorio aan onder de link 'GDPR' op haar website:

> "Legal Basis for Processing – we reviewed all processing activities to identify the legal basis for processing and ensuring that each basis is appropriate for the related activity. Where applicable, we also maintain records of our processing activities, ensuring that our obligations under Article 30 of GDPR and Schedule 1 of the Data Protection Bill are met."

Aanbevelingen

In de hoedanigheid van verwerker, zal Proctorio de gegevens verwerken in opdracht van de klant. De klant (i.c. de onderwijsinstelling) zal een juridische grondslag moeten hebben om deze gegevens van de betrokkenen (i.c. de studenten) in de applicatie te verzamelen en te verwerken.

In de hoedanigheid van verwerkingsverantwoordelijke kan Proctorio een van bovengenoemde grondslagen hebben om de PII, naam (email) adres, IP adres, etc. te verwerken. Hierbij kan gedacht worden aan toestemming voor het sturen van commerciële uitingen of het plaatsen en gebruikmaken van Cookies, aan gerechtvaardigd belang voor het sturen van services updates en aan het uitvoeren van de overeenkomst in geval dat een gebruiker zelf tegen betaling een dienst afneemt van Proctorio. Per geval zal bezien moeten worden welke situatie van toepassing is voor de onderwijsinstellingen en studenten.

5. Procedure om datalekken te melden en aansprakelijkheid

Introductie AVG beginsel

Er is sprake van een datalek bij een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens Afhankelijk van de omstandigheden van het geval moet een incident gemeld worden bij de (lokale) Privacy Autoriteit van de verwerkingsverantwoordelijke en bij de betrokkenen zelf.

De autoriteit moet binnen 72 uur geïnformeerd worden bij een datalek. Dit geldt altijd wanneer er persoonsgegevens betrokken zijn bij het incident. Uitzondering is wanneer het niet waarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

Onder de AVG is de verwerkingsverantwoordelijke (i.c. de onderwijsinstelling) aansprakelijk voor schade als gevolg van datalekken. Ook voor schade veroorzaakt door de verwerker. De verwerker is alleen aansprakelijk voor schade die is ontstaan, doordat deze verwerker niet aan de tot haar gerichte verplichtingen uit de AVG heeft voldaan (art. 28 AVG) of wanneer de verwerker buiten de instructies van de verwerkingsverantwoordelijke om heeft gehandeld. Deze instructies dienen in de verwerkersovereenkomst te zijn opgenomen.

Analyse van de (niet) AVG compliant onderdelen

Proctorio beschrijft in het kort de meldplicht procedure in haar Privacy Policy. Hierbij valt op dat Proctorio een datalek melding zowel aan de klant (i.c. onderwijsinstelling) als aan de betrokkenen binnen 72 uur na ontdekking van het incident per post zal melden. Dit is niet geheel conform de regels gesteld in de AVG (art. 33 en 34).

De AVG schrijft voor dat een inbreuk op de beveiliging van persoonsgegevens door een verwerkingsverantwoordelijke uiterlijk binnen 72 uur na ontdekking aan de privacy autoriteit dient plaats te vinden. Indien de inbreuk bij de verwerker plaatsvindt zal door de verwerker een melding bij de verwerkingsverantwoordelijk worden gedaan zodra hij kennis heeft genomen van het incident. I.c.

betekent dit dat Proctorio in haar rol van verwerker na ontdekking van een datalek zonder vertraging hiervan de onderwijsinstelling op de hoogte dient te brengen. Een melding van een datalek aan de betrokkene(n) vindt plaats als is vast te komen staan dat de inbreuk waarschijnlijk een hoog risico voor de rechten en vrijheden van de betrokkenen inhoudt. Deze melding aan betrokkenen wordt door de verwerkingsverantwoordelijke gedaan. Aan de melding aan de betrokkene is geen termijn verbonden, maar wel inhoudelijk vereisten waaraan de informatie moet voldoen.

Aanbevelingen

De meldplicht datalekken zoals beschreven in de Privacy Policy is niet volledig en juist.

Ten eerste zal Proctorio de meldplicht datalekken procedure moeten uitbreiden tot het melden van datalekken van 'persoonsgegevens' en niet uitsluitend tot het melden van datalekken van PII.

Daarnaast zal er een onderscheid gemaakt moeten worden in de rollen die Proctorio heeft. In geval er een inbreuk op de beveiliging van persoonsgegevens plaatsvindt waarvan Proctorio verwerkingsverantwoordelijk is zal Proctorio zelf – binnen 72 uur - de privacy toezichthouder moeten informeren en mogelijk de betrokkenen. Deze informatie en procedure dient zij ook in de Privacy Policy kenbaar te maken. In het geval dat er een inbreuk op de beveiliging van persoonsgegevens in het kader van de uitvoering van de dienst en dus in de rol van verwerker plaatsvindt zal Proctorio hierover zo spoedig mogelijk de klant (i.c. de onderwijsinstelling) moeten informeren.

I.c. betekent dit dat de onderwijsinstelling goeie afspraken dient te maken over de wijze waarop Proctorio een datalek dient te melden. Dit zal contractueel moeten worden vastgelegd in de verwerkersovereenkomst. Hierbij zal rekening moeten worden gehouden dat de onderwijsinstelling binnen 72 uur na ontdekking van het incident de toezichthouder moet informeren en zelf haar betrokkenen (studenten) wil informeren.

Aan de inhoud van de melding worden echter eisen gesteld (art. 33 en 34 AVG). Proctorio geeft weer wat zij minimaal zal vermelden richting de onderwijsinstelling dan wel betrokkenen. Deze opsomming is volledig en juist beschreven.

6. Bewaartermijnen

Introductie AVG beginsel

De AVG geeft geen concrete bewaartermijnen voor persoonsgegevens. De AVG geeft wel aan dat een persoonsgegeven alleen mag worden bewaard als identificeerbaar gegeven, voor zolang als het nodig is voor de doeleinden waarvoor het verzameld is. Dat betekent dus ook dat als de gegevens geanonimiseerd zijn en daarmee dus niet meer de directe of indirecte identificatie van een persoon mogelijk maken, gegevens langer bewaard mogen worden. De AVG schrijft ook voor dat de verwerkingsverantwoordelijke over de bewaartermijn voorafgaand aan de verzameling moet communiceren.

De belangrijkste processen voor onderwijsinstellingen zijn gericht op het opleiden van studenten en het verstrekken van bewijsstukken, die weergeven dat studenten de toetsen of examens met succes hebben afgelegd. In het geval van online proctoring zullen in beginsel de persoonsgegevens dan ook niet langer bewaard mogen worden dan voor het eventueel bewijs van rechtmatige toetsing noodzakelijk is. De verwerkingsverantwoordelijke zal de bewaartermijnen moeten bepalen en in een verwerkersovereenkomst voorschrijven op een dusdanige manier dat het ook technisch in te richten is in de applicatie.

Voor nadere onderbouwing van mogelijk vastgestelde bewaartermijnen voor toetsing en examinering voor de onderwijsinstellingen, wordt kortheidshalve verwezen naar de Selectielijst actualisatie 2016, voor de administratieve neerslag van de openbaargezag taken en niet-publiekrechtelijke werkprocessen van Nederlandse hogescholen.[9]

Analyse van de (niet) AVG compliant onderdelen

Over bewaartermijnen van informatie zegt Proctorio zelf in haar Privacy Policy:

> "Proctorio will store and maintain institutional data for up to 30 days after the termination of an applicable agreement, unless otherwise specified. If, however, you have entered into a SaaS Agreement with Proctorio then we will retain your data for six months by active data retention and for one year by cold storage. We may be able to retain your data for longer periods of time subject to an additional fee and agreement by you and Proctorio.
>
> According to the Institution's preference regarding data destruction, Proctorio will either: 1) destroy the data, or 2) deliver it to the Institution."

Bovendien stelt Proctorio onder de link 'GDPR' het volgende:

> "Data Retention & Erasure – we have updated our retention policy and schedule to ensure that we meet the 'data minimization' and 'storage limitation' principles and that personal information is stored, archived and destroyed compliantly and ethically. We have dedicated erasure procedures in place to meet the new 'Right To Be Forgotten' obligation and are aware of when this and other data subject's rights apply; along with any exemptions, response time frames and notification responsibilities."

Aanbevelingen

In beginsel is de onderwijsinstelling verantwoordelijk voor het vaststellen van de bewaartermijnen van de persoonsgegevens die worden opgeslagen en bewaard bij gebruikmaking van online proctoring tool van Proctorio. Deze termijnen zullen moeten worden voorgeschreven in de verwerkersovereenkomst. De onderwijsinstelling kan hierbij de selectielijst actualisatie 2016 als richtlijn gebruiken. Proctorio zal als ontwikkelaar van de tool moeten zorgdragen dat deze bewaartermijnen ook technisch uitvoerbaar zijn. Denk hierbij ook aan het correct en automatisch vernietigen van de gegevens na verloop van de bewaartermijn.

Dit betekent ook dat waar Proctorio in haar Privacy Policy aangeeft:

> "(…) If, however, you have entered into a SaaS Agreement with Proctorio then we will retain your data for six months by active data retention and for one year by cold storage. We may be able to retain your data for longer periods of time subject to an additional fee and agreement by you and Proctorio…",

deze bewaartermijnen niet of in ieder geval niet in alle gevallen van toepassing zijn.

[9] Vereniging Hogescholen, Selectielijst actualisatie 2016 voor de administratieve neerslag van de openbaar gezag taken en niet-publiekrechtelijke werkprocessen van Nederlandse scholen, https://www.verenigninghogescholen.nl/system/knowledge_base/attachments/files/000/000/583/original/VERE-3325-Selectielijst_hogescholen_2016_WEB.pdf?1467093338, blz. 73 en verder.

Voor wat betreft de bewaartermijnen van gegevens waarvoor Proctorio verwerkingsverantwoordelijke is, is het onduidelijk wat Proctorio bedoelt met 'institutional information' en 'your data' in haar Privacy Policy.

Bovendien is de 'geupdate retention policy', genoemd onder GDPR, niet beschikbaar. Welke bewaartermijnen Proctorio hanteert ten aanzien welke (categorieën) van persoonsgegevens is onbekend.

7. Subverwerkers en derde partijen

Introductie AVG beginsel

De verwerker verwerkt de persoonsgegevens in opdracht van de verwerkingsverantwoordelijke. De verwerker verwerkt gegevens volgens de instructies van en onder de verantwoordelijkheid van de verwerkingsverantwoordelijke, maar staat wel buiten de organisatie. Verder heeft de verwerker geen zeggenschap over het doel en de middelen van de verwerking. Beslissingen over het gebruik van de gegevens, de verstrekking aan derden, de duur van de opslag etc. worden genomen door de verwerkingsverantwoordelijke.

Een verwerker kan natuurlijk ook weer een derde partij inschakelen om werk voor hem uit te voeren. Deze onderaannemer noemen we dan een subverwerker. De verwerker mag een subverwerker alleen inschakelen na schriftelijk akkoord van de verwerkingsverantwoordelijke.[10]

Naast (sub-)verwerkers kan Proctorio verplicht worden aan derde partijen persoonsgegevens te verstrekken. Zo kan Proctorio als Amerikaans bedrijf verplicht worden een vordering tot het verstrekken van persoonsgegevens aan de Amerikaanse overheid te voldoen.

Analyse van de (niet) AVG compliant onderdelen

Over het inzetten van verwerkers door Proctorio wordt onder de link 'GDPR' wordt het volgende beschreven:

> "Processor Agreements – where we use any third-party to process personal information on our behalf (i.e. Payroll, Recruitment, Hosting, etc.), we have drafted compliant Processor Agreements and due diligence procedures for ensuring that they (as well as we), meet and understand their/our GDPR obligations. These measures include initial and ongoing reviews of the service provided, the necessity of the processing activity, the technical and organizational measures in place and compliance with GDPR."

Uit deze tekst valt in ieder geval op te maken dat derden partijen door Proctorio ingezet kunnen worden voor ondersteuning van de eigen bedrijfsvoering van Proctorio. Niet duidelijk is of Proctorio subverwerkers inzet ter ondersteuning van de dienstverlening aan klanten. Bij 'Hosting', kan gedacht worden aan een subverwerker, bijv. een derde partij die servers host voor Proctorio en haar klanten. Het woord 'hosting' is echter zo algemeen dat dit niet met zekerheid gesteld kan worden.

In de Privacy Policy wordt ook gerefereerd naar inzet van derden partijen:

> "Third Party Services - Proctorio uses a variety of services hosted by third parties to help provide our Services, such as hosting our various blogs, help center, and knowledge bases, and to help us understand the use of our Services. These services may collect information sent by your browser as part of a web page request, such as cookies or your IP request.

[10] artikel 28 lid 2 AVG

> We do not control third parties' tracking technologies. If you have any questions about these third-party technologies, you should contact the responsible provider directly."

Ook hier is door de woord keus en de uitleg onduidelijk of er sprake is van subverwerkers. De voorbeelden die aangedragen worden doet vermoeden dat Proctorio hier verwijst naar derde partijen, verwerkers, die ondersteuning bieden aan Proctorio als verwerkeringverantwoordelijken.

Over verstrekking van persoonsgegevens aan derden, niet zijnde (sub-)verwerkers zegt Proctiorio op haar website het volgende:

> "With respect to personal data received or transferred pursuant to the Privacy Shield frameworks, Proctorio is subject to the regulatory enforcement powers of the U.S. Federal Trade Commission (for issues pertaining to Privacy Shield). In situations where public authorities make lawful requests for information, such as to meet national security or law enforcement requirements, Proctorio may be required to disclose personal data.[11]"

Aanbevelingen

Uit de informatie beschikbaar kan niet worden opgemaakt of en zo ja, welke (sub-)verwerkers ingezet worden voor de uitvoering van de dienstverlening. Om te voldoen aan de AVG eisen zal verwerkingsverantwoordelijke (i.c. de onderwijsinstelling) hierover in een verwerkersovereenkomst duidelijkheid moeten creëren en afspraken maken. Navraag bij Proctorio leert dat Proctorio nog geen 'Processor Agreement' beschikbaar heeft voor klanten. De onderwijsinstelling zal hiervoor haar eigen verwerkersovereenkomst moeten gebruiken.

Mede gelet op de mogelijkheid dat Proctorio verplicht kan worden persoonsgegevens te verstrekken aan de Amerikaanse overheid in het kader van strafrechtelijk onderzoek of nationale veiligheid onder de US Cloud Act zal de verwerkingsverantwoordelijke extra alert moeten zijn op de verstrekking en opslag van persoonsgegevens door Proctorio in en buiten de Verenigde Staten.

8. Rechten van betrokkenen

Introductie AVG beginsel

Betrokkenen hebben het recht op inzage, correctie, wijziging, beperking van de verwerking, of verwijdering van hun persoonsgegevens. En daarnaast hebben betrokkenen het recht van bezwaar en het recht om niet onderworpen te worden aan een uitsluitend op geautomatiseerde verwerking gebaseerd besluit. In het onderstaande worden de rechten in het kort toegelicht.

Recht van inzage: een betrokkene mag een organisatie vragen of het persoonsgegevens heeft vastgelegd en zo ja, welke. Hiervoor hoeft betrokkene geen specifieke reden te noemen. Het recht op inzage betreft alleen inzage in iemands eigen gegevens.

Recht van correctie: een betrokkene mag verzoeken om gegevens te corrigeren, te wijzigen of om gegevens aan te vullen.

Recht van verwijdering: een betrokkene mag een organisatie verzoeken om persoonsgegevens te verwijderen.

[11] Hier wordt vermoedelijk gerefereerd naar de US Cloud Act (maart 2018), deze wet geeft Amerikaanse autoriteiten de bevoegdheid om gegevens op te vragen bij bedrijven die in de VS elektronische communicatiediensten of remote computing-diensten aanbieden.

Recht van bezwaar: een betrokkene mag bezwaar maken tegen verwerking van zijn gegevens. In geval van bezwaar tegen direct marketingactiviteiten dient de verwerkingsverantwoordelijke hieraan altijd gehoor te geven.

Recht van beperking van de verwerking: een betrokkene heeft het recht om opgeslagen persoonsgegevens door een organisatie te laten bevriezen en markeren met als doel de verdere verwerking (tijdelijk) stop te zetten.

Recht van dataportabiliteit: een betrokkene heeft het recht om gegevens van zichzelf over te laten dragen naar een ander. Bijvoorbeeld leengegevens over laten dragen van de ene bibliotheek naar de andere.

Profilering: verwerking waarbij aan de hand van persoonsgegevens persoonlijke aspecten van een betrokkene worden geëvalueerd om zo bijvoorbeeld beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen;

Analyse van de (niet) AVG compliant onderdelen

Proctorio stelt onder de link 'GDPR' op de website het volgende over de rechten van betrokkene:

> "In addition to the policies and procedures mentioned above that ensure individuals can enforce their data protection rights, we provide easy to access information via our website of an individual's right to access any personal information that Proctorio processes about them and to request information about:
>
> - (...)
> - The right to have incomplete or inaccurate data about them corrected or completed and the process for requesting this
> - The right to request erasure of personal data (where applicable) or to restrict processing in accordance with data protection laws, as well as to object to any direct marketing from us and to be informed about any automated decision-making that we use
> - (...)"

De link 'Privacy & Cookies' die leidt naar de Privacy Policy, licht de verschillende rechten nog toe in paragraaf '*European Economic Area (EEA) of Switserland'.* In deze paragraaf worden het inzage recht, correctie en verwijdering, het recht van verzet en de mogelijkheid om een klacht in te dienen bij de lokale autoriteit weergegeven. Het recht op vergetelheid, - beperking van de verwerking en - overdraagbaarheid van gegevens mist echter. Hierbij dient wel weer opgemerkt te worden dat Proctorio zich in haar Privacy Policy beperkt tot PII. De rechten van betrokkenen gelden ten aanzien van het bredere begrip persoonsgegevens uit de AVG.

Aanbevelingen

Proctorio dient er voor zorg te dragen dat de informatie over de bovengenoemde rechten van betrokkenen beschikbaar is op haar website juist en volledig is. Het niet volledige informeren van de betrokkene, kan gezien worden als een overtreding van art van de AVG voor zover Proctorio als verwerkingsverantwoordelijk gegevens van betrokkene verwerkt.

Daarnaast zullen onderwijsinstellingen in een verwerkersovereenkomst duidelijke afspraken moeten maken over de wijze waarop Proctorio bijstand zal verlenen aan de onderwijsinstelling indien een student een beroep doet op haar rechten.

9. Bijstand verlenen voor nakoming AVG compliance

Introductie AVG beginsel

Als verwerker is Proctorio verplicht[12] om verwerkingsverantwoordelijke, i.c. de instelling, te helpen in haar rol als verwerkingsverantwoordelijke voor de verwerking om aan haar wettelijke verplichtingen te kunnen voldoen. Denk hierbij aan meewerken aan de uitvoering van audits, data protection impact assessments, en meewerken aan onderzoeken van toezichthouders of verzoeken van betrokkenen.

Analyse van de (niet) AVG compliant onderdelen

In de beschikbare informatie wordt niets vermeld over de verplichting van Proctorio om medewerking te verlenen aan verwerkingsverantwoordelijke in geval van audits, onderzoeken van autoriteiten of verzoeken van betrokkenen.

Aanbevelingen

Het is gebruikelijk dat afspraken hierover, inclusief het dragen van de kosten ervan, tussen verantwoordelijke en verwerker worden vastgelegd in een verwerkersovereenkomst. De onderwijsinstelling zal dan ook hieraan de nodige aandacht moeten besteden.

10. Geautomatiseerde besluitvorming

Introductie AVG beginsel

Geautomatiseerde besluitvorming is een geautomatiseerde verwerking van persoonsgegevens ter beoordeling van persoonlijke aspecten van een natuurlijke persoon, zonder menselijke tussenkomst op basis waarvan vervolgens een besluit genomen wordt.

Profilering is een verwerking waarbij aan de hand van persoonsgegevens persoonlijke aspecten van een betrokkene worden geëvalueerd om zo bijvoorbeeld beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.

Bij online proctoring moet rekening worden gehouden met geautomatiseerde besluitvorming en profilering[13]. Het inzetten van online proctoring om fraude te kunnen detecteren kan negatieve gevolgen hebben voor de student. Wanneer er met online proctoring een geautomatiseerd besluit wordt genomen zonder menselijke tussenkomst, waardoor de student een sanctie of maatregel krijgt opgelegd, zoals een schorsing, heeft dit negatieve gevolgen voor de student. Volledig geautomatiseerde besluitvorming met online proctoring is dan ook niet toegestaan onder de AVG. Het is een vereiste dat er bij zulke besluiten altijd een beoordeling door een docent of examinator plaatsvindt.

[12] Artikel 28 lid 3 e en f AVG
[13] Artikel 22 AVG

Analyse van de (niet) AVG compliant onderdelen

Uit de beschikbare informatie valt niet op te maken of en in welke vorm er geautomatiseerde besluitvorming dan wel profilering door Proctorio plaatsvindt. Gelet op – het doel van- de dienstverlening en de wijze waarop studenten gemonitord worden met behulp van de software, is het aannemelijk dat er enige vorm van profilering plaatsvindt en mogelijk ook geautomatiseerde besluitvorming.

Aanbevelingen

Aanbevolen wordt te verifiëren of en voor hoe ver er aan geautomatiseerde besluitvorming dan wel profilering wordt gedaan. In het geval de onderwijsinstelling de Proctorio software wenst in te zetten zal zij hierover afspraken moeten vastleggen in de overeenkomst met Proctorio en transparant hierover communiceren naar studenten.

ProctorExam

ProctorExam, met haar hoofdvestiging in Amsterdam, Nederland biedt een online proctoring service. Met maximaal drie monitoringoplossingen, variërend van screensharing tot een 360° zicht op de werkruimte van een kandidaat met behulp van de smartphones van de kandidaten, biedt ProctorExam flexibiliteit voor testorganisatoren, om zich aan te passen aan alle online beoordelingscontexten.[14] ProctorExam biedt een aantal instellingen voor elke beoordeling, van live proctoring tot eenvoudige schermbewaking tot dubbele mobiele weergave. Met ProctorExam is interactie mogelijk via een learning management system, LMS, of testapplicatie[15]. Downloaden van een applicatie is niet nodig. Een plugin voor de browser is voldoende om gebruik te kunnen maken van ProctorExam. Met ProctorExam kan gebruik gemaakt worden van 'live proctoring' en ' opslag en controle achteraf'.[16]

Bronnen die zijn gebruikt bij de juridische analyse van ProctorExam:

- https://proctorexam.com/test-taker-support/, geraadpleegd op 4 april 2020.
- De privacyverklaring van ProctorExam: https://proctorexam.com/privacy-and-data-security/, geraadpleegd op 4 april 2020.
- De verwerkersovereenkomst van ProctorExam (versie 17 maart 2020), https://drive.google.com/file/d/1Aq6dkHCI_WrEqHBNC8oSFluwed98Msoq/view
- De Algemene Voorwaarden van ProctorExam (versie 17 maart 2020), https://partners.proctorexam.com/terms_and_conditions/

1. Definitie en gebruik van persoonsgegevens

Introductie AVG beginsel

Een persoonsgegeven is een gegeven over een geïdentificeerde of identificeerbare natuurlijke persoon. Informatie die direct over iemand gaat of naar iemand te herleiden is, zijn persoonsgegevens. Een persoonsgegeven is een stukje informatie dat zonder al te veel moeite herleidbaar is tot een individu (een identificeerbare persoon). Dat kan een (persoons)naam zijn, maar ook een telefoonnummer, (e-mail)adres en zelfs het IP-adres van een computer. Ook camerabeelden, telefoongesprekken, kentekens, persoonlijke verificatiecodes, paspoortgegevens, BSN en andere zaken vallen hier onder.

Analyse van de (niet) AVG compliant onderdelen

ProctorExam gebruikt de volgende definitie van persoonsgegevens in de verwerkersovereenkomst:

> "Personal Data" means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person."

[14] https://proctorexam.com/, geraadpleegd op 4 april 2020.
[15] https://proctorexam.com/solutions-for-higher-education/, geraadpleegd op 4 april 2020.
[16] Voor meer informatie over deze drie hoofdcategorieën van proctoring wordt verwezen naar de Whitepaper Online Proctoring van Surfnet https://www.surf.nl/files/2019-04/whitepaper-online-proctoring.pdf

In de verwerkersovereenkomst van ProctorExam wordt er gebruik gemaakt van de definitie van persoonsgegevens van de AVG.

In de Privacy Policy op de website (privacyverklaring) van ProctorExam wordt er geen definitie gegeven van persoonsgegevens. In het algemeen is het niet duidelijk welke definities er worden gehanteerd in de privacyverklaring van ProctorExam.

Aanbevelingen

ProctorExam zal de informatie over de (categorieën van) persoonsgegevens die zij verwerkt naar klanten en gebruikers toe moeten aanvullen en makkelijk toegankelijk maken wil zij voldoen aan de AVG. Dit betekent dat ProctorExam haar privacyverklaring moet aanvullen en de definitie met betrekking tot persoonsgegevens uit de AVG wordt gehanteerd.

2. Versturen van persoonsgegevens naar landen buiten de Europese Economische Ruimte

Introductie AVG beginsel

Persoonsgegevens doorgeven vanuit Nederland naar het buitenland mag alleen als een land voldoende bescherming biedt. Binnen de Europese Economische Ruimte (EER) is dit gewaarborgd door de AVG. Voor doorgifte naar landen buiten de EER gelden aparte regels.

Als een land buiten de EER in de nationale wetgeving een passend niveau van gegevensbescherming biedt, kan de Europese Commissie (EC) een 'adequaatheidsbeslissing' nemen (artikel 45 van de AVG). De EC stelt dan vast dat de gegevensbescherming in dat land van een vergelijkbaar niveau is als de AVG.

Als er een adequaatheidsbeslissing is genomen, hoeft er voor doorgifte naar dat land of die sector geen aanvullende waarborg te worden getroffen.

Het EU-VS Privacy Shield is een voorbeeld van een adequaatheidsbeslissing, met het verschil dat de beslissing alleen geldt voor zover het ontvangende bedrijf zich heeft gecertificeerd en zich houdt aan de principes die zijn vastgelegd in het Privacy Shield.

Als er geen sprake is van een adequaatheidsbeslissing, dan moet er een andere passende waarborg zijn als een organisatie persoonsgegevens wil doorgeven aan een land buiten de EU. Dat kan met een EU modelovereenkomst die door de Europese Commissie is vastgesteld (artikel 46 (2) onder c) of Bindende bedrijfsvoorschriften zijn (artikel 47). Dit laatste zijn 'global privacy policies' die gelden binnen organisaties voor doorgifte van persoonsgegevens naar landen zonder adequaat beschermingsniveau (derde landen) wereldwijd. Alle werknemers en entiteiten binnen het concern (ook de Nederlandse en Europese vestigingen) moeten zich houden aan deze interne global privacy policy.

Analyse van de (niet) AVG compliant onderdelen

Volgende privacyverklaring van ProctorExam worden de persoonlijke data gehost in Frankfurt, Duitsland. Verder maakt ProctorExam volgens de privacyverklaring gebruik van:

– Amazon Web Services physically store your data in data centers inside of the EU
– Google cloud also physically store your data in data centers inside of the EU

In de verwerkersovereenkomst staat een uitgebreider overzicht van verwerkers waar ProctorExam gebruikt van maakt:

Processor name - Processor activity - Hosting location

1. Tawk.To - Live chat functionality provider - Republic of Ireland
2. Amazon AWS - Streaming service provider - Platform hosting provider Germany
3. Google Cloud - Streaming service provider - Platform hosting provider Belgium
4. MonitorEdu - Invigilation support and technical support - USA
5. Google Analytics - Visit monitoring web application USA - EU
6. Sengrid - Transactional emails - USA

In de verwerkersovereenkomst staat het volgende:

> "***ProctorExam*** *agrees and warrants that it is prohibited from transferring Personal Data outside of* ***Europe/the U.S.*** *except if it obtains the explicit written consent of* ***The Client*** *and provided that the Personal Data are transferred to a country which has been considered to provide an adequate level of protection under EU Data Protection Law or to a data recipient which has implemented adequate safeguards under EU Data Protection Law such as ap-proved Binding Corporate Rules or the Privacy Shield Framework*."

Hierbij geeft ProctorExam aan dat er in beginsel geen persoonsgegevens buiten Europa of de VS worden getransporteerd, behalve wanneer de onderwijsinstelling schriftelijk toestemming geeft en wanneer het land of de ontvanger waar de persoonsgegevens naar worden verzonden adequate maatregelen heeft getroffen om de persoonsgegevens te beschermen. Opvallend is de toevoeging '***the U.S***.' in de eerste regel van deze bepaling. Dit is in niet in lijn met de AVG, want ook wanneer ProctorExam persoonsgegevens binnen de VS wil verwerken heeft ProctorExam eerst schriftelijke toestemming nodig van de onderwijsinstelling.

En in de verwerkersovereenkomst staat ook:

> "*In the context of the Service, The Client agrees that ProctorExam transfers or stores Personal Data Processed on behalf of The Client in the United States as necessary to perform services on behalf of The Client. ProctorExam agrees to protect Personal Data in the United States in compliance with EU Data Protection Law, and this Agreement and will not use the Personal Data transferred to the United States for its own purposes."*[17]

Hieruit blijkt ook dat er persoonsgegevens buiten de EER worden verwerkt. Het is echter niet duidelijk welke concrete maatregelen voor de bescherming van persoonsgegevens worden getroffen.

Aanbevelingen

ProctorExam mag alleen gegevens van klanten in de EER overbrengen naar landen met een adequaat niveau van gegevensbescherming. ProctorExam moet elke mogelijke overdracht naar landen buiten de EER in detail beschrijven en de uitdrukkelijke en voorafgaande toestemming van de klant verkrijgen voor de overdracht aan specifieke subverwerkers in specifieke landen. Het is wel aan te raden hier de nodige aandacht aan te besteden in het geval ProctorExam zich bedient van subverwerkers die in de Verenigde Staten gevestigd zijn. Het EU-V.S. Privacy Shield is al enkele jaren onderwerp van discussie. Privacy voorvechters stellen dat het regime onvoldoende de AVG standaarden waarborgt, het principe van '*je eigen vlees keuren*' (zelfcertificering) niet voldoet en een regelmatige controle door de Amerikaanse overheid of de bedrijven ook daadwerkelijk de regels naleven te wensen overlaat.

[17] Artikel 5.2 Data Processing Agreement ProctorExam, 17 maart 2020.

3. Rol van ProctorExam onder de AVG en doelbinding

Introductie AVG beginsel

Rol van ProctorExam: De wet maakt onderscheid tussen de verwerkingsverantwoordelijke (degene die verantwoordelijk is voor de verwerking van persoonsgegevens) en de verwerker (degene die in opdracht van de verwerkingsverantwoordelijke persoonsgegevens verwerkt).

Verwerkingsverantwoordelijke (ook wel verantwoordelijke): de verwerkingsverantwoordelijke is degene die (1) het doel en (2) de middelen van de verwerking vaststelt.

(1) Het gaat erom wie uiteindelijk bepaalt of er gegevens worden verwerkt en zo ja, welke verwerkingen er plaatsvinden, welke persoonsgegevens verwerkt worden en voor welk doel.

(2) Bij het bepalen van de middelen gaat het erom op welke wijze de verwerking van persoonsgegevens zal plaatsvinden, bijvoorbeeld met software.

Verwerker: de verwerker verwerkt de persoonsgegevens in opdracht van de verwerkingsverantwoordelijke. De verwerker verwerkt gegevens volgens de instructies van en onder de verantwoordelijkheid van de verwerkingsverantwoordelijke, maar staat wel buiten de organisatie. Verder heeft de verwerker geen zeggenschap over het doel en de middelen van de verwerking. Beslissingen over het gebruik van de gegevens, de verstrekking aan derden, de duur van de opslag etc. worden genomen door de verwerkingsverantwoordelijke. Voorbeelden zijn de IT-dienstverleners die via hun onlinedienst gegevens verwerken (bijvoorbeeld Dropbox), software leveranciers, callcenters en partijen die (digitale) nieuwsbrieven versturen namens de gemeente.

De verwerkingsverantwoordelijke is verplicht een overeenkomst aan te gaan met de verwerker, de zogenaamde verwerkersovereenkomst.

Subverwerker: een verwerker kan natuurlijk ook een ander inschakelen om werk voor hem uit te voeren. Deze onderaannemer noemen we dan een subverwerker. In de verwerkersovereenkomst is vaak bepaald dat een subverwerker alleen mag worden ingeschakeld na schriftelijk akkoord van de verwerkingsverantwoordelijke.

Doelbinding

Een verwerking mag alleen plaatsvinden als er een duidelijk omschreven en gerechtvaardigd doel is. De persoonsgegevens die worden verzameld mogen vervolgens ook niet verder worden verwerkt op een manier die niet te verenigen is met dat doel.

Analyse van de (niet) AVG compliant onderdelen

ProctorExam als verwerker

ProctorExam ziet zichzelf als een verwerker voor de organisaties die ProctorExam gebruiken.

> "Your education institution decides which data we can process, and how we can use it. ProctorExam will never process data in any other way or for any other purpose than what is agreed with your educational institution."

De organisatie die ProctorExam gebruikt, bepaalt welke persoonsgegevens er worden verwerkt. Dit kunnen onder andere de volgende persoonsgegevens zijn: Naam van de examinandus, E-mailadres van de examinandus, Studenten- of werknemers-ID-nummer - of gepseudonimiseerde identificatoren zoals Kandidaat-ID, Schermopname van de PC van de examinandus, Webcam opname van uw omgeving inclusief uw gezicht, Smartphone camera opname van uw omgeving en

Geassocieerd exameninstituut van de examinandus.[18] In de verwerkersovereenkomst in Annex 1 staat ook nog "Any other data relating to individuals provided to ProctorExam via the Services, by (or at the direction of) Customer or by Customer End Users."

Wanneer er gebruik wordt gemaakt van ProctorExam kunnen de volgende persoonsgegevens gebruikt worden voor de volgende doeleinden:

- Om je als gebruiker te identificeren
- Om je omgeving te monitoren om het mogelijk te maken de integriteit van het examen te beschermen
- En om ervoor te zorgen dat de persoonsgegevens alleen zichtbaar zijn door diegene die daar een goede reden en goedkeuring voor hebben.

ProctorExam verzamelt daarnaast informatie over de 'browser and operating system' en je IP adres voor de volgende doeleinden:

> "We use this data to make the services work on your device, to aid troubleshooting, and to document user behaviour relevant to the correctness of the exam."
>
> "We also log user-related events on the system to support and control the workflow. For instance, we log an event if staff members view or alter exam sets."[19]

De bovenstaande verwerkingen voor het kunnen bieden van de diensten, de troubleshooting en gegevens over 'user behaviour' gerelateerd aan de juistheid van de afgenomen examens doet ProctorExam in zijn rol als verwerker. Het is niet duidelijk wat met de term 'support and control the workflow' wordt bedoeld. Dit zou beter gespecificeerd moeten worden. Gaat het hier om het loggen gelet op het raadplegen en aanpassen van de examens, dan hangt het samen met het doel van de diensten en worden de verwerkingen gedaan vanuit de verwerkersrol. Of gaat het hier om een verwerking dat meer omvat? Hier zal duidelijkheid over moeten worden verkregen.

In de verwerkersovereenkomst zegt ProctorExam daar het volgende over:

> "The Client appoints ProctorExam as Processor, for the Processing of Personal Data for the purpose of providing the Services specified in the Principal Agreement as implemented by each individual Statement of Work. In that context, The Client, as Controller has the sole and exclusive authority to determine the purposes and means of the Processing of Personal Data that are disclosed to and collected by the ProctorExam. ProctorExam will Process Personal Data only on behalf and for the benefit of The Client and only to carry out its obligations under the Principal Agreement as implemented and to the extent required by each individual Statement of Work and The Client's written instructions. ProctorExam shall not share, transfer, transmit, disclose or otherwise provide access to or make available any Personal Data to any third party unless The Client has authorized ProctorExam to do so in writing."

ProctorExam als verwerkingsverantwoordelijke

ProctorExam verwerkt ook persoonsgegevens als verwerkingsverantwoordelijke:

> "ProctorExam stores and processes data from customers, vendors, and employees.
>
> We only do this when we have a lawful basis to do so – to fulfill contracts and deliver agreed

[18] https://proctorexam.com/privacy-and-data-security/, onder Privacy for Test Takers, What personal data do we hold and for what purpose?, geraadpleegd op 3 april 2020.
[19] https://proctorexam.com/privacy-and-data-security/, onder Privacy for Test Takers, Data we collect automatically when you use ProctorExam, geraadpleegd op 3 april 2020.

services, or if we identify a legitimate interest by having conversations with prospects and vendors.

If we want to send you information regarding our services, that is not any of the above, we will ask for your explicit consent to receive the communication. You can unsubscribe at any time."[20]

Bovenstaande verwerkingen zijn verwerkingen die ProctorExam als verwerkingsverantwoordelijke doet. Dit zijn niet de enige verwerkingen die ProctorExam als verwerkingsverantwoordelijke doet, ProctorExam maakt ook gebruik van de persoonsgegevens voor "secondary use". ProctorExam zegt daarover op hun website dat: "We anonymize data before making secondary use of them in statistics."[21] In het gedeelte op de website wat gaat over ProctorExam als een verwerkingsverantwoordelijke wordt niks gezegd over deze analyses. Het is niet duidelijk of ProctorExam deze analyses maakt op verzoek van de organisaties/klanten of dat ProctorExam deze analyses voor eigen doeleinden verricht. Daarnaast is de beschrijving van het doel "statistics" niet specifiek genoeg. ProctorExam mag alleen de persoonsgegevens van de onderwijsinstelling voor eigen doeleinden gebruiken wanneer ProctorExam hier toestemming van de onderwijsinstelling voor heeft gekregen.

Aanbevelingen

In de verwerkersovereenkomst moeten concretere afspraken worden gemaakt over welke gegevens worden verwerkt, voor hoe lang, wat de grondslag is en wat de aard en het doel van de verwerking is.

ProctorExam is de verwerker voor de klant en daarmee bepaalt de klant welke persoonsgegevens ProctorExam voor welke doeleinden verwerkt. ProctorExam mag deze persoonsgegevens alleen voor eigen doeleinden verwerken met toestemming van de klant/onderwijsinstelling.

De huidige doelen die nu worden genoemd in de privacyverklaring voor "secondary use" en het gebruik voor "statistics" zijn te breed en niet specifiek genoeg. ProctorExam mag alleen de persoonsgegevens van de onderwijsinstelling voor eigen doeleinden gebruiken wanneer ProctorExam hier toestemming van de onderwijsinstelling voor heeft gekregen. Kortom het is belangrijk om te weten:

- Welke specifieke gegevens verzamelt ProctorExam voor 'secondary use' en 'statistics?
- Welke gebruiks- en/of inhoudelijke gegevens kunnen precies worden verwerkt voor ondersteuningsdoeleinden?
- Verzamelt ProctorExam 'stille' bug- en of crashrapporten, of alleen als een klant actief vraagt om voor hulp?
- Kan ProctorExam gedetailleerde informatie en voorbeelden van 'geanonimiseerde, geaggregeerde analyses' publiceren?

4. Grondslagen

Introductie AVG beginsel

Bij het gebruik en de inzet van proctoring software bij toetsing en examinering worden persoonsgegevens van de student en de proctors (in geval van 'live proctoring' en 'record & review

[20] https://proctorexam.com/privacy-and-data-security/, onder Privacy Outside of a Test, ProctorExam as a Data Controller, geraadpleegd op 3 april 2020.
[21] https://proctorexam.com/privacy-and-data-security/, onder Privacy for Test Takers, How does ProctorExam store and protect you information, geraadpleegd op 3 april 2020.

proctoring') verwerkt. Dit betekent dat er een juridische grondslag moet zijn om deze persoonsgegevens rechtmatig te verwerken.

De wet kent zes grondslagen. Het zijn de volgende:

1. Toestemming
2. Overeenkomst
3. Wettelijke verplichting
4. Bescherming van de vitale belangen van een betrokkene
5. Taak van algemeen belang
6. Gerechtvaardigd belang

Analyse van de (niet) AVG compliant onderdelen

In geen een van de juridische documenten worden de grondslagen omschreven op basis waarvan de verwerkingen plaatsvinden. Dit wordt niet genoemd in de verwerkersovereenkomst of Annex 1 van de verwerkersovereenkomst en niet in de privacyverklaring. Daarnaast wordt er ook niet onderbouwd op basis van welke grondslagen ProctorExam de persoonsgegevens mag gebruiken voor 'secondary use' en 'statistics'. De enige informatie over grondslagen die te vinden is, is dit gedeelte in de privacyverklaring: "ProctorExam uses this data to identify you as a user, to monitor your environment in order to safeguard the exam integrity and to ensure that data is only viewable by those who have a legitimate reason (and permission) to do so." Deze tekst is niet specifiek genoeg.

Aanbevelingen

In de hoedanigheid van verwerker, zal ProctorExam de gegevens verwerken in opdracht van de klant. De klant (i.c. de onderwijsinstelling) zal een juridische grondslag moeten hebben om deze gegevens van de betrokkenen (i.c. de studenten) in de applicatie te verzamelen en te verwerken.

In de hoedanigheid van verwerkingsverantwoordelijke kan ProctorExam een van bovengenoemde grondslagen hebben om de persoonsgegevens. te verwerken. Hierbij kan gedacht worden aan toestemming voor het sturen van commerciële uitingen of het plaatsen en gebruikmaken van Cookies, aan gerechtvaardigd belang voor het sturen van services updates. Per geval zal bezien moeten worden welke situatie van toepassing is voor de onderwijsinstellingen en studenten.

ProctorExam moet een specifieke en uitputtende lijst van verwerkingsdoeleinden opstellen, zodat haar klanten de juiste wettelijke basis voor elk doel van de gegevensverwerking kunnen bepalen. Dit kan een groot aantal specifieke doeleinden omvatten, zoals "onderhoud van de dienst", "beveiliging van de dienst", "verbetering van de dienst/en of de inkomsten", "het opstellen van statistieken", "het verzenden van facturen", "het reageren op juridische processen/bevelen van de wetshandhaving", enz.

5. Procedure om datalekken te melden en aansprakelijkheid

Introductie AVG beginsel

Er is sprake van een datalek bij een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens. Afhankelijk van de omstandigheden van het geval moet een incident gemeld worden bij de (lokale) Privacy Autoriteit van de verwerkingsverantwoordelijke en bij de betrokkenen zelf.

De autoriteit moet binnen 72 uur geïnformeerd worden bij een datalek. Dit geldt altijd wanneer er persoonsgegevens betrokken zijn bij het incident. Uitzondering is wanneer het niet waarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

Onder de AVG is de verwerkingsverantwoordelijke (i.c. de onderwijsinstelling) aansprakelijk voor schade als gevolg van datalekken. Ook voor schade veroorzaakt door de verwerker. De verwerker is alleen aansprakelijk voor schade die is ontstaan, doordat deze verwerker niet aan de tot haar gerichte verplichtingen uit de AVG heeft voldaan (art. 28 AVG) of wanneer de verwerker buiten de instructies van de verwerkingsverantwoordelijke om heeft gehandeld. Deze instructies dienen in de verwerkersovereenkomst te zijn opgenomen.

Analyse van de (niet) AVG compliant onderdelen

ProctorExam heeft als verwerker de plicht om datalekken zo snel mogelijk te melden bij de onderwijsinstelling, die als verwerkingsverantwoordelijke optreedt. Daarnaast moet ProctorExam maatregelen nemen om de impact van een datalek zo snel mogelijk te verkleinen. Het volgende staat hierover in de verwerkersovereenkomst:

> "**ProctorExam** will inform **The Client** in writing, without undue delay, and no later than 48 forty eight) hours after having become aware of a Personal Data Breach. **ProctorExam** will assist **The Client** in complying with its own obligations or with **The Client**'s customers' obligations under EU Data Protection Law to notify a Personal Data Breach. Parties must document all Personal Data Breaches, including the facts relating to the Personal Data Breach, its effects and the remedial actions taken. **ProctorExam** must promptly take all necessary corrective actions (at its sole cost and expense), and must cooperate fully with **The Client**, acting as a Controller or a Processor on behalf of its customers, in all reasonable and lawful efforts to mitigate the effects of Personal data Breach."

ProctorExam geeft aan volledig (en op haar kosten) mee te werken met de onderwijsinstelling bij een datalek, zoals ook verplicht is onder de AVG.[22]

In de verwerkersovereenkomst is niet geconcretiseerd hoe het datalek teruggekoppeld moet worden aan de onderwijsinstelling. Hoe wordt het datalek praktisch gecommuniceerd naar de onderwijsinstelling? Er moeten tussen ProctorExam en de onderwijsinstelling afspraken gemaakt worden over welke informatie, binnen welke termijn, op welke wijze, en met welke contactpersoon gecommuniceerd moet worden.

De AVG schrijft voor dat een inbreuk op de beveiliging van persoonsgegevens door een verwerkingsverantwoordelijke uiterlijk binnen 72 uur na ontdekking aan de privacy autoriteit dient plaats te vinden. Indien de inbreuk bij de verwerker plaatsvindt zal door de verwerker een melding bij de verwerkingsverantwoordelijk worden gedaan zodra hij kennis heeft genomen van het incident. I.c. betekent dit dat ProctorExam in haar rol van verwerker na ontdekking van een datalek zonder vertraging hiervan de onderwijsinstelling op de hoogte dient te brengen. Een melding van een datalek aan de betrokkene(n) vindt plaats als is vast te komen staan dat de inbreuk waarschijnlijk een hoog risico voor de rechten en vrijheden van de betrokkenen inhoudt. Deze melding aan betrokkenen wordt door de verwerkingsverantwoordelijke gedaan. Aan de melding aan de betrokkene is geen termijn verbonden, maar wel inhoudelijk vereisten waaraan de informatie moet voldoen.

In de verwerkersovereenkomst staat geen bepaling opgenomen over aansprakelijkheid ten aanzien van datalekken. Er staat nergens in de verwerkersovereenkomst dat de bepalingen, zoals aansprakelijkheid (zie ook art. 7 Terms and Conditions), uit de verwerkersovereenkomst waar deze

[22] Artikel 28 lid 3 sub f AVG

afwijken van de Terms and Conditons gelden boven de Terms and Conditions. Dit is een specifiek punt ten aanzien van aansprakelijkheid waar goed naar gekeken moet worden.

Aanbevelingen

ProctorExam moet dergelijke inbreuken en door haar subverwerkers zo snel mogelijk aan de onderwijsinstelling melden. Verantwoordelijken voor de verwerking moeten een datalek binnen 72 uur na het bekend worden ervan melden bij de Autoriteit Persoonsgegevens. In geval van een ernstige inbreuk, met grote gevolgen voor de gegevensbescherming van de betrokkenen, is de termijn van 48 uur die ProctorExam heeft om de onderwijsinstelling te informeren, te lang. Aangezien er consequenties kunnen zijn voor de betrouwbaarheid en integriteit van de examens. En er waarschijnlijk publiciteit kan zijn die klanten en/of eindgebruikers al waarschuwt vóór een officiële kennisgeving door ProctorExam.

Daarom wordt geadviseerd de termijn van 48 uur te wijzigen in 24 uur in geval van ernstige inbreuken op de beveiliging. Zodat de onderwijsinstelling kan voldoen aan zijn 72-uursverplichting om datalekken aan de Autoriteit Persoonsgegevens en/of de betrokkenen te melden.

Daarnaast is het niet duidelijk welke informatie ProctorExam deelt met de onderwijsinstelling over het beveiligingsincident of datalek. Het advies is om een extra bijlage op te nemen in de verwerkersovereenkomst waarin dit geregeld wordt. In de bijlage worden afspraken gemaakt over welke informatie, binnen welke termijn, op welke wijze, aan welke contactpersoon geleverd moet worden.

Zorg ervoor dat er ten aanzien van aansprakelijkheid en datalekken goede afspraken worden gemaakt in de verwerkersovereenkomst.

6. Bewaartermijnen

Introductie AVG beginsel

Bewaartermijnen worden gebruikt als hulpmiddel om data-minimalisatie te realiseren. De AVG geeft wel aan dat een persoonsgegeven alleen mag worden bewaard als identificeerbaar gegeven, voor zolang als het nodig is voor de doeleinden waarvoor het verzameld is. Dat betekent dus ook dat als de gegevens geanonimiseerd zijn en daarmee dus niet meer de directe of indirecte identificatie van een persoon mogelijk maken, gegevens langer bewaard mogen worden. De AVG schrijft ook voor dat de verwerkingsverantwoordelijk over de bewaartermijn voorafgaand aan de verzameling moet communiceren.

De belangrijkste processen voor onderwijsonderwijsinstellingen zijn gericht op het opleiden van studenten en het verstrekken van bewijsstukken, die weergeven dat studenten de toetsen of examens met succes hebben afgelegd. In het geval van online proctoring zullen in beginsel de persoonsgegevens dan ook niet langer bewaard mogen worden dan voor het eventueel bewijs van rechtmatige toetsing noodzakelijk is. De verwerkingsverantwoordelijke zal de bewaartermijnen moeten bepalen en in een verwerkersovereenkomst voorschrijven op een dusdanige manier dat het ook technisch in te richten is in de applicatie.

Voor nadere onderbouwing van mogelijk vastgestelde bewaartermijnen voor toetsing en examinering voor de onderwijsonderwijsinstellingen, wordt kortheidshalve verwezen naar de

Selectielijst actualisatie 2016, voor de administratieve neerslag van de openbaargezag taken en niet-publiekrechtelijke werkprocessen van Nederlandse hogescholen.[23]

Analyse van de (niet) AVG compliant onderdelen

ProctorExam legt op hun website uit dat de organisatie die de tests afneemt bepaalt hoelang de persoonsgegevens worden bewaard. In Annex 1 van de verwerkersovereenkomst van ProctorExam wordt bovenstaande bevestigd:

> "*The Client decides and controls retention periods and can at any moment delete personal data that is processed on its behalf by ProctorExam, including all back-ups of personal data*.[24]"

In Annex 3 van de verwerkersovereenkomst staat dat ProctorExam een Deletion Procedure heeft. Het is niet duidelijk op welke manier ProctorExam de bewaartermijnen en verwijdering van persoonsgegevens in de praktijk (technisch) uitvoert en kan uitvoeren. In de verwerkersovereenkomst staat niet wat er gebeurt wanneer de onderwijsinstelling de persoonsgegevens verwijdert en of de onderwijsinstelling een bevestiging van ProctorExam krijgt wanneer de persoonsgegeven zijn verwijderd zowel uit het systeem als uit de back-ups (bij beëindiging van de overeenkomst).

Aanbevelingen

In beginsel is de onderwijsonderwijsinstelling verantwoordelijk voor het vaststellen van de bewaartermijnen van de persoonsgegevens die worden opgeslagen en bewaard bij gebruikmaking van online proctoring tool van ProctorExam. De onderwijsonderwijsinstelling kan hierbij de selectielijst actualisatie 2016 als richtlijn gebruiken. ProctorExam zal als ontwikkelaar van de tool moeten zorgdragen dat deze bewaartermijnen ook technisch uitvoerbaar zijn. Denk hierbij ook aan het correct en automatisch vernietigen van de gegevens na verloop van de bewaartermijn. Daarnaast is het dringend advies om in de verwerkersovereenkomst op te nemen dat de persoonsgegevens na de beëindiging van de overeenkomst verwijderd en/of overgedragen worden (zowel in het systeem als in de back up) en dat de onderwijsinstelling een bevestiging krijgt van ProctorExam wanneer de persoonsgegevens verwijderd zijn.

7. Subverwerkers en derde partijen

Introductie AVG beginsel

De verwerker verwerkt de persoonsgegevens in opdracht van de verwerkingsverantwoordelijke. De verwerker verwerkt gegevens volgens de instructies van en onder de verantwoordelijkheid van de verwerkingsverantwoordelijke, maar staat wel buiten de organisatie. Verder heeft de verwerker geen zeggenschap over het doel en de middelen van de verwerking. Beslissingen over het gebruik van de gegevens, de verstrekking aan derden, de duur van de opslag etc. worden genomen door de verwerkingsverantwoordelijke.

Een verwerker kan natuurlijk ook weer een derde partij inschakelen om werk voor hem uit te voeren. Deze onderaannemer noemen we dan een subverwerker. In de verwerkersovereenkomst is vaak

[23] Vereniging Hogescholen, Selectielijst actualisatie 2016 voor de administratieve neerslag van de openbaar gezagtaken en niet-publiekrechtelijke werkprocessen van Nederlandse scholen, < https://www.verenigingenhogescholen.nl/system/knowledge_base/attachments/files/000/000/583/original/VERE-3325-Selectielijst_hogescholen_2016_WEB.pdf?1467093338 >, blz. 73 en verder.

[24] Data Processing Agreement ProctorExam, 17 maart 2020, blz. 8.

bepaald dat een subverwerker alleen mag worden ingeschakeld na schriftelijk akkoord van de verwerkingsverantwoordelijke. Daarnaast is de verwerker aansprakelijk en verantwoordelijk voor de subverwerker[25].

Analyse van de (niet) AVG compliant onderdelen

De persoonsgegevens die worden verwerkt door ProctorExam worden gehost in Frankfurt, Duitsland. Verder maakt ProctorExam gebruik van:

– Amazon Web Services physically store your data in data centers inside of the EU
– Google cloud also physically store your data in data centers inside of the EU

In de verwerkersovereenkomst staat een uitgebreider overzicht van verwerkers waar ProctorExam gebruikt van maakt:

Processor name - Processor activity - Hosting location

1. Tawk.To - Live chat functionality provider - Republic of Ireland
2. Amazon AWS - Streaming service provider - Platform hosting provider Germany
3. Google Cloud - Streaming service provider - Platform hosting provider Belgium
4. MonitorEdu - Invigilation support and technical support - USA
5. Google Analytics - Visit monitoring web application USA - EU
6. Sengrid - Transactional emails - USA

In de verwerkersovereenkomst staat opgenomen dat de onderwijsinstelling voorafgaande toestemming heeft gegevens voor het gebruik van bovenstaande subverwerkers:

> "**ProctorExam** has appointed the Sub-Processors that are listed in Annex 2 to Process Personal Data in the context of the Services specified in the Principal Agreement and each individual Statement of Work with **The Client's** prior written consent."

ProctorExam beschrijft op hun website dat ze geen data verkoopt aan derde partijen.[26]

In de algemene voorwaarden zegt ProctorExam, dat:

> "*ProctorExam may subcontract or delegate any of its obligations under this Agreement to any subcontractors, affiliates, or delegates in its sole discretion.*[27]"

En in de verwerkersovereenkomst van ProctorExam staat het volgende:

> "The Client specifically authorizes the engagement of ProctorExam's affiliates as Sub-Processors. In addition, The Client generally authorizes the engagement of any other third parties as a Sub-processor."

Uit deze tekst valt in ieder geval op te maken dat derden partijen door ProctorExam ingezet kunnen worden voor ondersteuning van de uitvoering van de verplichtingen onder de overeenkomst. Hiermee wordt bedoeld dat ProctorExam subverwerkers kan inzetten voor de ondersteuning van de dienstverlening aan klanten. Dit onderdeel van de algemene voorwaarden spreekt de tekst in de privacyverklaring op de website tegen. Op de website staat, dat alleen wanneer de organisatie die ProctorExam gebruikt er mee instemt, worden er oplossingen van derde partijen ingezet om persoonsgegevens te verwerken.

[25] Artikel 28 lid 4 AVG
[26] https://proctorexam.com/privacy-and-data-security/, onder Privacy Outside of a Test, ProctorExam as Data Controller, geraadpleegd op 4 april 2020.
[27] https://partners.proctorexam.com/terms_and_conditions/, onder 9, geraadpleegd op 6 april 2020.

Verder staat in de verwerkersovereenkomst:

> "ProctorExam will notify The Client 45 days prior to engaging any new Sub-processors. The Client can object to the engagement of any new Sub-processors by sending a written reasoned objection. If ProctorExam cannot remove the objections, both parties can terminate the principal agreement.[28]"

ProctorExam mag alleen subverwerkers inschakelen met voorafgaande schriftelijke goedkeuringen van de onderwijsinstelling.[29] ProctorExam licht de onderwijsinstelling schriftelijk in over de beoogde veranderingen. De onderwijsinstelling heeft hierbij de mogelijkheid om bezwaar te maken.

ProctorExam zegt op haar website dat ProctorExam geen data verkoopt aan derde partijen. Het is goed om de verkoop van persoonsgegevens na te gaan bij ProctorExam, zodat de onderwijsinstelling zeker weet dat er ook geen persoonsgegeven worden gedeeld met andere partijen.

Aanbevelingen

Alleen met akkoord van de verwerkingsverantwoordelijke, in dit geval de onderwijsinstelling, mag ProctorExam derde partijen inschakelen voor de dienstverlening aan de onderwijsinstelling. Daarnaast is het advies dat met ProctorExam wordt afgesproken dat ProctorExam de onderwijsinstelling ruim van tevoren op de hoogte stelt indien ProctorExam een nieuwe subverwerker wil inschakelen. Deze periode is nodig om de onderwijsinstelling voldoende tijd te geven om de overeenkomst te beëindigen indien de onderwijsinstelling ernstige bezwaren heeft tegen een dergelijke subverwerker.

Ten aanzien van subverwerkers van ProctorExam die in de Verenigde Staten gevestigd zijn, zal de verwerkingsverantwoordelijke extra alert moeten zijn op de verstrekking en opslag van persoonsgegevens door ProctorExam – en haar subverwerkers – in en buiten de Verenigde Staten. Mede gelet op de mogelijkheid dat partijen verplicht kunnen worden persoonsgegevens te verstrekken aan de Amerikaanse overheid in het kader van strafrechtelijk onderzoek of nationale veiligheid onder de US Cloud Act.

8. Rechten van betrokkenen

Introductie AVG beginsel

Betrokkenen hebben het recht op inzage, correctie, wijziging, beperking van de verwerking, of verwijdering van hun persoonsgegevens. En daarnaast hebben betrokkenen het recht van bezwaar en het recht om niet onderworpen te worden aan een uitsluitend op geautomatiseerde verwerking gebaseerd besluit. In het onderstaande worden de rechten in het kort toegelicht.

Recht van inzage: een betrokkene mag een organisatie vragen of het persoonsgegevens heeft vastgelegd en zo ja, welke. Hiervoor hoeft betrokkene geen specifieke reden te noemen. Het recht op inzage betreft alleen inzage in iemands eigen gegevens.

Recht van correctie: een betrokkene mag verzoeken om gegevens te corrigeren, te wijzigen of om gegevens aan te vullen.

Recht van verwijdering: een betrokkene mag een organisatie verzoeken om persoonsgegevens te verwijderen.

[28] Artikel 6.3 Data Processing Agreement ProctorExam, 17 maart 2020.

[29] Artikel 28 lid 2 AVG

Recht van bezwaar: een betrokkene mag bezwaar maken tegen verwerking van zijn gegevens. In geval van bezwaar tegen direct marketingactiviteiten dient de verwerkingsverantwoordelijke hieraan altijd gehoor te geven.

Recht van beperking van de verwerking: een betrokkene heeft het recht om opgeslagen persoonsgegevens door een organisatie te laten bevriezen en markeren met als doel de verdere verwerking (tijdelijk) stop te zetten.

Recht van dataportabiliteit: een betrokkene heeft het recht om gegevens van zichzelf over te laten dragen naar een ander. Bijvoorbeeld leengegevens over laten dragen van de ene bibliotheek naar de andere.

Profilering: verwerking waarbij aan de hand van persoonsgegevens persoonlijke aspecten van een betrokkene worden geëvalueerd om zo bijvoorbeeld beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.

Analyse van de (niet)l AVG compliant onderdelen

ProctorExam stelt het volgende in de verwerkersovereenkomst:

> "ProctorExam will immediately inform **The Client,** in writing, in relation to any Personal Data Processed in the context of the Services of: (i) any Data Subjects' requests to their rights of (a) access, (b) rectification, (c) erasure, (d) data portability, (e) restriction of Processing, and (f) objection to the Processing; (ii) any request or complaint received from **The Client'**s customers, consumers, employees or from any other individual" en
>
> "**ProctorExam** agrees and warrants that it will provide a copy of any such requests within 48 (forty eight) hours and that it will respond to such requests only in accordance with **The Client**'s prior written authorization and instructions. **Proctor- Exam** will assist **The Client** in fulfilling its obligations or **The Client'**s customers' obligations to respond to individuals' requests in accordance with EU Data Protection Law" en
>
> "ProctorExam will cooperate with **The Client** to comply with EU Data Protection Law, this Agreement, **The Client'**s customers' instructions when **The Client** acts as Processor, and to assist **The Client** fulfil its own obligations under EU Data Protection Law and as applicable **The Client**'s customer's instructions, including complying with Data Subjects' requests to exercise their rights, replying to complaints from Data Subjects, replying to investigation and inquiries from supervisory authorities, conducting data protection impact assessments and prior consultations with supervisory authorities ("Cooperation and Assistance")."

ProctorExam werkt kosteloos mee met verzoeken van betrokkenen[30], klachten van betrokkenen, verzoeken van autoriteiten en met het van een data protection impact assessment (DPIA). Dit is in lijn met de verplichtingen die een verwerker heeft onder de AVG[31].

Op de website staat niets vermeld over het uitoefenen van de rechten die je als gebruiker hebt. Als verwerker en in haar rol als verwerkingsverantwoordelijke heeft ProctorExam de plicht om transparant naar betrokkenen te zijn. Het feit dat er niet over de rechten van betrokkenen op de website staat voldoet niet aan het transparantiebeginsel.

[30] Artikel 28 lid 2 sub e AVG
[31] Artikel 28 lid 3 sub f AVG

Aanbevelingen

ProctorExam dient er voor zorg te dragen dat de informatie over de rechten van betrokkenen beschikbaar op haar website juist en volledig is. Het niet volledige informeren van de betrokkene, kan gezien worden als een overtreding van artikel 13 en/of 14 van de AVG. Dit is verplicht voor ProctorExam als ProctorExam in de hoedanigheid van verwerkingsverantwoordelijk gegevens van betrokkene verwerkt.

Daarnaast zullen onderwijsinstellingen in een verwerkersovereenkomst duidelijke afspraken moeten maken over de wijze waarop ProctorExam bijstand zal verlenen aan de onderwijsinstelling indien een student een beroep doet op haar rechten.

9. Bijstand verlenen voor nakoming AVG compliance

Introductie AVG beginsel

Als verwerker is ProctorExam verplicht om de onderwijsinstelling, in haar rol als verwerkings-verantwoordelijke van de verwerkingen,[32] te helpen om aan haar wettelijke verplichtingen te voldoen. Denk hierbij aan meewerken aan de uitvoering van audits, data protection impact assessments, onderzoeken van toezichthouders en verzoeken van betrokkenen.

Analyse van de (niet) AVG compliant onderdelen

In de verwerkersovereenkomst van ProctorExam staat niets opgenomen over de kosten voor het meehelpen aan rechten van betrokken, DPIA's, informeren over datalekken aan de onderwijsinstelling en maatregelen treffen om de impact van de datalek zo klein mogelijk te maken en het doen van audits. Zie hiervoor ook onder 8. Rechten van Betrokkenen en 5. Procedure om datalekken te melden.

Aanbevelingen

Het is gebruikelijk dat afspraken over het dragen van de kosten om de onderwijsinstelling mee te helpen om aan haar wettelijke verplichtingen te voldoen, worden vastgelegd in een verwerkersovereenkomst. De onderwijsinstelling zal dan ook hieraan de nodige aandacht moeten besteden om dit op te nemen in de verwerkersovereenkomst.

10. Geautomatiseerde besluitvorming en profilering

Introductie AVG beginsel

Geautomatiseerde besluitvorming is een geautomatiseerde verwerking van persoonsgegevens ter beoordeling van persoonlijke aspecten van een natuurlijke persoon, zonder menselijke tussenkomst op basis waarvan vervolgens een besluit genomen wordt.

Profilering is een verwerking waarbij aan de hand van persoonsgegevens persoonlijke aspecten van een betrokkene worden geëvalueerd om zo bijvoorbeeld beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.

[32] Artikel 28 lid 3 sub e en f AVG

Bij online proctoring moet rekening worden gehouden met geautomatiseerde besluitvorming en profilering[33]. Het inzetten van online proctoring om fraude te kunnen detecteren kan negatieve gevolgen hebben voor de student. Wanneer er met online proctoring een geautomatiseerd besluit wordt genomen zonder menselijke tussenkomst, waardoor de student een sanctie of maatregel krijgt opgelegd, zoals een schorsing, heeft dit negatieve gevolgen voor de student. Volledig geautomatiseerde besluitvorming met online proctoring is dan ook niet toegestaan onder de AVG. Het is een vereiste dat er bij zulke besluiten altijd een beoordeling door een docent of examinator plaatsvindt.

Analyse van de (niet) AVG compliant onderdelen

Uit de beschikbare informatie valt niet op te maken of en in welke vorm er geautomatiseerde besluitvorming dan wel profilering door ProctorExam plaatsvindt. Gelet op – het doel van- de dienstverlening en de wijze waarop studenten gemonitord worden met behulp van de software, is het aannemelijk dat er enige vorm van profilering plaatsvindt en mogelijk ook geautomatiseerde besluitvorming.

Aanbevelingen

Aanbevolen wordt te verifiëren of en voor hoe ver er aan geautomatiseerde besluitvorming dan wel profilering wordt gedaan. In het geval de onderwijsinstelling de ProctorExam software wenst in te zetten zal zij hierover afspraken moeten vastleggen in de overeenkomst met ProctorExam en transparant hierover communiceren naar studenten.

[33] Artikel 22 AVG

RPNow (PSI online)

RPNow (Remote Proctor Now) is een dienst van PSI Services LCC, met haar hoofdvestiging in Glendale, California, Verenigde Staten. Haar Europese vestigingen zijn in het Verenigd Koninkrijk, Zwitserland en Zweden. RPNow zegt op haar website over haar software het volgende: "RPNow is een on-demand service waarmee online de toetsomgeving van studenten kan worden beveiligd en de mogelijkheid wordt geboden om ID verificatie te doen. RPNow biedt een 'opslag en controle achteraf' oplossing. Dit betekent voornamelijk dat de software geluid en video beelden opslaat, welke vervolgens door een examinator (proctor) versneld worden terug gekeken om te controleren op onregelmatigheden."[34] RPNow kan met elk learning management systeem (LMS) worden gebruikt door middel van rechtstreekse LTI-integratie. Dit stelt tevens de onderwijsinstelling instaat om alle beschikbare instellingen en informatie rechtstreeks binnen het LMS te beheren. Studenten kunnen inloggen in de persoonlijke en bekende leeromgeving van de onderwijsinstelling zonder dat dit installatie van software op de computer van de student vereist .

Voor de juridische analyse van RPNow software zijn de volgende bronnen gebruikt:

- PSI online Privacy Policy, versie van 1 januari 2020, https://www.psionline.com/en-gb/privacy
- Data Processing Agreement PSI, versie 18 maart 2018, https://www.psionline.com/en-gb/privacy/gdpr-compliance/data-processing-agreement
- Lijst met subverwerkers, geraadpleegd op 8 april 2020, https://www.psionline.com/en-gb/privacy/gdpr-compliance/sub-processors
- PSI Privacy Shield Policy, geraadpleegd op 8 april 2020, https://www.psionline.com/en-gb/psi-privacy-shield-policy

Op de website zijn geen Algemene voorwaarden of andere vergelijkbare voorwaarden gepubliceerd. De inhoud van de algemene voorwaarden zijn dan ook niet meegenomen in deze analyse.

1. Definitie en gebruik van persoonsgegevens

Introductie AVG beginsel

Een persoonsgegeven is een gegeven over een geïdentificeerde of identificeerbare natuurlijke persoon. Informatie die direct over iemand gaat of naar iemand te herleiden is, zijn persoonsgegevens. Een persoonsgegeven is een stukje informatie dat zonder al te veel moeite herleidbaar is tot een individu (een identificeerbare persoon). Dat kan een (persoons)naam zijn, maar ook een telefoonnummer, (e-mail)adres en zelfs het IP-adres van een computer. Ook camerabeelden, telefoongesprekken, kentekens, persoonlijke verificatiecodes, paspoortgegevens, BSN en andere zaken vallen hier onder.

Analyse van (niet) AVG compliant onderdelen

In de privacyverklaring van RPNow is het niet duidelijk welke definitie van persoonsgegevens RPNow hanteert. In het algemeen is het niet duidelijk welke definities er worden gehanteerd in de privacyverklaring van RPNow.

[34] voor meer informatie over deze drie hoofdcategorieën van proctoring wordt verwezen naar de Whitepaper Online Proctoring van Surfnet https://www.surf.nl/files/2019-04/whitepaper-online-proctoring.pdf

In de verwerkersovereenkomst gebruikt RPNow de volgende definitie voor persoonsgegevens:

> "Personal Data" means the data described in Annex 1 (*Details of Processing of Personal Data*) and any other personal data, as that term is defined in Data Protection Laws, processed by Supplier or any Subprocessor on behalf of Customer."

Deze zin geeft een indicatie dat de definities uit de privacywetgeving van de verwerkingsverantwoordelijke, de onderwijsinstelling, van toepassing is. Hetzelfde geldt voor andere definities die worden gehanteerd in de verwerkersovereenkomst:

> "Terms such as "(sub)process/(sub)processing", "data subject", "data processor, "data controller", "personal data breach", "data protection impact assessment", "appropriate technical and organisational measures", "recipient" shall have the same meaning ascribed to them in the Data Protection Laws"

Aanbevelingen

RPNow zal de informatie over de (categorieën van) persoonsgegevens die zij verwerkt naar klanten en gebruikers toe moeten verduidelijken, aanvullen en makkelijk toegankelijk maken, wil zij voldoen aan de AVG. Zorg ervoor dat door RPNow wordt bevestigd dat de definities uit de AVG worden gehanteerd in de verwerkersovereenkomst en privacyverklaring. Zodat RPNow in haar privacyverklaring en de verwerkersovereenkomst de definities uit de AVG hanteert en deze beide documenten dusdanig en in overeenstemming aanpast.

2. Versturen van persoonsgegevens naar landen buiten de Europese Economische Ruimte

Introductie AVG beginsel

Persoonsgegevens doorgeven vanuit Nederland naar het buitenland mag alleen als een land voldoende bescherming biedt. Binnen de Europese Economische Ruimte (EER) is dit gewaarborgd door de AVG. Voor doorgifte naar landen buiten de EER gelden aparte regels.

Als een land buiten de EER in de nationale wetgeving een passend niveau van gegevensbescherming biedt, kan de Europese Commissie (EC) een 'adequaatheidsbeslissing' nemen (artikel 45 van de AVG). De EC stelt dan vast dat de gegevensbescherming in dat land van een vergelijkbaar niveau is als de AVG.

Als er een adequaatheidsbeslissing is genomen, hoeft er voor doorgifte naar dat land of die sector geen aanvullende waarborg te worden getroffen.

Het EU-VS Privacy Shield is een voorbeeld van een adequaatheidsbeslissing, met het verschil dat de beslissing alleen geldt voor zover het ontvangende bedrijf (i.c. RPNow) zich heeft gecertificeerd en zich houdt aan de principes die zijn vastgelegd in het Privacy Shield.

Als er geen sprake is van een adequaatheidsbeslissing, dan moet er een andere passende waarborg zijn als een organisatie persoonsgegevens wil doorgeven aan een land buiten de EU. Dat kan met een EU modelovereenkomst die door de Europese Commissie is vastgesteld (artikel 46 (2) onder c) of Bindende bedrijfsvoorschriften zijn (artikel 47). Dit laatste zijn 'global privacy policies' die gelden binnen organisaties voor doorgifte van persoonsgegevens naar landen zonder adequaat beschermingsniveau (derde landen) wereldwijd. Alle werknemers en entiteiten binnen het concern (ook de Nederlandse en Europese vestigingen) moeten zich houden aan deze interne global privacy policy.

Analyse van (niet) AVG compliant onderdelen

RPNow heeft het volgende in de verwerkersovereenkomst staan:

> "Supplier shall not (permanently or temporarily) process the Personal Data nor permit any Authorised Subprocessor to (permanently or temporarily) process the Personal Data in a country outside of the EEA without an adequate level of protection as defined in Data Protection Laws other than in respect of those recipients in such countries listed at https://www.psionline.com/privacy-policy (Authorised Transfers of Personal Data), unless authorised in writing by Customer in advance."

Uit bovenstaande kan worden opgemaakt dat persoonsgegevens van EER ingezetenen kunnen worden verwerkt buiten de EER en meer specifiek in de Verenigde Staten. RPNow geeft aan dat er geen persoonsgegevens buiten Europa worden getransporteerd, behalve wanneer het land of de ontvanger waar de persoonsgegevens naar worden getransporteerd adequate maatregelen heeft getroffen om de persoonsgegevens te beschermen, tenzij de klant (i.c. de onderwijsinstelling) daarvoor toestemming heeft gegeven. Daarnaast maakt RPNow gebruik van een heel aantal subverwerkers[35]. Het is niet duidelijk waar de subverwerkers hun persoonsgegevens verwerken en welke maatregelen de subverwerkers hebben getroffen. Het is dus onduidelijk waar persoonsgegevens van EER gebruikers worden opslagen en verwerkt en er wordt geen garantie of mogelijkheid gegeven om persoonsgegevens van EER ingezetenen uitsluitend binnen de EU te verwerken.

RPNow zegt het volgende over de certificering van de EU-U.S. Privacy Shield:

> "Supplier has certified to the EU-US Privacy Shield Programme and shall process Customer Data in the United States. When requested by Customer, and to the extent required by applicable Data Protection Laws, Supplier shall promptly enter into (or procure that any relevant Subprocessor of Supplier enters into) an applicable agreement for data transfer such as the Standard Contractual Clauses and/or such variation as Data Protection Laws might require, in respect of any processing of Personal Data in a country outside of the European Economic Area without an adequate level of protection."

RPNow zegt in bovenstaande dat RPNow op verzoek van de onderwijsinstelling, en wanneer noodzakelijk om aan de AVG te voldoen, ervoor zorgt dat elke subverwerker die RPNow inschakelt een Standard Contractual Clauses of een equivalent afsluit met RPNow. RPNow is als verwerker verantwoordelijk voor de subverwerkers die RPNow inschakelt. RPNow moet ervoor zorgen dat de subverwerkers die worden ingeschakeld door RPNow de verplichtingen onder de AVG nakomen en naleven. Dit is geen keuzemogelijkheid, maar een verplichting onder de AVG[36].

Daarnaast staat in de privacyverklaring van RPNow het volgende:

> "We may share your personal information within the PSI Group. This will involve transferring your information outside the European Economic Area (EEA)."

Het is niet zomaar toegestaan om persoonsgegevens binnen een concern te delen. Onderdelen van een concern worden gezien als verschillende bedrijven. Hiervoor moeten dus apart afspraken gesloten worden, zoals verwerkersovereenkomsten of binding corporate rules.

[35] https://www.psionline.com/en-gb/privacy/gdpr-compliance/sub-processors/, geraadpleegd op 8 april 2020.
[36] Artikel 28 lid 4 AVG

Aanbevelingen

RPNow moet elke mogelijke overdracht naar landen buiten de EER in detail beschrijven en de uitdrukkelijke en voorafgaande toestemming van de klant verkrijgen voor de overdracht aan specifieke subverwerkers in specifieke landen. Met de EU-VS Privacy Shield zelfcertificering bewijst RPNow dat zij aan de eisen van het Privacy Shield voldoen. Een EU modelovereenkomst is dan dus niet meer nodig indien een onderwijsonderwijsinstelling een SaaS-overeenkomst sluit met RPNow. Dit betekent overigens niet dat een verwerkersovereenkomst overbodig is. Het is aan te bevelen hieraan de nodige aandacht te besteden. Het EU-V.S. Privacy Shield is al enkele jaren onderwerp van discussie. Privacy voorvechters stellen dat het regime onvoldoende de AVG standaarden waarborgt, het principe van '*je eigen vlees keuren*' (zelfcertificering) niet voldoet en een regelmatige controle door de Amerikaanse overheid of de bedrijven ook daadwerkelijk de regels naleven te wensen overlaat.

Daarnaast moet RPNow ervoor zorgen dat de subverwerkers die worden ingeschakeld door RPNow de verplichtingen onder de AVG nakomen en naleven. Dit is geen keuzemogelijkheid, maar een verplichting onder de AVG. Daarnaast moeten er, om binnen het concern persoonsgegevens te kunnen delen, aparte afspraken worden gemaakt door bijvoorbeeld het afsluiten van verwerkersovereenkomsten of binding corporate rules.

3. Rol van RPNow onder de AVG en doelbinding

Introductie AVG beginsel

De rol van RPNow: De wet maakt onderscheid tussen de verwerkingsverantwoordelijke (degene die verantwoordelijk is voor de verwerking van persoonsgegevens) en de verwerker (degene die in opdracht van de verwerkingsverantwoordelijke persoonsgegevens verwerkt).

Verwerkingsverantwoordelijke (ook wel verantwoordelijke): de verwerkingsverantwoordelijke is degene die (1) het doel en (2) de middelen van de verwerking vaststelt.

(1) Het gaat erom wie uiteindelijk bepaalt of er gegevens worden verwerkt en zo ja, welke verwerkingen er plaatsvinden, welke persoonsgegevens verwerkt worden en voor welk doel.
(2) Bij het bepalen van de middelen gaat het erom op welke wijze de verwerking van persoonsgegevens zal plaatsvinden, bijvoorbeeld met software.

Verwerker: de verwerker verwerkt de persoonsgegevens in opdracht van de verwerkingsverantwoordelijke. De verwerker verwerkt gegevens volgens de instructies van en onder de verantwoordelijkheid van de verwerkingsverantwoordelijke, maar staat wel buiten de organisatie. Verder heeft de verwerker geen zeggenschap over het doel en de middelen van de verwerking. Beslissingen over het gebruik van de gegevens, de verstrekking aan derden, de duur van de opslag etc. worden genomen door de verwerkingsverantwoordelijke. Voorbeelden zijn de IT-dienstverleners die via hun onlinedienst gegevens verwerken (bijvoorbeeld Dropbox), software leveranciers, callcenters en partijen die (digitale) nieuwsbrieven versturen namens de gemeente.

De verwerkingsverantwoordelijke is verplicht een overeenkomst aan te gaan met de verwerker, de zogenaamde verwerkersovereenkomst.

Subverwerker: een verwerker kan natuurlijk ook een ander inschakelen om werk voor hem uit te voeren. Deze onderaannemer noemen we dan een subverwerker. In de verwerkersovereenkomst is vaak bepaald dat een subverwerker alleen mag worden ingeschakeld na schriftelijk akkoord van de verwerkingsverantwoordelijke.

Doelbinding

Een verwerking mag alleen plaatsvinden als er een duidelijk omschreven en gerechtvaardigd doel is. De persoonsgegevens die worden verzameld mogen vervolgens ook niet verder worden verwerkt op een manier die niet te verenigen is met dat doel.

Analyse van (niet) AVG compliant onderdelen

RPNow beschouwt zichzelf als een verwerker. Over het verwerken van persoonsgegevens wordt het volgende gezegd in de verwerkersovereenkomst:

> "Supplier shall process the Personal Data relating to the categories of data subjects for the purposes set forth in this Agreement, which are enumerated in Annex 1 (*Details of Processing of Personal Data*) to this Agreement. Supplier shall not process, transfer, modify, amend or alter the Personal Data, or disclose or permit the disclosure of the Personal Data to any third party other than in accordance with Customer's documented instructions (whether in the Agreement or otherwise) except as otherwise required by applicable EU law to which Supplier is subject, in which case Supplier shall, to the extent permitted by such law, inform Customer of that legal requirement before processing that Personal Data."

In Annex 1 van de verwerkersovereenkomst staat het volgende en enige doel omschreven:

> "*The nature and purpose of the processing of Personal Data* Processing of data subjects' data for the purpose of testing or testing related service provided by Supplier at the request of Customer.[37]"

In de privacyverklaring staat het volgende over online proctoring en worden de volgende doeleinden genoemd:

> "Remote Proctoring: We may collect Identity Information through remote proctoring. We provide a service whereby clients who may conduct examinations outside of our examination centres use our remote proctoring service. This service requires the users to log onto our Remote Proctoring platform and the user takes the exam while being monitored through their webcam, microphone and through their computer's desktop which are all accessible to a remote examiner. We collect this information for identity verification, conducting the examination, for fraud prevention, security and integrity, and as otherwise required by law."

Volgens de verwerkersovereenkomst verwerkt RPNow dus alleen persoonsgegevens om de service van online proctoring voor de onderwijsinstelling mogelijk te maken. Dat is erg breed geformuleerd en daar kunnen allerlei verwerkingen onder vallen. In de privacyverklaring worden de doeleinden iets meer gespecificeerd: identiteit verificatie, afnemen van het examen, fraudepreventie, beveiliging en integriteit en andere doeleinden bij wet verplicht. De doeleinden moeten beter omschreven en gespecificeerd worden in de verwerkersovereenkomst en in de privacyverklaring.

RPNow verwerkt onder andere de volgende persoonsgegevens om de service tot stand te kunnen brengen:

> "The types of personal information that PSI may collect in order to provide its services include, but are not limited to: (1) name; (2) address; (3) email address; (4) telephone number; (5) payment card information; (6) scoring, ranking, and assessment data; (7) psychometric

[37] Annex 1 Details of processing of personal data, Data Processing Agreement PSI, 18 maart 2018, https://www.psionline.com/en-gb/privacy/gdpr-compliance/data-processing-agreement/, geraadpleegd op 8 april 2020.

test respondent data; (8) Photo ID and (9) and any other information generated from such personal information as a result of PSI providing its services.[38]"

RPNow licht haar rol als verwerker in de verwerkersovereenkomst toe, maar benoemt niet expliciet de rol van verwerkingsverantwoordelijke die zij (mogelijk) ook heeft. In haar Privacy Policy stelt RPNow dat RPNow persoonsgegevens verwerkt op basis van het gerechtvaardigde belang van RPNow voor de volgende doeleinden:

> "Legitimate Business Purpose. We process personal information where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests. This includes activities related to everyday business operations, such as invoice processing, business planning, improving the content of our Site, improving our products and services, undertaking transactional and statistical analysis and related research, and handling client service-related queries and complaints. We also may use the information that we learn about you to assist us in advertising our Services on third party websites.[39]"

Het is niet duidelijk wat doeleinden, zoals *'improving our products and services'*, *'undertaking transactional and statistical analysis and related research'* en *'we may also use the information that we learn about you to assist us in advertising our Services on third party websites'* betekenen. Deze doeleinden zijn (te) breed geformuleerd en niet specifiek genoeg. RPNow mag alleen met toestemming van de onderwijsinstelling de persoonsgegevens die voor de online proctoring van de onderwijsinstelling worden gebruikt, gebruiken voor andere doeleinden dan de onderwijsinstelling RPNow heeft opgedragen en heeft vastgelegd in de verwerkersovereenkomst.

Aanbevelingen

In de verwerkersovereenkomst moeten concretere afspraken worden gemaakt over welke gegevens worden verwerkt, voor hoe lang, wat de grondslag is en wat de aard en het doel van de verwerking is.

RPNow is de verwerker voor de onderwijsinstelling en daarmee bepaalt de onderwijsinstelling welke persoonsgegevens RPNow voor welke doeleinden verwerkt. RPNow mag deze persoonsgegevens alleen voor eigen doeleinden verwerken met toestemming van de onderwijsinstelling.

De huidige doelen die nu worden genoemd in de privacyverklaring voor 'improving our products and services', 'undertaking transactional and statistical analysis and related research' zijn te breed en niet specifiek genoeg. RPNow mag alleen de persoonsgegevens van de onderwijsinstelling voor eigen doeleinden gebruiken wanneer RPNow hier toestemming van de onderwijsinstelling voor heeft gekregen. Kortom het is belangrijk om te weten:

- Welke specifieke gegevens verzamelt RPNow voor 'improving our products and services', 'undertaking transactional and statistical analysis and related research'?
- Welke gebruiks- en/of inhoudelijke gegevens kunnen precies worden verwerkt voor ondersteuningsdoeleinden?
- Verzamelt RPNow 'stille' bug- en of crashrapporten, of alleen als een klant actief vraagt om voor hulp?
- Kan RPNow gedetailleerde informatie en voorbeelden van 'geanonimiseerde, geaggregeerde analyses' publiceren?

[38] Annex 1 Details of processing of personal data, Data Processing Agreement PSI, 18 maart 2018, https://www.psionline.com/en-gb/privacy/gdpr-compliance/data-processing-agreement/, geraadpleegd op 8 april 2020.
[39] https://www.psionline.com/en-gb/privacy/privacy-policy/, onder IV. Purposes for Collecting and Processing Personal Information (How We Use Your Personal Information), geraadpleegd op 8 april 2020.

4. Grondslagen

Introductie AVG beginsel

Bij het gebruik en de inzet van proctoring software bij toetsing en examinering worden persoonsgegevens van de student en de proctors (in geval van 'live proctoring' en 'record & review proctoring') verwerkt. Dit betekent dat er een juridische grondslag moet zijn om deze persoonsgegevens rechtmatig te verwerken.

De wet kent zes grondslagen. Het zijn de volgende:

1. Toestemming
2. Overeenkomst
3. Wettelijke verplichting
4. Bescherming van de vitale belangen van een betrokkene
5. Taak van algemeen belang
6. Gerechtvaardigd belang

Analyse van (niet) AVG compliant onderdelen

In het Privacy Policy stelt RPNow verschillende grondslagen te hebben (als verwerkingsverantwoordelijke) om gegevens te verwerken welke afhankelijk zijn van de situatie. Zij noemt zowel toestemming, uitvoering van de overeenkomst als gerechtvaardigd belang. In specifieke situaties zelfs wettelijk verplichting.

> "Performance of a Contract. We collect and process personal information, including Identity Information, Contact Information, Financial Information, and Professional Information, for the purposes of the performance of a contract we are about to enter or have entered into with a client to provide exam-related services, fulfil requests for information about exam and examination opportunities, facilitate registration for exams, and provide examination services to both candidates and clients. Where permitted by law, we may send exam candidates commercial communications and offers for additional examination or training services on behalf of clients.
>
> Consent. We will process your personal information, only to the extent you have consented, when you have given us your specific and informed consent for us to use your personal information. For example, we may use your information, such as your email address, to send you news and newsletters, special offers, and promotions, or to otherwise contact you about products or information we think may interest you.
>
> Legitimate Business Purpose. We process personal information where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests. This includes activities related to everyday business operations, such as invoice processing, business planning, improving the content of our Site, improving our products and services, undertaking transactional and statistical analysis and related research, and handling client service-related queries and complaints. We also may use the information that we learn about you to assist us in advertising our Services on third party websites.
>
> Legal Obligation. We will process your personal information when we need to comply with a legal obligation, meet our on-going regulatory and compliance obligations including in relation to recording and monitoring communications, disclosures to taxe authorities,

financial service regulators and other regulatory and governmental bodies, and to investigate security incidents and in preventing crime.[40]"

Als ook al onder onderdeel vier (4) besproken zijn de huidige doelen die nu worden genoemd in de privacyverklaring voor 'improving our products and services', 'undertaking transactional and statistical analysis and related research' te breed en niet specifiek genoeg. Daarnaast mag RPNow alleen de persoonsgegevens van de onderwijsinstelling voor eigen doeleinden gebruiken wanneer RPNow hier toestemming van de onderwijsinstelling voor heeft gekregen.

Aanbevelingen

In de hoedanigheid van verwerker, zal RPNow de gegevens verwerken in opdracht van de klant. De klant (i.c. de onderwijsinstelling) zal een juridische grondslag moeten hebben om deze gegevens van de betrokkenen (i.c. de studenten) in de applicatie te verzamelen en te verwerken.

In de hoedanigheid van verwerkingsverantwoordelijke kan RPNow een van bovengenoemde grondslagen hebben om de persoonsgegevens. te verwerken. Hierbij kan gedacht worden aan toestemming voor het sturen van nieuwsbrieven, commerciële acties of promoties, aan gerechtvaardigd belang voor het verbeteren van services updates. Per geval zal bezien moeten worden welke situatie van toepassing is voor de onderwijsinstellingen en studenten.

RPNow moet een specifieke en uitputtende lijst van verwerkingsdoeleinden opstellen, zodat haar klanten de juiste wettelijke basis voor elk doel van de gegevensverwerking kunnen bepalen. Dit kan een groot aantal specifieke doeleinden omvatten, zoals "onderhoud van de dienst", "beveiliging van de dienst", "verbetering van de dienst/en of de inkomsten", "het opstellen van statistieken", "het verzenden van facturen", "het reageren op juridische processen/bevelen van de wetshandhaving", enz.

5. Procedure om datalekken te melden en aansprakelijkheid

Introductie AVG beginsel

Er is sprake van een datalek bij een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens. Afhankelijk van de omstandigheden van het geval moet een incident gemeld worden bij de (lokale) Privacy Autoriteit van de verwerkingsverantwoordelijke en bij de betrokkenen zelf.

De autoriteit moet binnen 72 uur geïnformeerd worden bij een datalek. Dit geldt altijd wanneer er persoonsgegevens betrokken zijn bij het incident. Uitzondering is wanneer het niet waarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

Onder de AVG is de verwerkingsverantwoordelijke (i.c. de onderwijsinstelling) aansprakelijk voor schade als gevolg van datalekken. Ook voor schade veroorzaakt door de verwerker. De verwerker is alleen aansprakelijk voor schade die is ontstaan, doordat deze verwerker niet aan de tot haar gerichte verplichtingen uit de AVG heeft voldaan (art. 28 AVG) of wanneer de verwerker buiten de instructies van de verwerkingsverantwoordelijke om heeft gehandeld. Deze instructies dienen in de verwerkersovereenkomst te zijn opgenomen.

[40] https://www.psionline.com/en-gb/privacy/privacy-policy/, onder The Information We Collect From You, geraadpleegd op 8 april 2020.

Analyse van (niet) AVG compliant onderdelen

RPNow heeft als verwerker de plicht om datalekken zo snel mogelijk te melden bij de onderwijsinstelling, die als verwerkingsverantwoordelijke optreedt. Daarnaast moet RPNow maatregelen nemen om de impact van een datalek zo snel mogelijk te verkleinen. Het volgende staat hierover in de verwerkersovereenkomst:

> "Supplier shall notify Customer immediately, and in any case within forty-eight (48) hours, upon becoming aware of a personal data breach. Such notification shall, to the extent known within the notification window: (i) describe the nature of the personal data breach, including, where possible, the categories and approximate number of affected data subjects, and the categories and approximate number of personal data records concerned; (ii) the name and contact details of a contact person at Supplier who can provide additional information; (iii) describe, to the extent known, the likely consequences of such personal data breach; and (iv) describe proposed mitigation efforts, as applicable."

In de verwerkersovereenkomst is niet geconcretiseerd hoe het datalek teruggekoppeld moet worden aan de onderwijsinstelling. Hoe wordt het datalek praktisch gecommuniceerd naar de onderwijsinstelling? Er moeten tussen RPNow en de onderwijsinstelling afspraken gemaakt worden over op welke wijze en met welke contactpersoon binnen de onderwijsinstelling en RPNow gecommuniceerd moet worden.

De AVG schrijft voor dat een inbreuk op de beveiliging van persoonsgegevens door een verwerkingsverantwoordelijke uiterlijk binnen 72 uur na ontdekking aan de privacy autoriteit dient plaats te vinden. Indien de inbreuk bij de verwerker plaatsvindt zal door de verwerker een melding bij de verwerkingsverantwoordelijk worden gedaan zodra hij kennis heeft genomen van het incident. I.c. betekent dit dat RPNow in haar rol van verwerker na ontdekking van een datalek zonder vertraging hiervan de onderwijsonderwijsinstelling op de hoogte dient te brengen. Een melding van een datalek aan de betrokkene(n) vindt plaats als is vast te komen staan dat de inbreuk waarschijnlijk een hoog risico voor de rechten en vrijheden van de betrokkenen inhoudt. Deze melding aan betrokkenen wordt door de verwerkingsverantwoordelijke gedaan. Aan de melding aan de betrokkene is geen termijn verbonden, maar wel inhoudelijk vereisten waaraan de informatie moet voldoen.

In de verwerkersovereenkomst staat geen bepaling opgenomen over aansprakelijkheid ten aanzien van datalekken.

Aanbevelingen

RPNow moet dergelijke inbreuken en door haar subverwerkers zo snel mogelijk aan de onderwijsinstelling melden. Verwerkingsverantwoordelijken voor de verwerking moeten een datalek binnen 72 uur na het bekend worden ervan melden bij de Autoriteit Persoonsgegevens. In geval van een ernstige inbreuk, met grote gevolgen voor de gegevensbescherming van de betrokkenen, is de termijn van 48 uur die RPNow heeft om de onderwijsinstelling te informeren, te lang. Aangezien er consequenties kunnen zijn voor de betrouwbaarheid en integriteit van de examens. En er waarschijnlijk publiciteit kan zijn die klanten en/of eindgebruikers al waarschuwt vóór een officiële kennisgeving door RPNow.

Daarom wordt geadviseerd de termijn van 48 uur te wijzigen in 24 uur in geval van ernstige inbreuken op de beveiliging. Zodat de onderwijsinstelling kan voldoen aan zijn 72-uursverplichting om datalekken aan de Autoriteit Persoonsgegevens en/of de betrokkenen te melden.

Daarnaast wordt geadviseerd om een extra bijlage op te nemen in de verwerkersovereenkomst waarin de informatie over de datalek die gecommuniceerd moet worden aan de onderwijsinstelling

geregeld wordt. In de bijlage worden afspraken gemaakt over welke informatie, binnen welke termijn, op welke wijze en welke contactpersoon binnen de onderwijsinstelling de informatie geleverd moet worden.

Zorg ervoor dat er ten aanzien van aansprakelijkheid en datalekken goede afspraken worden gemaakt in de verwerkersovereenkomst.

6. Bewaartermijnen

Introductie AVG beginsel

Bewaartermijnen worden gebruikt als hulpmiddel om data-minimalisatie te realiseren. De AVG geeft geen concrete bewaartermijn voor persoonsgegevens. De AVG geeft wel aan dat een persoonsgegeven alleen mag worden bewaard als identificeerbaar gegeven, voor zolang als het nodig is voor de doeleinden waarvoor het verzameld is. Dat betekent dus ook dat als de gegevens geanonimiseerd zijn en daarmee dus niet meer de directe of indirecte identificatie van een persoon mogelijk maken, gegevens langer bewaard mogen worden. De AVG schrijft ook voor dat de verwerkingsverantwoordelijk over de bewaartermijn voorafgaand aan de verzameling moet communiceren.

De belangrijkste processen voor onderwijsonderwijsinstellingen zijn gericht op het opleiden van studenten en het verstrekken van bewijsstukken, die weergeven dat studenten de toetsen of examens met succes hebben afgelegd. In het geval van online proctoring zullen in beginsel de persoonsgegevens dan ook niet langer bewaard mogen worden dan voor het eventueel bewijs van rechtmatige toetsing noodzakelijk is. De verwerkingsverantwoordelijke zal de bewaartermijnen moeten bepalen en in een verwerkersovereenkomst voorschrijven op een dusdanige manier dat het ook technisch in te richten is in de applicatie.
Voor nadere onderbouwing van mogelijk vastgestelde bewaartermijnen voor toetsing en examinering voor de onderwijsonderwijsinstellingen, wordt kortheidshalve verwezen naar de Selectielijst actualisatie 2016, voor de administratieve neerslag van de openbaargezag taken en niet-publiekrechtelijke werkprocessen van Nederlandse hogescholen.[41]

Analyse van (niet) AVG compliant onderdelen

RPNow geeft geen overzicht van concrete bewaartermijnen, maar zet in het algemeen uiteen in haar privacyverklaring welke uitgangspunten zij hanteert bij het bepalen van de bewaartermijnen van de verschillende categorieën van gegevens. Zo stelt zij in hoofdstuk 8:

> "We will only retain your personal information for as long as reasonably necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, regulatory, taxe, accounting or reporting requirements. We may retain your personal information for a longer period in the event of a complaint or if we reasonably believe there is a prospect of litigation in respect to our relationship with you.
> To determine the appropriate retention period for personal information, we consider the amount, nature and sensitivity of the personal information, the potential risk of harm from unauthorised use or disclosure of your personal information, the purposes for which we process your personal information, whether we can achieve those purposes through other

[41] Vereniging Hogescholen, Selectielijst actualisatie 2016 voor de administratieve neerslag van de openbaar gezagtaken en niet-publiekrechtelijke werkprocessen van Nederlandse scholen, < https://www.verenigingh ogescholen.nl/system/knowledge_base/attachments/files/000/000/583/original/VERE-3325-Selectielijst_hogescholen_2016_WEB.pdf?1467093338 >, blz. 73 en verder.

means, and the applicable legal, regulatory, taxe, accounting or other retention requirements."

Dat de persoonsgegevens worden bewaard voor zolang '*reasonably necessary*'[42] geeft te denken. De AVG bepaalt ten slotte dat persoonsgegevens niet langer bewaard mogen worden dan *noodzakelijk* voor het doel waarvoor de gegevens verzameld zijn. De toevoeging van '*reasonably*' lijkt een mogelijkheid te bieden om de bewaartermijnen op te rekken.

Aanbevelingen

In beginsel is de onderwijsonderwijsinstelling verantwoordelijk voor het vaststellen van de bewaartermijnen van de persoonsgegevens die worden opgeslagen en bewaard bij gebruikmaking van online proctoring tool van RPNow. Deze termijnen zullen moeten worden opgenomen in de verwerkersovereenkomst, Annex 1 onder de '*subject matter and the duration of the processing of Personal Data*'. De onderwijsonderwijsinstelling kan hierbij de selectielijst actualisatie 2016 als richtlijn gebruiken. RPNow zal als ontwikkelaar van de tool moeten zorgdragen dat deze bewaartermijnen ook technisch uitvoerbaar zijn. Denk hierbij ook aan het correct en automatisch vernietigen van de gegevens na verloop van de bewaartermijn. Daarnaast is het dringend advies om in de verwerkersovereenkomst op te nemen dat de persoonsgegevens na de beëindiging van de overeenkomst verwijderd en/of overgedragen worden (zowel in het systeem als in de back up) en dat de onderwijsinstelling een bevestiging krijgt van RPNow wanneer de persoonsgegevens verwijderd zijn. Het is aan te bevelen om te controleren wat bedoeld wordt met 'reasonably necessary'. Hoe gaat RPNow hiermee om in de praktijk?

7. Subverwerkers en derde partijen

Introductie AVG beginsel

De verwerker verwerkt de persoonsgegevens in opdracht van de verwerkingsverantwoordelijke. De verwerker verwerkt gegevens volgens de instructies van en onder de verantwoordelijkheid van de verwerkingsverantwoordelijke, maar staat wel buiten de organisatie. Verder heeft de verwerker geen zeggenschap over het doel en de middelen van de verwerking. Beslissingen over het gebruik van de gegevens, de verstrekking aan derden, de duur van de opslag etc. worden genomen door de verwerkingsverantwoordelijke.

Een verwerker kan natuurlijk ook weer een derde partij inschakelen om werk voor hem uit te voeren. Deze onderaannemer noemen we dan een subverwerker. In de verwerkersovereenkomst tussen verantwoordelijk en verwerker is vaak bepaald dat een subverwerker alleen mag worden ingeschakeld na schriftelijk akkoord van de verwerkingsverantwoordelijke. Wanneer de verwerker (i.c. RPNow) een subverwerker inzet worden op deze subverwerker dezelfde schriftelijke verplichtingen opgelegd als tussen de verwerkingsverantwoordelijke en de verwerker. De verwerker blijft verantwoordelijk voor de subverwerker voor het nakomen van die verplichtingen door subverwerker.

Naast (sub-)verwerkers kan RPNow verplicht worden aan derde partijen persoonsgegevens te verstrekken. Zo kan RPNow als Amerikaans bedrijf verplicht worden een vordering tot het verstrekken van persoonsgegevens aan de Amerikaanse overheid te voldoen.

[42] PSI online Privacy Policy, hoofdstuk 8 data retention & storage, geraadpleegd op 8 april 2020.

Analyse van (niet) AVG compliant onderdelen

RPNow, als verwerker, maakt gebruik van subverwerkers. In de Data Processing Agreement zegt RPNow hierover het volgende:

> "As at the Effective Date, Customer hereby authorises Supplier to engauge those Subprocessors set out athttps://www.psionline.com/privacy-policy.
> Authorised Subprocessors. Supplier shall update such list by providing notice to Customer at https://www.psionline.com/privacy-policy Customer shall be deemed to have consented to such additional or changed subprocessor if Customer does not object within ten (10) calendar days of the date of such notice
>
> With respect to each Subprocessor, Supplier shall (i) provide Customer with full details of the processing to be undertaken by each Subprocessor; and (ii) include terms in the contract between Supplier and each Subprocessor that are equivalent to those set out in this Agreement."

In de Privacy Shield Policy wordt dit laatste nogmaals bevestigd en als volgt verwoord:

> "We will ensure that any third party to which PSI discloses personal information provides the same level of privacy protection as is required by the Privacy Shield principles and agrees in writing to provide an adequate level of privacy protection.
>
> We may transfer personal information to third-party agents, or service providers, who perform functions on our behalf, such suppliers and licensors that process, store or archive data on our behalf, vendors for customer relationship management, vendors that provide services for us, and vendors that process payments and otherwise facilitate e-commerce. We enter into written agreements with those third-party agents and service providers requiring them to provide the same level of protection the Privacy Shield requires and limiting their use of the personal information to the specified services provided on our behalf."

Een lijst met subverwerkers is vindbaar op de website onder GDPR Compliance Sub-Processors[43] en geeft een overzicht van de verschillende partijen en de werkzaamheden die zij voor RPNow uitvoeren.

In het algemeen zegt RPNow in haar Privacy Policy over het delen van gegevens met derden:

> "We may disclose your personal information to a third party for a business purpose. When we disclose personal information for a business purpose, we enter into a contract that describes the purpose and requires the recipient to both keep that personal information confidential and not use it for any purpose except in performance of the contract."

De verschillende bedrijfsdoeleinden, waarvoor gegevens worden gedeeld, worden breed omschreven evenals de ontvangers waaraan gegevens worden verstrekt. Ontvangers, of wel derden, zijn onder meer commerciële partijen, (lokale) overheidsinstanties of partijen betrokken bij mogelijke bedrijfsovernames.

In de Privacy Shield Policy stelt RPNow vast dat zij aansprakelijk is voor het handelen van subverwerkers en derden:

> "PSI is potentially liable in cases of onward transfers of personal information to third parties, such as when third parties that act as agents on our behalf process personal information in a manner inconsistent with the Privacy Shield Principles."

[43] https://www.psionline.com/en-gb/privacy/gdpr-compliance/sub-processors/, geraadpleegd op 8 april 2020.

Naast verstrekking van gegevens aan (sub-)verwerkers en derde partijen kan RPNow ook verplicht worden, als Amerikaans bedrijf, om aan een vordering tot het verstrekken van persoonsgegevens aan de Amerikaanse overheid te voldoen. Zonder dat dit met zoveel woorden genoemd wordt, wordt hier waarschijnlijk ook naar de US Cloud Act verwezen.[44]

Aanbevelingen

De beschikbare informatie geeft een duidelijk overzicht van welke (sub-)verwerkers ingezet worden door RPNow voor de uitvoering van de dienstverlening. Voor het inzetten van nieuwe subverwerkers wordt de onderwijsonderwijsinstelling vooraf geïnformeerd en krijgt 10 kalenderdagen de mogelijkheid om bezwaar te maken. 10 dagen is een veel te korte tijdsperiode. Het advies is dat met RPNow wordt afgesproken dat RPNow de onderwijsinstelling ruim van tevoren op de hoogte stelt indien RPNow een nieuwe subverwerker wil inschakelen. Deze periode is nodig om de onderwijsinstelling voldoende tijd te geven om de overeenkomst te beëindigen indien de onderwijsinstelling ernstige bezwaren heeft tegen een dergelijke subverwerker. Daarnaast mist de locaties van de verschillende subverwerkers. Er is vooralsnog alleen schriftelijke bevestiging[45] dat RPNow noch haar subverwerkers persoonsgegevens in een land buiten de EEA zullen verwerken, tenzij er sprake is van een land met een adequaatheidsbesluit of handelend onder het EU-U.S.Privacy Shield framework.

Mede gelet op de mogelijkheid dat RPNow verplicht kan worden persoonsgegevens te verstrekken aan de Amerikaanse overheid in het kader van strafrechtelijk onderzoek of nationale veiligheid onder de US Cloud Act zal de onderwijsonderwijsinstelling extra alert moeten zijn op de verstrekking en opslag van persoonsgegevens door RPnow in en buiten de Verenigde Staten.

8. Rechten van betrokkenen

Introductie AVG beginsel

Betrokkenen hebben het recht op inzage, correctie, wijziging, beperking van de verwerking, of verwijdering van hun persoonsgegevens. En daarnaast hebben betrokkenen het recht van bezwaar en het recht om niet onderworpen te worden aan een uitsluitend op geautomatiseerde verwerking gebaseerd besluit. In het onderstaande worden de rechten in het kort toegelicht.

Recht van inzage: een betrokkene mag een organisatie vragen of het persoonsgegevens heeft vastgelegd en zo ja, welke. Hiervoor hoeft betrokkene geen specifieke reden te noemen. Het recht op inzage betreft alleen inzage in iemands eigen gegevens.

Recht van correctie: een betrokkene mag verzoeken om gegevens te corrigeren, te wijzigen of om gegevens aan te vullen.

Recht van verwijdering: een betrokkene mag een organisatie verzoeken om persoonsgegevens te verwijderen.

Recht van bezwaar: een betrokkene mag bezwaar maken tegen verwerking van zijn gegevens. In geval van bezwaar tegen direct marketingactiviteiten dient de verwerkingsverantwoordelijke hieraan altijd gehoor te geven.

---

[44] Privacy Policy, Disclosure of your Personal Information-Law Enforcement/Public Authority, geraadpleegd op 8 april 2020.

[45] GDPR Compliance - Data Processing Agreement – International transfers of customer personal data, https://www.psionline.com/en-gb/privacy/gdpr-compliance/data-processing-agreement/, geraadpleegd op 8 april 2020.

Recht van beperking van de verwerking: een betrokkene heeft het recht om opgeslagen persoonsgegevens door een organisatie te laten bevriezen en markeren met als doel de verdere verwerking (tijdelijk) stop te zetten.

Recht van dataportabiliteit: een betrokkene heeft het recht om gegevens van zichzelf over te laten dragen naar een ander. Bijvoorbeeld leengegevens over laten dragen van de ene bibliotheek naar de andere.

Profilering: verwerking waarbij aan de hand van persoonsgegevens persoonlijke aspecten van een betrokkene worden geëvalueerd om zo bijvoorbeeld beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen;

Analyse van (niet) AVG compliant onderdelen

In de Privacy Policy onder '*your legal rights*' op de website geeft RPNow een opsomming van de rechten van betrokken onder de AVG. Daarbij geeft ze het e-mail adres waarnaar de betrokkenen rechtstreeks zijn/haar verzoek kan sturen.
Daarnaast geeft RPNow aan haar medewerking te verlenen aan de klant (i.c. de onderwijsinstelling) om aan een verzoek van de betrokkenen te voldoen. In de verwerkersovereenkomst zegt RPNow hierover:

> "Data subject rights - Supplier shall notify Customer within ten (10) calendar days if it receives a data subject access request, including requests by a data subject to exercise rights in chapter III GDPR, and shall provide full details of that request.
>
> Supplier shall fully co-operate as requested by Customer to enable Customer to comply with any exercise of rights by a data subject under Chapter III GDPR regarding Personal Data."

Aanbevelingen

Alhoewel alle rechten van betrokkenen in de privacyverklaring worden weergegeven, zijn deze wel erg summier. Slechts een onderdeel mist, namelijk het recht om een klacht in te dienen bij de autoriteit. In het kader van dit advies is voornamelijk van belang dat RPNow haar volledige medewerking verleent in geval een betrokkenen een verzoek indient bij een onderwijsinstelling. Deze medewerking is voldoende beschreven in de verwerkersovereenkomst.

9. Bijstand verlenen voor nakoming AVG compliance

Introductie AVG beginsel

Als verwerker is RPNow verplicht[46] om de onderwijsonderwijsinstelling, in haar rol als verwerkingsverantwoordelijke van de verwerkingen, te helpen om aan haar wettelijke verplichtingen te voldoen. Denk hierbij aan meewerken aan de uitvoering van audits, data protection impact assessments, onderzoeken van toezichthouders en verzoeken van betrokkenen.

[46] Artikel 28 lid 3 sub e en f AVG

Analyse van (niet) AVG compliant onderdelen

In de verwerkersovereenkomst vermeldt RPNow het volgende daarover:

> "Audit rights: Supplier shall make available to Customer on request all information necessary to demonstrate compliance with Data Protection Laws and this Agreement and allow for and contribute to audits, including inspections by Customer or another auditor mandated by Customer of any premises where the processing of Personal Data takes place. Supplier shall permit Customer or another auditor mandated by Customer to inspect, audit and copy any relevant records, processes and systems in order that Customer may satisfy itself that Supplier is in compliance with the Data Protection Laws and this Agreement."

In de verwerkersovereenkomst van RPNow staat niets opgenomen over de kosten voor het meehelpen aan rechten van betrokken, DPIA's, informeren over datalekken aan de onderwijsinstelling en maatregelen treffen om de impact van de datalek zo klein mogelijk te maken en het doen van audits.

Aanbevelingen

Het is gebruikelijk dat afspraken over het dragen van de kosten om de onderwijsinstelling mee te helpen om aan haar wettelijke verplichtingen te voldoen, worden vastgelegd in een verwerkersovereenkomst. De onderwijsinstelling zal dan ook hieraan de nodige aandacht moeten besteden om dit op te nemen in de verwerkersovereenkomst.

10. Geautomatiseerde besluitvorming en profilering

Introductie AVG beginsel

Geautomatiseerde besluitvorming is een geautomatiseerde verwerking van persoonsgegevens ter beoordeling van persoonlijke aspecten van een natuurlijke persoon, zonder menselijke tussenkomst op basis waarvan vervolgens een besluit genomen wordt.

Profilering is een verwerking waarbij aan de hand van persoonsgegevens persoonlijke aspecten van een betrokkene worden geëvalueerd om zo bijvoorbeeld beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.
Bij online proctoring moet rekening worden gehouden met geautomatiseerde besluitvorming en profilering[47]. Het inzetten van online proctoring om fraude te kunnen detecteren kan negatieve gevolgen hebben voor de student. Wanneer er met online proctoring een geautomatiseerd besluit wordt genomen zonder menselijke tussenkomst, waardoor de student een sanctie of maatregel krijgt opgelegd, zoals een schorsing, heeft dit negatieve gevolgen voor de student. Volledig geautomatiseerde besluitvorming met online proctoring is dan ook niet toegestaan onder de AVG. Het is een vereiste dat er bij zulke besluiten altijd een beoordeling door een docent of examinator plaatsvindt.

Analyse van de (niet) AVG compliant onderdelen

Uit de beschikbare informatie valt niet op te maken of en in welke vorm er geautomatiseerde besluitvorming dan wel profilering door RPNow plaatsvindt. Gelet op – het doel van- de dienstverlening en de wijze waarop studenten gemonitord worden met behulp van de software, is

[47] Artikel 22 AVG

het aannemelijk dat er enige vorm van profilering plaatsvindt en mogelijk ook geautomatiseerde besluitvorming.

Aanbevelingen

Aanbevolen wordt te verifiëren of en voor hoe ver er aan geautomatiseerde besluitvorming dan wel profilering wordt gedaan. In het geval de onderwijsinstelling de RPNow software wenst in te zetten zal zij hierover afspraken moeten vastleggen in de overeenkomst met RPNow en transparant hierover communiceren naar studenten.

Bijlage

Tabel ter vergelijking van de drie verschillende online proctoring aanbieders: Proctorio, ProctorExam en RPNow

Op basis van de uitkomsten van de juridische analyses is onderstaande tabel gecreëerd. Deze geeft een globaal overzicht hoe de drie online proctoring aanbieders op het gebied van Algemene Verordening Gegevensbescherming (AVG) compliance scoren. De tabel is uitsluitend bedoeld als een overzicht en niet als uitkomst van de gehele juridische analyses. De kleuren zijn bedoeld om de uitkomsten te visualiseren. Deze zijn echter subjectief. De daadwerkelijke (kleur)score is ook mede afhankelijk van de (overige) afspraken die tussen de onderwijsinstelling en de aanbieder worden gemaakt.

De onderwijsinstelling wordt geadviseerd om voor een volledig beeld de uitgebreide analyses te raadplegen met betrekking tot de tien punten die zijn onderzocht.

		Proctorio*	ProctorExam	RPNow
1.	**Definitie en gebruik persoons-gegevens**	Gebruik van (de term) PII en daarmee beperkte(re) omvang van bescherming van persoonsgegevens. Geen hantering van de definitie van persoonsgegevens AVG.	Gebruik van definitie AVG.	Gebruik van definitie van geldende privacywetgeving. Niet duidelijk gedefinieerd dat definitie van AVG van toepassing is.
2.	**Doorgifte 3de landen**	Persoonsgegevens worden opgeslagen in de VS. Afspraken en beveiligingsmaatregelen (met subverwerkers) niet duidelijk.	Persoonsgegevens worden (mogelijk) opgeslagen in de VS. Afspraken en beveiligingsmaatre-gelen (met subverwerk-ers) moeten worden geconcretiseerd.	Persoonsgegevens worden opgeslagen in de VS. Afspraken en beveiligingsmaatrege-len (met subverwer-kers) moeten worden geconcretiseerd.
3.	**Rollen & doeleinden**	Kwalificeert zich als verwerker.	Kwalificeert zich als verwerker.	Kwalificeert zich als verwerker.
		Specifieke lijst met doeleinden voor eigen verwerkingen mist. Afspraken vastleggen over uitsluiten van of beperkte mogelijkheid voor verdere verwerking voor eigen doeleinden.	Specifieke lijst met doeleinden voor eigen verwerkingen mist. Afspraken vastleggen over uitsluiten van beperkte mogelijkheid voor verdere verwerking voor eigen doeleinden.	Algemene lijst met doeleinden voor eigen verwerkingen. Afspraken vastleggen over uitsluiten van of beperkte mogelijkheid voor verdere verwerking voor eigen doeleinden.
4.	**Grondslagen**	Geen specifieke lijst met grondslagen voor eigen doeleinden.	Geen specifieke lijst met grondslagen voor eigen doeleinden.	Geen specifieke lijst met grondslagen voor eigen doeleinden.

5.	**Datalekken melden**	Beperkte en niet volledige procedure meldplicht datalekken.	Concretere afspraken nodig m.b.t. 1) melden datalekken aan onderwijsinstelling, 2) aansprakelijkheid en datalekken en 3) het advies voor een meldtermijn voor de verwerker van 24 uur.	Concretere afspraken nodig m.b.t. 1) datalekken aan onderwijsinstelling, 2) aansprakelijkheid en datalekken en 3) het advies voor een meldtermijn voor de verwerker van 24 uur.
6.	**Bewaartermijnen**	Geen specifieke informatie beschikbaar over bewaartermijnen. Bewaartermijnen moeten worden opgenomen in de verwerkersovereenkomst	Bewaartermijnen moeten worden opgenomen in de verwerkersovereen-komst.	Bewaartermijnen moeten worden opgenomen in de verwerkersovereen-komst.
7.	**Subverwerkers en derde partijen**	Geen informatie beschikbaar over (afspraken met) subverwerkers en derde partijen. Verstrekking van gegevens onder Cloud Act is aandachtspunt.	Voorafgaande notificatie met mogelijkheid tot bezwaar. Opslaglocatie verdient aandacht.	Voorafgaande notificatie met mogelijkheid tot bezwaar. Opslaglocatie verdient aandacht. Verstrekking van gegevens onder Cloud Act is aandachtspunt.
8.	**Rechten van betrokkenen**	Geen volledige informatie beschikbaar over het uitoefenen van rechten van betrokkenen op de website.	Geen informatie beschikbaar over het uitoefenen rechten van betrokkenen op de website.	Voldoet aan AVG.
9.	**Bijstand AVG compliance**	Geen informatie beschikbaar (bij afwezigheid van verwerkersovereenkomst).	Voldoet aan AVG. Advies om procesafspraken en afspraken m.b.t. kosten vast te leggen.	Voldoet aan AVG. Advies om procesafspraken en afspraken m.b.t. kosten vast te leggen
10.	**Geautomatiseerde besluitvorming en profilering**	Geen informatie verstrekking over geautomatiseerde besluitvorming en / of profilering.	Geen informatie verstrekking over geautomatiseerde besluitvorming en/of profilering.	Geen informatie verstrekking over geautomatiseerde besluitvorming en/of profilering.

* Door het ontbreken van een verwerkersovereenkomst is er weinig informatie over de wijze waarop Proctorio haar verantwoordelijkheden als verwerker uitvoert.

Deze analyse is geschreven in opdracht van SURF

www.privacycompany.eu
info@privacycompany.nl
070 – 820 96 90

Maanweg 174
Den Haag
KvK 63080052