

Onderwijs en data – een risico of een kans

Onderwijs speelt een cruciale rol in de ontwikkeling van onze samenleving. Onderwijsorganisaties en hun medewerkers geven door middel van kennisoverdracht aan leerlingen en studenten mede vorm aan onze cultuur, ethiek en benadering van de wereld. Een enorme verantwoordelijkheid, die alleen slaagt als onderwijsorganisaties zelf het goede voorbeeld geven.

Het is daarom van fundamenteel belang dat onderwijsorganisaties op alle gebieden een goed voorbeeld geven en de best mogelijke diensten leveren. Onderwijsorganisaties die dit structureel op een goede wijze doen, trekken de beste studenten en medewerkers aan. Gegevensbescherming is een gebied dat rechtstreeks kan bijdragen aan het versterken van een merk en daarmee het vertrouwen in onderwijsorganisaties vergroot.

Met de introductie van de Algemene Verordening Gegevensbescherming (AVG), bijna twee jaar geleden, kwam er een grote golf van uitdagingen op alle organisaties af binnen de Europese Economische Ruimte (EER), die te maken hebben met het verwerken van persoonsgegevens. Maar dit geldt ook voor veel organisaties die daarbuiten gevestigd zijn.

De AVG is bijvoorbeeld van toepassing op onderwijsorganisaties die gevestigd zijn in de EER, die studenten of personeel in de EER hebben, die studenten hebben ingeschreven voor uitwisselingsprogramma's naar EER-landen, die bepaalde beurzen of leningen aan en van in de EER gevestigde instellingen en individuen ontvangen of aanbieden, en/of die banden hebben met oud-studenten of leveranciers die zich in de EER bevinden.

De AVG heeft onder meer gezorgd voor:

- versterking en uitbreiding van privacyrechten;
- meer verantwoordelijkheden voor organisaties;
- stevige bevoegdheden voor alle Europese privacytoezichthouders, zoals de
- bevoegdheid om boetes tot 4% van de omzet of 20 miljoen euro op te leggen. waaronder het opleggen van een maximale boete van 20 miljoen euro of 4 van de wereldwijde omzet van het voorgaande boekjaar.

Onderwijsorganisaties stonden rond de introductie van de AVG dan ook onder grote druk, als gevolg van de enorme hoeveelheden door hen verwerkte persoonsgegevens. Dat begint al bij het inschrijven van een leerling of student. In hun dossier worden de gegevens van leerlingen, studenten en medewerkers verwerkt. Ook werken scholen en universiteiten met digitale systemen als

Make sure.

www.privacyperfect.com | info@privacyperfect.com | +31 10 310 07 40

toetsingsprogramma's en leerlingvolgsystemen en wordt steeds meer gebruik gemaakt van sociale media en apps. Om nog maar te zwijgen van onderzoeksgegevens. Onderwijsorganisaties zijn er voor verantwoordelijk al deze gegevens zorgvuldig en veilig te behandelen. Zeker als het gaat om kinderen, omdat deze extra kwetsbaar zijn. Kinderen verdienen volgens de AVG dan ook specifieke bescherming.

Toch is er nog steeds veel onduidelijkheid met betrekking tot de AVG in het onderwijs. Veel onderwijsorganisaties weten dat de AVG bestaat en dat ze iets aan privacy moeten doen. Sommige onderwijsorganisaties weten dat ze misschien een persoon moeten aanwijzen die verantwoordelijk is voor de gegevensbescherming - een functionaris gegevensbescherming. Vaak krijgt een docent, bestuurder of administratief medewerker deze rol. [Maar wat moeten de kwalificaties en taken van deze persoon zijn?](#) Welke rechten hebben personen van wie de gegevens worden verwerkt? Waar moeten onderwijsorganisaties verder rekening mee houden om aan de AVG te voldoen? En wat kan er gebeuren als een onderwijsorganisatie dat niet doet?

Wat betekent de AVG voor onderwijsorganisaties?

De AVG-regels dwingen onderwijsorganisaties om goed na te denken over hoe persoonsgegevens worden verwerkt en beschermd. De AVG legt de verantwoordelijkheid bij de onderwijsorganisatie om aan te tonen dat ze aan de privacyregels voldoen. Een onderwijsorganisatie moet bijvoorbeeld kunnen aantonen dat een verwerking aan de privacybeginselen voldoet, zoals **rechtmatigheid, transparantie, doelbinding, juistheid, dataminimalisatie** en **opslagbeperking**.

Mensen hebben verschillende rechten om controle te houden over hun persoonsgegevens. Gehoor geven aan mensen die een beroep doen op hun privacyrechten is een belangrijk onderdeel van een gezond privacybeleid. En een gezond privacybeleid draagt bij aan het vertrouwen van mensen in een organisatie. Onder de AVG bestaan de volgende rechten:

- Allereerst hebben mensen recht op duidelijke informatie over wat een onderwijsorganisatie met hun persoonsgegevens doet. Dit is een belangrijk onderdeel van het **transparantiebeginsel**, en waarom een onderwijsorganisatie privacyinformatie moet geven aan personen van wie deze organisatie persoonsgegevens wil verwerken, bijvoorbeeld in een privacyverklaring. Deze informatie moet in het bijzonder begrijpelijk zijn voor kinderen als een onderwijsorganisatie hun gegevens verwerkt.

Make sure.

www.privacyperfect.com | info@privacyperfect.com | +31 10 310 07 40

- Het recht op inzage. Dit is het recht van mensen om onder meer een kopie te ontvangen van de persoonsgegevens die een onderwijsorganisatie van hen verwerkt.
- Het recht op vergetelheid.
- Het recht op rectificatie en aanvulling. Het recht om de persoonsgegevens die een onderwijsorganisatie verwerkt te laten wijzigen als deze onjuist of onvolledig zijn, en deel van het **beginsel van juistheid**.
- Het recht op dataportabiliteit. Het recht om persoonsgegevens over te laten dragen aan een andere partij.
- Het recht op beperking van de verwerking. Het recht om onder omstandigheden de verwerking van persoonsgegevens tijdelijk te laten stoppen.
- Het recht met betrekking tot geautomatiseerde besluitvorming en profilering. Oftewel: het recht op een menselijke blik bij deze besluiten.
- Het recht om bezwaar te maken tegen de gegevensverwerking.

Elke verwerking van persoonsgegevens is een kleinere of grotere inbreuk op de privacy van de mensen over wie het gaat. Daarom mogen persoonsgegevens alleen worden verwerkt als onderwijsorganisaties zonder deze gegevens een specifiek **doel** niet kunnen bereiken. Deze beperking aan de hoeveelheid verwerkte gegevens heet ook wel **dataminimalisatie**. Persoonsgegevens die voor het ene doel zijn verzameld, kunnen niet zomaar voor een ander doel worden gebruikt. Dit noemt men **doelbinding**. Ook moeten de gegevens op een gegeven en redelijk moment verwijderd worden. Dat noemt de AVG **opslagbeperking**.

Laten we eens kijken naar een eenvoudig voorbeeld dat de meeste onderwijsorganisaties zullen herkennen om onder andere het **beginsel van rechtmatigheid** te verkennen.

Jaarlijkse klassenfoto's door een externe fotograaf zijn de norm op de meeste basisscholen en middelbare scholen. Universiteiten en Hogescholen organiseren ook vaak het maken van groepsfoto's van afgestudeerden. Klassenfoto's vormen persoonsgegevens. Als een onderwijsorganisatie in de EER gevestigd is, is de AVG van toepassing. De foto's worden bijvoorbeeld verzameld met het doel een hechter groepsgevoel te creëren. Als het niet vooraf duidelijk was, mogen deze foto's niet later ter promotie gebruikt worden.

Scholen en universiteiten moeten een goede reden hebben om persoonsgegevens te verwerken, een zogenaamde 'grondslag'. De meest relevante grondslagen voor onderwijsorganisaties zijn:

Make sure.

www.privacyperfect.com | info@privacyperfect.com | +31 10 310 07 40

- **Toestemming** van de persoon om wie het gaat voor de verwerking voor een specifiek doel.
- Het is noodzakelijk om gegevens te verwerken om een **overeenkomst** uit te voeren.
- Het is noodzakelijk om gegevens te verwerken omdat u dit **wettelijk verplicht** bent.
- Het is noodzakelijk om gegevens te verwerken om uw **gerechtvaardigde belang** te behartigen (en dit belang weegt zwaarder dan de rechten en vrijheden van de persoon om wie het gaat)

Deze grondslagen gelden voor alle persoonsgegevens. Persoonsgegevens die door hun aard bijzonder gevoelig zijn, noemen we bijzondere persoonsgegevens. Deze krijgen extra bescherming. Onder deze persoonsgegevens vallen onder andere die waaruit etnische afkomst, religie of seksuele geaardheid blijken, en gegevens over iemands gezondheid. De verwerking van bijzondere persoonsgegevens is verboden, tenzij een onderwijs organisatie zich kan beroepen op een wettelijke uitzondering én een van de grondslagen voor het verwerken van 'gewone' persoonsgegevens. Voor onderwijsorganisaties is vooral de uitzondering **uitdrukkelijk toestemming** van belang.

Onder de AVG hebben onderwijsorganisaties over het algemeen toestemming nodig voor het maken en publiceren van foto's of video's van leerlingen. In uitzonderingsgevallen, als ze voor identificatiedoeleinden worden gebruikt, gelden foto's als bijzondere persoonsgegevens. Alle leerlingen op de foto moeten dan hun uitdrukkelijke en schriftelijke toestemming geven om de foto te maken, publiceren of verspreiden. Als de personen op de foto minderjarig zijn, is toestemming van de ouders of verzorgers nodig. Onderwijsorganisaties moeten kunnen aantonen dat een persoon op de foto daadwerkelijk toestemming heeft gegeven.

Waar ligt de verantwoordelijkheid voor het verwerken van persoonsgegevens?

Organisaties schakelen vaak externe organisaties in om persoonsgegevens voor hen te verwerken, een schoolfotograaf is hier opnieuw een goed voorbeeld. Het is dan belangrijk dat alle betrokken partijen weten wie verantwoordelijk is voor de juiste behandeling van de gegevens.

In de situatie dat de onderwijsorganisatie de fotograaf gedetailleerde instructies geeft zijn werk op een bepaalde manier in te vullen, zal deze instelling waarschijnlijk verwerkingsverantwoordelijke blijven voor het maken van de foto's. Doorslaggevend is

Make sure.

www.privacyperfect.com | info@privacyperfect.com | +31 10 310 07 40

wie de doeleinden waarvoor de gegevens worden verwerkt en de wijze van verwerking bepaalt. Onderwijsorganisaties zullen dus ook de verantwoordelijkheid dragen dat het maken van de klassenfoto's volgens de AVG verloopt. De fotograaf is dan slechts verwerker onder deze verantwoordelijkheid. De verwerkingsverantwoordelijke en verwerkers moeten samen een verwerkersovereenkomst afsluiten. Doen zij dat niet, dan zijn beide partijen in overtreding.

Belangrijke maatregelen van de Autoriteit Persoonsgegevens om aan de AVG te voldoen

De Autoriteit Persoonsgegevens heeft een lijst gepubliceerd om te toetsen of een organisatie (nog steeds) aan een aantal belangrijke AVG-verplichtingen voldoet. Hiermee kunnen onderwijsorganisaties weten of, en zo ja waar, zij in actie moeten komen. Onderstaand een aantal punten:

- Het hebben van een uitgebreide, organisatiebrede en duidelijke strategie voor gegevensbescherming.
- Ervoor zorgen dat een functionaris voor gegevensbescherming is aangesteld.
- Een overzicht hebben van alle verwerkingen, aangezien het type gegevens dat een organisatie verwerkt gevolgen heeft voor hoe deze moeten worden beschermd en welke AVG-regels daarop van toepassing zijn.
- Ervoor zorgen dat een onderwijsorganisatie op de hoogte is van en kan aantonen aan individuen waarom, hoe en op welke manier persoonsgegevens door de onderwijsorganisatie worden verwerkt en voor welk specifiek doel.
- Opnieuw controleren of onderwijsorganisaties nog een basis hebben voor het verwerken van persoonsgegevens voor alle verwerkingen. Is een verwerking niet langer "noodzakelijk voor het uitvoeren van een overeenkomst"? Dan mag een onderwijsorganisatie zich daar niet meer op baseren.
- Alle persoonsgegevens op een veilige manier bewaren en binnen de door de onderwijsorganisatie gestelde bewaartermijn.
- Opleiding van personeel en vergroten van privacybewustzijn, toewijzing van verantwoordelijkheden voor naleving. Ervoor zorgen dat alle nieuwe medewerkers ook privacybewust zijn.
- Toedelen van verantwoordelijkheden in geval van een intern of extern beveiligingsincident of datalek. Het hebben van een vastgelegde procedure en een artikel 33-register, waar alle (al dan niet gemelde) incidenten moeten worden opgeslagen.
- Het regelmatig uitvoeren en bijwerken van DPIA's, het van tevoren

Make sure.

www.privacyperfect.com | info@privacyperfect.com | +31 10 310 07 40

identificeren van potentiële risico's van nieuwe projecten en toepassingen, en terugkijken of de voorgestelde mitigerende maatregelen zijn geïmplementeerd.

- Ervoor zorgen dat alle noodzakelijke verwerkersovereenkomsten zijn ondertekend voor het geval een onderwijsorganisatie samenwerkt met derden die namens de organisatie persoonsgegevens verwerken.
- Controleren of een onderwijsorganisatie toegangsverzoeken van betrokkenen heeft ontvangen en of de verzoeken zijn afgehandeld volgens de AVG. Zijn de processen op orde?
- Voldoet een onderwijsorganisatie aan het verplichte vereiste van Privacy by Design en Default (vastgelegd in artikel 25 van de AVG)? Privacy by Design houdt in dat een organisatie er al bij het ontwerpen van producten en diensten voor zorgt dat persoonsgegevens goed worden beschermd. Privacy by Default betekent dat de standaardinstellingen van programma's, apps, websites en diensten maximale privacy bieden.

Gegevensbescherming is een risico maar biedt ook mogelijkheden

Het merendeel van de onderwijsorganisaties heeft rond de introductie van de AVG een aantal van de bovenstaande maatregelen genomen om de risico's te verminderen en in overeenstemming te brengen met de regelgeving. Naleving van de AVG is echter meer dan alleen risicobeheer.

In een wereld waar de reputatie van een onderwijsorganisatie kan worden aangetast met een enkele post op sociale media, willen bestuurders, studenten en personeel zekerheid dat hun onderwijsorganisatie er alles aan doet om de door haar verwerkte gegevens goed te beheren en over robuuste compliance structuren beschikt. Maar in plaats van gegevensbescherming slechts als kostenpost te beschouwen, zouden onderwijsorganisaties er ook goed aan doen gegevensbescherming te zien als kans om concurrentievoordeel te behalen.

Opbouwen van een sterk merk duurt jaren, beschadiging is met een klik gedaan

Uit [onderzoek](#) blijkt dat studenten de reputatie van een universiteit beschouwen als een van de belangrijkste factoren waarmee rekening wordt gehouden bij het kiezen van hun studie.

Make sure.

www.privacyperfect.com | info@privacyperfect.com | +31 10 310 07 40

Ondertussen zijn er in de EU de afgelopen 2 jaar [meer dan 160.000 datalekken gemeld](#). Organisaties werden geconfronteerd met een aanzienlijke reputatieschade en hoge boetes voor niet-naleving van de AVG. Van de (tot voor kort) 28 EU-lidstaten meldde Nederland in deze periode de meeste datalekken, gevolgd door Duitsland en het VK. [Studies tonen aan](#) dat de grootste impact van een datalek verloren omzet door verminderd vertrouwen is.

Bij onderwijsorganisaties worden regelmatig incidenten en datalekken veroorzaakt, ofwel door menselijke fouten, die een intern datalek veroorzaakten, ofwel door een toenemend aantal cyberaanvallen, met een extern datalek als gevolg.

Uit [het laatste jaarverslag van de Engels privacy autoriteit ICO](#) blijkt dat van de 13.840 datalekmeldingen die zij in 2018-2019 heeft ontvangen, meer dan 13% afkomstig was uit de onderwijssector. De enige twee sectoren die hoger scoorden, waren commerciële bedrijven (18%) en de gezondheidszorg (16%).

Datalekken en beveiligingsincidenten

De belangrijkste oorzaak van datalekken zijn menselijke fouten. Waar mensen werken, zullen zij fouten maken. Zo was vorig jaar [67% van de in Nederland gemelde datalekken](#) het gevolg van het versturen of afgeven van persoonsgegevens aan de verkeerde ontvanger.

In juni 2017 stuurde de University of East Anglia, een toonaangevende universiteit uit de top 15 van Britse ranglijsten, een e-mail naar bijna 300 studenten die een lezing promootten, maar deelde ten onrechte persoonsgegevens van ongeveer 2.000 studenten in een spreadsheet die aan de e-mail was bijgevoegd. Uiteindelijk besloot de Britse gegevensbeschermingsautoriteit (ICO) de universiteit niet te beboeten, maar aan de studenten van wie de persoonsgegevens naar honderden van hun klasgenoten werden gemaaild, is [meer dan £ 140.000 aan compensatie uitgekeerd](#). Om niet te spreken van de schade aan het imago van de universiteit.

Dit was slechts een van de vele datalekken die de afgelopen vijf jaar door onderwijsorganisaties over de hele wereld zijn gemeld, en het onderwijs behoort wereldwijd [consequent tot de top vijf van sectoren voor het aantal gemelde informatiebeveiligingsincidenten](#).

Het Cambridge Analytica-schandaal, waarbij Facebook betrokken was, heeft veel mensen wakker geschud en bewust gemaakt van het belang van een goede bescherming van persoonsgegevens. Zowel grotere organisaties als universiteiten, als verschillende scholen zijn in het verleden getroffen door datalekken. Bij velen zal de

Make sure.

www.privacyperfect.com | info@privacyperfect.com | +31 10 310 07 40

[ransomware-aanval](#) waarvan de Universiteit Maastricht eind vorig jaar het slachtoffer werd nog vers in het geheugen liggen. Ook de Universiteit Utrecht werd in 2019 getroffen door een datalek, waarbij persoonsgegevens van onder andere [promovendi inzichtelijk waren voor \(oud-\)medewerkers](#).

Belangrijk is dat ook kleinere incidenten worden opgepakt door de media: [een basisschool stuurde per ongeluk een lijst met kinderen die recht hadden op gratis kerstlunches aan elke ouder](#), en had vier maanden later opnieuw een datalek vanwege een menselijke fout. Deze incidenten hebben voor veel publieke turbulentie gezorgd, maar de gevolgen voor de organisaties zelf zijn nog niet bekend.

Een van de beste manieren om het aantal interne datalekken te verminderen, is het bewustzijn te vergroten door middel van opleiding van het personeel. Het geven van cursussen, certificeringen en trainingen over het belang van gegevensbescherming, veelvoorkomende valkuilen en verzachtende maatregelen kan een enorm verschil maken. [Trainingen en cursussen worden vaak tegen een kleine vergoeding door derden aangeboden](#). Bovendien kan samenwerking tussen verschillende afdelingen op het gebied van compliance helpen de instelling als geheel op één lijn te brengen. Bijvoorbeeld door het samenwerken van de HR-, Marketing-, Admin- en IT- afdelingen in één platform.

In Nederland is een werkgever in het algemeen verantwoordelijk voor schade veroorzaakt door een werknemer. De werkgever kan de schade in de regel slechts verhalen als er sprake is van opzet of bewuste roekeloosheid van de kant van de werknemer. Dit maakt het belangrijker dan ooit om ervoor te zorgen dat er een centraal overzicht is in hoe de organisatie persoonsgegevens verwerkt. De AVG eist dan ook dat elke verwerkingsactiviteit wordt geregistreerd. Daardoor kunnen datalekken en risico's worden geïdentificeerd en gemitigeerd.

Cyberaanvallen zijn ook voor onderwijsorganisaties steeds meer een probleem geworden. Het is niet voor niets dat de Autoriteit Persoonsgegevens in haar publicatie 'Jaarcijfers meldplicht datalekken 2019' de aandacht vestigt op de grote stijging van het aantal meldingen van hacking, phishing en malware-incidenten.

In de bovenstaande gevallen is het evident dat het datalek moet worden gemeld aan de toezichthouder, maar dat is niet altijd het geval.

Een typische uitdaging - wanneer melden we een datalek?

Een grote uitdaging voor onderwijsorganisaties is om te weten wanneer een datalek moet worden gemeld bij de toezichthouder. Volgens NAHT, de grootste vakbond voor

Make sure.

www.privacyperfect.com | info@privacyperfect.com | +31 10 310 07 40

senior leiders in het onderwijs in het VK, behandelde de ICO alleen al 1.385 mogelijke datalekken bij scholen in het eerste jaar van de AVG, in slechts 15% van de gemelde gevallen is tot actie overgegaan. Van de 665 zelf gemelde incidenten van scholen was in ongeveer 80% geen actie nodig. Het uitblijven van actie op incidenten betekent niet automatisch dat deze onnodig waren.

Als er een datalek optreedt, moet de verwerkingsverantwoordelijke binnen 72 uur na bekendheid een melding doen van het datalek, tenzij het onwaarschijnlijk is dat het lek een risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

Gezien het zeer krappe tijdsbestek van 72 uur en de complexiteit van de AVG, kan het een uitdaging zijn om vast te stellen of er al dan niet melding moet worden gemaakt. Het hebben van een compliance software tool, waarbij onderwijsorganisaties automatisch de risico's kunnen identificeren, de betrokken partijen inzichtelijk maken, de omvang van het incident kunnen bepalen, een verslag hiervan kunnen maken en rechtstreeks aan de privacy autoriteiten kunnen rapporteren, kan een enorme opluchting zijn en rendement op de investering van de onderwijsorganisatie opleveren.

Naast het managen van datalekken die al plaats hebben gevonden is het ook belangrijk om mitigerende maatregelen te nemen om de kans op een incident te verkleinen. Passende maatregelen kunnen vastgesteld worden door een [Data Protection Impact Assessment](#) (DPIA) uit te voeren. Dat is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen.

Het recht op inzage en inzageverzoeken

Een andere factor die tegenwoordig als een uitdaging wordt beschouwd voor organisaties, is het reageren op de toegenomen hoeveelheid inzageverzoeken.

Tegenwoordig zijn individuen zich veel meer bewust van hun recht om bij organisaties hun persoonsgegevens op te vragen, waardoor het aantal inzageverzoeken in 2019 sterk is toegenomen.

[Volgens de Autoriteit Persoonsgegevens](#) werden er in 2019 in Nederland meer dan 27.000 klachten over privacy geregistreerd, een stijging van 79% ten opzichte van 2018. De meeste klachten (29%) hadden betrekking op de mogelijke schending van de rechten van betrokkenen, zoals het recht op toegang en het recht op verwijdering van persoonsgegevens. Ondertussen lieten onderzoeken in het VK zien dat van de 90 door hen onderzochte organisaties er 64 een significante toename zagen van het aantal inzageverzoeken. Van de [schoolzaken die in het VK door de ICO in het eerste jaar van](#)

Make sure.

www.privacyperfect.com | info@privacyperfect.com | +31 10 310 07 40

[de AVG werden behandeld](#), had 38% betrekking op openbaarmaking van gegevens en 29% op verzoeken tot inzage van betrokkenen.

Ondertussen stelt de AVG dat de eerste reactie moet plaatsvinden binnen 30 dagen na ontvangst van het verzoek. Omdat deze verzoeken een tijdgevoelig proces inhouden, vergt dat vaak veel inspanning en middelen. Zelfs als de juiste procedures bestaan, kan het dus aanzienlijke extra kosten voor organisaties met zich meebrengen. In het eerder genoemde Engelse onderzoek zag van de 64 onderzochte organisaties gemiddeld 67% een stijging van de kosten in verband met reageren op inzageverzoeken.

Met de juiste voorbereidingen, passende veiligheidsmaatregelen, een procedure voor inzageverzoeken, of zelfs met de hulp van een derde partij, kan het afhandelen versimpeld en versoepeld worden. Hierdoor kunnen tijd, middelen en extra kosten worden bespaard. Het helpt onderwijsorganisaties [AVG-compliant te blijven, een goede reputatie te behouden en betrokkenen tevreden te houden](#).

Hoe cloudgebaseerde software kan helpen

De handhaving van de AVG brengt tal van vereisten met zich mee voor onderwijsorganisaties. Gelukkig is er na de inwerkingtreding van de AVG een schat aan ondersteunende bedrijven ontstaan om organisaties te helpen hun compliance-uitdagingen het hoofd te bieden. Voor elke uitdaging zijn er partijen beschikbaar om de druk op de middelen te verlichten. Van datamapping en het bijhouden van gegevens, tot het zorgen voor voortdurende naleving, zelfs als de richtlijnen en regelgeving veranderen. Zo kan cloudgebaseerde software onderwijsorganisaties helpen om eenvoudig:

- Inzicht te krijgen in hoe persoonsgegevens worden verwerkt en waar ze worden bewaard.
- De kwetsbare applicaties binnen de instelling te detecteren.
- Datalekken op een duidelijke, beknopte, conforme manier te registreren.
- Privacybewustzijn binnen uw instelling te vergroten.
- Processen te automatiseren.
- Kosten te reduceren.
- Compliance-inspanningen efficiënter te maken.

Dergelijke software kan onderwijsorganisaties ook helpen vast te stellen of een Data Protection Impact Assessment (DPIA) vereist is, voordat een specifiek project wordt gestart, en zo ja, een gecentraliseerd systeem bieden van waaruit de informatie met

Make sure.

www.privacyperfect.com | info@privacyperfect.com | +31 10 310 07 40

betrekking tot de DPIA kan worden verkregen en opgeslagen.

Of een onderwijsorganisatie nu besluit om een gecentraliseerde cloudgebaseerde compliance-softwaretool te gebruiken of niet, de organisatie moet ervoor zorgen dat alle noodzakelijke maatregelen zijn genomen om aan de AVG te voldoen. Het waarborgen hiervan zorgt ervoor dat alle door de organisatie uitgevoerde verwerkingen eerlijk en rechtmatig zijn, dat de voorwaarden voor gegevensbewaring duidelijk worden gecommuniceerd, dat de gegevens nauwkeurig zijn, dat ze op een veilige manier worden opgeslagen en dat alle persoonsgegevens op een transparante en verantwoorde manier worden verwerkt.

Houd de regie in handen

Al met al biedt de AVG-naleving een geweldige kans doordat het verantwoordelijkheid en transparantie mogelijk maakt naar zowel leerlingen, studenten en personeel. Het vertrouwen in en imago van basisscholen, middelbare scholen en universiteiten wordt hierdoor vergroot. Onderwijsorganisaties die aan de AVG voldoen, zullen concurrentievoordelen behalen ten opzichte van andere instellingen en betere leerlingen, studenten en medewerkers aantrekken.

De sleutel tot succes bij het bereiken van naleving van de AVG is het proces als een investering te zien. In plaats van meer taken toe te bedelen aan personeel dat al overbelast is, kan de onderwijsorganisatie het beschikbare aanbod aan AVG software onderzoeken en er een selecteren die helpt de AVG-nalevingsdoelstellingen snel en eenvoudig te bereiken. Zodat het personeel kan doen waar ze goed in zijn: zich richten op het leveren van het beste onderwijs en het aantrekken van nieuwe leerlingen en studenten.

PrivacyPerfect heeft tot doel om bij te dragen aan een wereld waarin mensen bedrijven en organisaties vertrouwen door middel van compliance. We streven ernaar om dit te bereiken door het aanbieden van een cloudgebaseerde, gebruiksvriendelijke software tool voor AVG-compliance, waardoor de privacy van leerlingen, studenten en medewerkers moeiteloos wordt gewaarborgd.

Ervaar zelf de voordelen van onze SaaS-oplossing via [een 14-daagse gratis proefperiode](#) voor onderwijsorganisaties en verken de mogelijkheden, of [meld u aan voor onze wekelijkse nieuwsbrief](#) om ervoor te zorgen dat u op de hoogte blijft van nieuws over gegevensbescherming en inhoud met betrekking tot

Make sure.

www.privacyperfect.com | info@privacyperfect.com | +31 10 310 07 40

onderwijsorganisaties.

Als u vragen heeft, aarzel dan niet om contact met ons op te nemen via

info@privacyperfect.com

Make sure.

www.privacyperfect.com | info@privacyperfect.com | +31 10 310 07 40