Beleid Gegevensbescherming

Inleiding

In mei 2018 treedt de Europese Algemene Verordening Gegevensbescherming (AVG of GDPR in het Engels) in werking. De AVG verplicht organisaties om persoonlijke gegevens te beschermen, verplicht het om contactpersonen toe te staan hun gegevens te bekijken en te bewerken of te verwijderen. Dit beleid maakt transparant welke gegevens worden verzameld door EduDivers en welke maatregelen worden genomen om de gegevens te beschermen en hoe we deze beheren en hoe we risico's beheren.

Juridisch is EduDivers een stichting gevestigd in Nederland. De stichting onderhoudt een website die deels fungeert als een platform voor deelnemers aan het MijnID programma. EduDivers is wettelijk verantwoordelijk is voor de gegevens op het platform.

EduDivers wil de kwaliteit van het onderwijs over diversiteit verbeteren en de samenwerking op dit gebied bevorderen. We werken daarin veel samen met kwetsbare minderheden. Diversiteit is een aantal landen is taboe, of zelfs verboden en in sommige gevallen zelfs wettelijk geëtiketteerd als 'terrorisme'. Dit geldt bijvoorbeeld voor Moslims en homoseksuelen en transgenders. Het eventueel zichtbaar worden of uitlekken van persoonsgegevens kan ernstige consequenties hebben en het zorgen voor een goede gegevensbescherming is daarom een essentieel onderdeel van ons werk.

EduDivers werkt samen met haar internationale zusterstichting GALE (Global Alliance for LGBT Education) waar zulke risico’s een nog grotere rol spelen dan in Nederland. Daarom werken we al sinds 2007 aan structurele gegevensbescherming. Binnen EduDivers verzamelen we geen gegevens over seksuele geaardheid en genderidentiteit. Toch kan in een aantal landen het lid zijn van een organisatie die gelijkheid op het gebied van seksuele geaardheid en genderidentiteit bevordert al verdacht of strafbaar zijn. Daar hebben onze leden en partners misschien nu geen last van, maar het is moeilijk te voorzien hoe hun situatie over enkele jaren zal zijn. Daarom staan we kwetsbare leden altijd toe om zich bij EduDivers te registreren met een alibi of/en een niet-traceerbaar e-mailadres.

Functionaris voor gegevensbescherming en register

EduDivers heeft weinig personeel. De directeur, Peter Dankmeijer, functioneert als

Publicatiedatum: 2 April 2018; werkversie

functionaris voor gegevensbescherming. Hij is te bereiken op p.dankmeijer@edudivers.nl; +31 20 737 2959.
Alle gegevens die op verzoek van personen zijn gewijzigd of gedeeld, worden genoteerd in het EduDivers gegevensregister. Het register zal op verzoek beschikbaar zijn voor de juiste autoriteiten.
EduDivers is gevestigd in Nederland en de Autoriteit Persoonsgegevens is de toezichthoudende autoriteit.

Privacy principes

Het EduDivers gegevensbeschermingsbeleid volgt de regels van de Europese Algemene Verordening Gegevensbescherming (AVG/GDPR). Specifieker:

1. Al onze medewerkers, vrijwilligers, leden en partners zullen bewust worden gemaakt van de risico's van het verspreiden van persoonlijke gegevens en het beheren van dergelijke risico's.
2. We verzamelen geen persoonlijke informatie die niet noodzakelijk is voor ons functioneren.
3. We vragen personen toestemming om hun gegevens voor specifieke doeleinden te gebruiken.
4. Personen hebben het recht om hun gegevens te laten bewerken of verwijderen.
5. Wanneer nieuwe producten met persoonsgegevens worden ontwikkeld, zal gegevensbescherming deel uitmaken van het ontwerpproces.

Risicoinventarisatie

EduDivers onderhoudt de volgende databases en gegevens. In de matrix geven we ook de locatie van de database aan, of specifieke databases kunnen worden bewerkt door de contactpersonen en onze risicobeoordeling.

Risico beoordelingsmatrix

databases	doel	bewaard op	toegang	risico
ONLINE				
MijnID contacten	informatie en uitwisseling	www.edudivers.nl	moderators	medium
E-zine	informatievoorziening	www.edudivers.nl	moderators	laag
Moodle users	deelname e-cursussen	sexualdiversityacademy.org	moderators	laag
CLOUD				

Centraal adresboek	contact management	tresor	dir/secr	laag
Project databases	contact management	tresor	werknemers	laag
Project logboeken	process management	tresor	werknemers	laag
Onderzoek databases	verzamelen onderzoeksdata	google sheets	werknemers	laag
OFFLINE				
Outlook	contact management	hard drive	dir/secr	laag
Mobiele telefoons	contact management	synced	staff	laag

We hebben de risico's verdeeld over drie niveaus: hoog, medium en laag. Hoog risico verwijst naar ernstige risico's voor personen als kwetsbare gegevens zouden worden gelekt. Medium risico verwijst naar de gevolgen van andere databases die kunnen worden gelekt. Laag risico verwijst naar onlinegegevens die veilig worden verwerkt en naar Cloud- en offlinegegevens die veilig worden opgeslagen.

Profielen van MijnID partners

EduDivers profileert zich vanaf juli 2018 niet meer als LHBTI-kenniscentrum, maar als diversiteitsorganisatie. We vragen MijnID partners niet naar seksuele voorkeur of genderidentiteit. Daarom schatten we het risico van het hebben van een profiel voor MijnID partners niet hoog in. Het kan wel zijn dat als MijnID partners naar het buitenland verhuizen, of zich in een gemeenschap bevinden waar risico op eerwraak is als vermoed wordt dat een persoon (seksuele) diversiteit verdedigt, dit een risico oplevert. Hoewel dit risico relatief onwaarschijnlijk is, definiëren we het uit extra zorgvuldigheid als “medium”.

Niet-openbare databases

De centrale database voor contactbeheer van EduDivers, tijdelijke adressenlijsten voor projecten en tijdelijke projectlogboeken met namen bevinden zich in een gecodeerde Tresor Drive van de directeur. EduDivers heeft voor Tresor gekozen om de gegevens veilig te bewaren. Tresor codeert de bewaarde bestanden op zo’n manier dat buitenstaanders, overheden en zelf Tresor medewerkers zelf op geen enkele manier toegang hebben tot de bestanden. De provider en servers bevinden zich in Zwitserland, wat het risico verkleint dat andere overheden, zoals de VS, deze gegevens delen met andere overheden. EduDivers beschouwt providers in de USA als per definitie onveilig omdat de overheid van bedrijven eist dat zijn hun gegevens beschikbaar stellen; dit is in ieder geval zo bij de veelgebruikte Cloud services Google, Microsoft OneDrive en Dropbox.

Alleen de directeur en zijn secretaris hebben toegang tot de PC’s en laptops met de Tresor Drive. Dit wordt als laag risico beschouwd. Deze databases bevatten overigens geen informatie die ernstig schadelijk kan zijn als ze worden gelekt.

EduDivers doet regelmatig kleinschalig onderzoek. Hiervoor worden Google Formulieren en

Google Spreadsheets gebruikt. De onderzoeksgegevens zijn meestal anoniem. In specifieke gevallen kunnen namen worden gevraagd. Dit gebeurt als we kleinschalig kwalitatief onderzoek doen waarin persoonlijke suggesties of aanbevelingen worden gegeven. Deze gegevens worden als laag risico beschouwd als ze geen risico's voor respondenten opleveren. Onderzoek dat wel mogelijke risico's kan opleveren, documenteren we offline.

Databases voor persoonlijk contact

De persoonlijke (en deels professionele) contacten van de directeur en het personeel worden opgeslagen in het Outlook-profiel van de directeur en de persoonlijke adresboeken van het personeel. Het Outlook-adresboek van de directeur wordt gesynchroniseerd tussen pc, laptop en telefoon. Deze worden als laag risico beschouwd omdat alleen verlies van diefstal een risico vormt.

Maatregelen

EduDivers maakt onderscheid tussen algemene maatregelen en specifieke maatregelen. De algemene maatregelen zijn geldig voor alle omstandigheden. De specifieke maatregelen zijn relevant voor specifieke databases of evenementen en hebben betrekking op het beheer van specifieke risico's die aan deze databases zijn gekoppeld.

Algemene maatregelen

Websites

1. De website www.edudivers.info is beveiligd met een https-certificaat en de web service YPOS heeft de ACG-conformiteit geïntegreerd in het websitesysteem. Het websitesysteem wordt automatisch regelmatig geüpgraded door YPOS om de hoogste normen te handhaven. Wachtwoorden die voor de site worden gebruikt, zijn gecodeerd en de overdracht van gegevens online is SSL-gecodeerd. Deze bescherming wordt formeel overeengekomen in een bewerkersovereenkomst tussen EduDivers en YPOS.
2. E-cursussen van EduDivers worden aangeboden via de Moodle-website www.sexualdiversityacadmy.org, die eigendom is van de EduDivers GALE. Het beheer van de gegevens in deze Moodle website is daarom formeel de verantwoordelijkheid van GALE. Het GALE Privacy Beleid is the vinden op https://www.gale.info/doc/accountabilty/GALE-Data-Protection-Policy-2018.pdf.
3. Wanneer we om persoonlijke gegevens vragen, geven we het doel aan en vragen we toestemming om de gegevens te onderhouden en te informeren hoe de persoon de

gegevens kan bewerken of verwijderen.

4. In het geval van een (waargenomen of reëel) gegevenslek, informeert het personeel, de vrijwilliger, het lid of de gegevensverwerker onmiddellijk de verantwoordelijke voor de verwerking die de juiste maatregelen zal treffen of treffen.
5. De online profielen op de EduDivers website worden door gebruikers ingediend en kunnen door hen worden bewerkt en verwijderd. Eens in de vijf jaar worden profielen die niet worden gebruikt (Moodle) of die onjuiste gegevens bevatten (niet-toegankelijke e-mailadressen) verwijderd.
6. Tijdelijke maillijsten (voor projecten of specifieke taken) worden verwijderd na het voltooien van de taken.
7. Permanente maillijsten worden voor onbepaalde tijd bewaard, maar de leden worden geïnformeerd over hoe zij hun gegevens kunnen bewerken of hun gegevens kunnen laten verwijderen.

Onderzoek

Normaal gesproken is EduDivers onderzoek anoniem en kunnen de gegevens niet worden herleid tot individuen. In sommige gevallen is een dergelijke koppeling noodzakelijk, bijvoorbeeld bij het uitvoeren van een kwalitatieve behoefteanalyse bij een kleine maar deskundige doelgroep. In die gevallen worden de respondenten op de hoogte gebracht van het doel en van het gebruik van hun gegevens. Na online verzamelen wordt de onlinedatabase verwijderd en worden de gegevens offline opgeslagen op een veilige locatie. Onderzoeksgegevens die mogelijk risico's opleveren voor respondenten worden niet online verzameld. Onderzoeksgegevens die op langere termijn worden bewaard, worden (indien nodig) ontdaan van hun (link met) persoonlijke gegevens.

Bescherming voor pc, laptop en telefoon

PC's, laptops en telefoons van personeel worden beschermd met wachtwoorden en/of vingerafdruktoegang en beschermd tegen virussen en ransomware met Bitdefender.

Datalekprocedure

Wanneer een datalek optreedt of zich kan voordoen, wordt een Datalek Memo gemaakt met daarin:

1. Datum, tijd en plaats van (mogelijk) datalek
2. Datum en tijdstip van ontdekking
3. Gegevens en tijdstip van blokkeren van toegang tot de gegevens
4. Waarschijnlijke oorzaak
5. Maatregelen die zijn genomen om het item te herstellen, te wissen of de gegevens te

verplaatsen

6. Correctiemaatregelen om de huidige bescherming te herstellen en indien nodig het ontwerp van de bescherming te verbeteren
7. Beoordeling van de noodzaak om te rapporteren aan de Autoriteit Persoonsgegevens en beslissing
8. Het memo wordt gedocumenteerd in het Data Register.

Verlies of diefstal van datadragers

Wanneer laptops, telefoons, USB's of andere datadragers met gegevens worden verloren of gestolen, worden de verloren items geblokkeerd voor gebruik zodra het verlies is ontdekt. De datalekprocedure wordt gevolgd.

Dataportabiliteit

Gegevens worden bewaard of kunnen worden gedownload in MS Excel-indeling. Op verzoek kunnen personen kopieën van bestanden krijgen met hun gegevens in dit formaat. MS Excel-bestanden met persoonlijke gegevens worden niet gedeeld met derden, tenzij expliciet vermeld bij de registratie en met een zinvol doel. Wijziging van gegevens in opdracht van de persoon of overdracht van gegevens wordt gedocumenteerd in het Data Register.

Klachten

Personen kunnen een klacht indienen over het niet naleven van dit gegevensbeschermingsbeleid of over het beleid zelf. De normale procedure hiervoor is om te schrijven aan de directeur, die de klacht zo snel mogelijk, maar in ieder geval binnen vier weken, zal behandelen. Personen kunnen ook een klacht indienen bij de Autoriteit Persoonsgegevens. Klachten over privacy worden gedocumenteerd in het Data Register.

Richtlijnen voor personeel

Alle medewerkers en vrijwilligers worden op de hoogte worden gesteld van dit beleid en de richtlijnen voor gegevensbescherming wanneer ze beginnen te werken voor EduDivers, of wanneer ze lid worden van EduDivers mailinglijsten of van het MijnID platform.
Het is uitdrukkelijk verboden voor personeelsleden om persoonlijke gegevens van EduDivers te delen via lekkende clouddiensten zoals Dropbox, Google Drive en OneDrive.
Het personeel zal erop worden gewezen dat eventuele datalekken onmiddellijk aan de directeur moeten worden gemeld en dat een Datalek Memo moet worden ingediend om het risico goed te kunnen beoordelen en om transparant te zijn over genomen beslissingen en maatregelen.

Periodieke herziening van het beleid

Het gegevensbeschermingsbeleid zal om de vijf jaar worden herzien, of vaker als incidenten wijzen op de noodzaak om het beleid bij te werken.

Informatie voor het publiek

Het gegevensbeschermingsbeleid is beschikbaar op http://www.edudivers.nl/over_ons/edudivers-verantwoording. Bij de inschrijving van nieuwe leden van het MijnID platform of van maillijsten wordt verwezen naar de samenvattende EduDivers Privacyverklaring.