

Data Protection Impact Assessment (DPIA) voor Workflower-pakket 'Jobstudenten gezocht'

Indien u gebruik maakt van de Workflower-oplossing 'Jobstudenten gezocht', is het risico op privacyschending uiterst gering. Niettemin wil Amaron u aan de hand van deze Data Protection Impact Assessment (DPIA) inzicht geven in de risico's, hoe klein ze ook zijn.

1. Organisatiegegevens

Naam, adres van organisatie: Amaron, Kapellestraat 13, 8755 Ruiselede

Opsteller DPIA: Tom De Caluwé

Overige betrokkenen en geraadpleegde experts: DPO H.-Hartziekenhuis Lier: Dhr. Tom van Vooren; jurist: Dhr. Philippe Van Liefferinge

Stappenplan uitvoering:

| | | |
|---------------------|---|--|
| Vrijdag 18/01/2019 | GDPR-team Amaron (Tom De Caluwé, Cedric Steenbeke, David Pardo) | Workshop bij Amaron DPIA vakantiejoboplossing |
| Woensdag 30/01/2019 | Dhr. Tom van Vooren, Heilig Hart Lier | DPIA voorgelegd aan ziekenhuis DPO |
| Dinsdag 05/02/2019 | Dhr. Philippe Van Liefferinge | DPIA juridisch laten valideren |

2. Welke gegevens vormen het voorwerp van deze DPIA?

Deze DPIA is van toepassing op de **persoonsgegevens** die over de jobstudent als natuurlijke persoon verzameld worden. Dat zijn alle gegevens die de student ingeeft in het sollicitatieformulier waarmee hij of zij zich kandidaat stelt voor een vakantiejob.

De persoonsgegevens worden in opdracht van uw instelling verzameld, tijdelijk op het Amaron Workflower-platform bewaard en onmiddellijk aangeboden aan de HR-dienst van uw instelling met als doel deze te verwerken in het kader van de aanvraag voor een vakantiejob.

In deze context is Amaron de processor en uw instelling de controller van de persoonsgegevens geregistreerd door studenten die zich kandidaat stellen voor een vakantiejob.

Deze DPIA heeft betrekking op een nieuwe werkwijze in uw zorginstelling, waarbij de opvolging van bepaalde taken binnen het proces om een vakantiejob aan te vragen, geautomatiseerd wordt, maar waarbij de besluitvorming niet geautomatiseerd is.

3. Moet een DPIA worden uitgevoerd?

Een DPIA is alleen verplicht als een gegevensverwerking waarschijnlijk een hoog privacy-risico inhoudt voor de betrokkenen en wanneer er op grote schaal bijzondere persoonsgegevens verwerkt worden. In het geval van de Workflower-oplossing 'Jobstudent gezocht' is het risico op privacy-schending beperkt en worden er slechts op beperkte schaal gegevens verwerkt.

De toezichthouders volgens de DPIA-template van Sieuwert van Otterloo gebruiken als vuistregel dat er geen uitgebreide DPIA nodig is, als minder dan twee van onderstaande negen evaluatiecriteria positief scoren.

In het kader van het proces 'Jobstudenten gezocht' is er slechts één criterium dat een ja-score krijgt:

| Nummer | Criterium | Beoordeling |
|--------|--|--|
| 1 | Evaluatie van personen of scoretoekenning | JA, in context van selectie van vakantiejob |
| 2 | Geautomatiseerde besluitvorming met rechtsgevolg of vergelijkbaar wezenlijk gevolg | Neen, besluitvorming is niet geautomatiseerd |
| 3 | Stelselmatige monitoring | Neen, geen monitoring |
| 4 | Gevoelige gegevens of gegevens van zeer persoonlijke aard | Neen, geen gevoelige gegevens |
| 5 | Op grote schaal verwerkte gegevens | Neen, geen grote schaal |
| 6 | Matching of samenvoeging van datasets | Neen, geen matching of samenvoegen |
| 7 | Gegevens met betrekking tot kwetsbare betrokkenen | Neen, geen gegevens m.b.t. kwetsbare betrokkenen |
| 8 | Innovatieve toepassing van nieuwe technologische of organisatorische oplossing | Neen, geen nieuwe technologische of organisatorische oplossing. De oplossing draait al 4 jaar in zorginstellingen. |
| 9 | Blokkering van een recht, dienst of contract | Neen, geen blokkering van recht, dienst of contract, want is aanzet tot opmaak van contract |

Op basis van deze analyse kunnen we stellen dat een uitgebreide DPIA niet nodig is. Toch heeft Amaron ervoor gekozen om de DPIA uit te werken, zodat de klant inzicht krijgt in de mogelijke risico's, hoe klein ze ook zijn.

4. Hoe worden de gegevens verwerkt?

De persoonsgegevens worden verzameld in het Amaron Workflower-platform dat in de Azure Cloud tenant van Amaron staat; ze worden tijdelijk bewaard in een database die hoort bij het Amaron Workflower-platform en onmiddellijk aangeboden ter verwerking aan de HR-dienst van uw instelling. Deze verwerking houdt in: de gegevens vanuit de Amaron-webapplicatie exporteren naar een Excel-bestand lokaal op de pc van de HR-verantwoordelijke of -medewerker.

De verwachte omvang van de gegevensverwerking is kleinschalig. Het aantal betrokkenen in het proces 'Jobstudent gezocht' is beperkt tot de leden van de HR-afdeling die de aanvragen afhandelen en de diensten aan wie de informatie over de jobstudenten bezorgd wordt.

Om GDPR-compliant te zijn, nemen Amaron en uw instelling in de context van 'Jobstudent gezocht' de volgende voorzorgen:

Amaron:

- Het invulformulier voor de jobstudent staat op het Workflower-platform in de cloud en is enkel beschikbaar via HTTPS.
- De e-mails die uitgestuurd worden naar de jobstudenten volgen de normale regels van e-mailverkeer en omvatten geen informatie die privacygevoelig is.
- Het exporteren van de persoonsdata gebeurt onder HTTPS.
- De kans dat iemand inbreekt op Workflower op Azure en zo de logs in plain text kan bekijken, is quasi nihil door het volgen van de Azure GDPR-compliant blueprints.
- Amaron heeft een eigen GDPR-compliant managementsysteem dat voldoet aan de Icuvo-regels, in de scope van processor. Zie website: <https://amaron.be/data-protection-policy-amaron-bvba/?lang=en>
- Amaron is processor omdat Amaron in opdracht van de klant de gegevens slechts tijdelijk verzamelt en bewaart (zonder er zelf baat bij te hebben), en deze onmiddellijk aan de instelling ter verwerking aanbiedt. Amaron houdt geen archief bij van de persoonsgegevens en verwijdert deze 1 jaar na registratie, gezien het proces van een vakantiejobaanvraag maximaal 1 jaar kan lopen.
- Amaron houdt wel gedurende meerdere jaren de auditlog bij, die alle informatie over het proces bevat en daarvoor ook de basisdata van het proces. Deze zal enkel gebruikt worden als er bij een klacht over de geleverde service bewijslast nodig zou zijn.
- Amaron verzamelt informatie over de jobstudent als deze er vrijwillig voor kiest om zich kandidaat te stellen voor een vakantiejob. Amaron vraagt hem/haar via het aanvraagformulier te bevestigen dat de instelling zijn/haar gegevens mag bewaren in deze context.
- Amaron wijst de jobstudent via het formulier ook op zijn/haar rechten, in overeenstemming met de toepasselijke wetgeving, zijnde:

- de toestemming voor de verwerking van persoonsgegevens in te trekken, voor zover de verwerking van de persoonsgegevens aanvankelijk op de toestemming van de jobstudent gebaseerd was;
- de toegang tot correctie, wissing of beperking van zijn/haar persoonsgegevens te vragen;
- zich tegen elke verwerking voor direct marketing te verzetten;
- de overdraagbaarheid te vragen van de persoonsgegevens, die hij/zij heeft verstrekt en die de instelling als klant van Amaron heeft verwerkt in het kader van de evaluatie van zijn/haar kandidatuur voor de vakantiejob;
- een klacht in te dienen bij de toezichthoudende autoriteit in de Europese Lidstaat waarin de jobstudent gewoonlijk verblijft, werkt of waar de vermeende inbreuk op de toepasselijke gegevensbeschermingswetgeving is gebeurd.

Uw instelling:

- Via een link op de website van uw instelling geeft u de studenten die zich kandidaat wensen te stellen voor een vakantiejob, toegang tot het webformulier dat zich op het Workflower-platform bevindt.
- De webpagina van uw instelling die de link naar dit webformulier bevat, moet ook een e-mailadres vermelden (bv. hr@instelling.be) dat de student kan gebruiken indien hij/zij vragen heeft met betrekking tot het uitoefenen van zijn rechten.
- In geval er vragen zijn die een actie van Amaron veronderstellen, brengt de HR-verantwoordelijke Amaron op de hoogte van de gevraagde actie, bv. de vraag om de gegevens van een persoon vóór het verstrijken van de termijn van 1 jaar te verwijderen. Amaron voert dan deze actie uit.
- Er mag er geen sprake zijn van doorgifte van de persoonsgegevens door de instelling – nationaal noch internationaal. Deze voorwaarde moet door de instelling worden gerespecteerd.
- De archivering van de gegevens betreffende de vakantiejobaanvragen gebeurt in uw instelling.
- De HR-dienst van uw instelling doet ten minste elke 3 maanden een export van de aanwezige gegevens.

5. Beoordeling van de privacy-risico's

Inschatting risico's:

We schatten de kans en impact van de volgende risico's in als volgt:

| Risico | Hoe kan dit risico zich voordoen? | Kans dat dit binnen de termijn van een jaar gebeurt | Impact op betrokkenen |
|--|---|---|---|
| Onrechtmatige toegang – door medewerkers van Amaron of medewerkers van de zorginstelling | Amaron-medewerkers volgen de Amaron GDPR compliancy regels niet of de HR-medewerkers van de instelling geven hun login van Workflower door aan niet-gerechtigd personeel. | Laag, want elke Amaron-medewerker beseft de consequentie als hij/zij deze regel overtreedt. Hetzelfde geldt ook voor de HR-medewerkers van de instelling. Auditlogs zijn enkel consulteerbaar door personen die hiertoe gerechtigd zijn en er wordt gelogd wie deze raadpleegt. Per gebruiker is er een login omwille van traceability redenen. Er gebeurt logging van de toegangen. | Laag, want met het uitlekken van deze persoonsgegevens kan de medewerker van Amaron of van de zorginstelling weinig risicovol doen. |

| | | | |
|---|---|---|--|
| | | Er is een interne Amaron-procedure voor toegangsbeveiliging. | |
| Onrechtmatige toegang door derden | Hacken van de Workflower-applicatie of de Workflower-database op Azure. | Laag, want Azure borgt applicatie- en data-inbreuk. + Via een extern bedrijf garandeert Amaron een penetration testing op hacking en zorgt het ervoor dat de gevonden issues worden aangepakt. | Lage impact omdat deze persoonsgegevens geen heel gevoelige of heel persoonlijke gegevens bevatten. |
| Ongewenste wijziging van gegevens door de medewerkers van Amaron, door medewerkers van de zorginstelling of door derden | Iemand wijzigt de gegevens die de jobstudent heeft ingebracht via het webformulier. | Laag, want het Workflower-formulier is zo opgebouwd dat de gegevens ingevuld door de jobstudent niet gewijzigd kunnen worden. Er is toegangslogging, en alle wijzigingen die er toch zouden gebeuren, worden in de logfiles bijgehouden. | Laag, het heeft geen zin om de gegevens te wijzigen, want dan loopt het achteraf in het proces fout. |
| Verdwijnen/zoekraken van gegevens | Dit kan gebeuren in een rampscenario of wanneer een medewerker een record zou kunnen verwijderen. | Azure heeft een disaster recovery scenario tegen verlies van data. Workflower voorkomt dat medewerkers een record uit de database kunnen verwijderen. | Lage impact op de persoon. Het risico bestaat er dan in dat de student de kans misloopt om een vakantiejob te krijgen. |

Amaron garandeert dat de beschreven maatregelen ter inperking van de risico's op regelmatige basis geëvalueerd worden door de betrokken projectmanager.

6. Conclusie

Amaron stelt alles in het werk om de persoonsgebonden gegevens van de studenten die zich kandidaat stellen voor een vakantiejob te beschermen tegen onrechtmatige toegang. Maar zelfs als de gegevens zouden uitlekken, is de impact op de persoon zo goed als nihil, omdat er geen gevoelige data in de applicatie wordt ingegeven.

7. Contactgegevens

Hebt u vragen over deze Data Protection Impact Assessment (DPIA), neem dan contact op met Tom De Caluwé: tom@amaron.be of tel 0492 91 85 82