Privacy Impact Assessment

Classificatie	Vertrouwelijk
Gegenereerd door	https://www.classity.nl

Privacy Impact Assessment

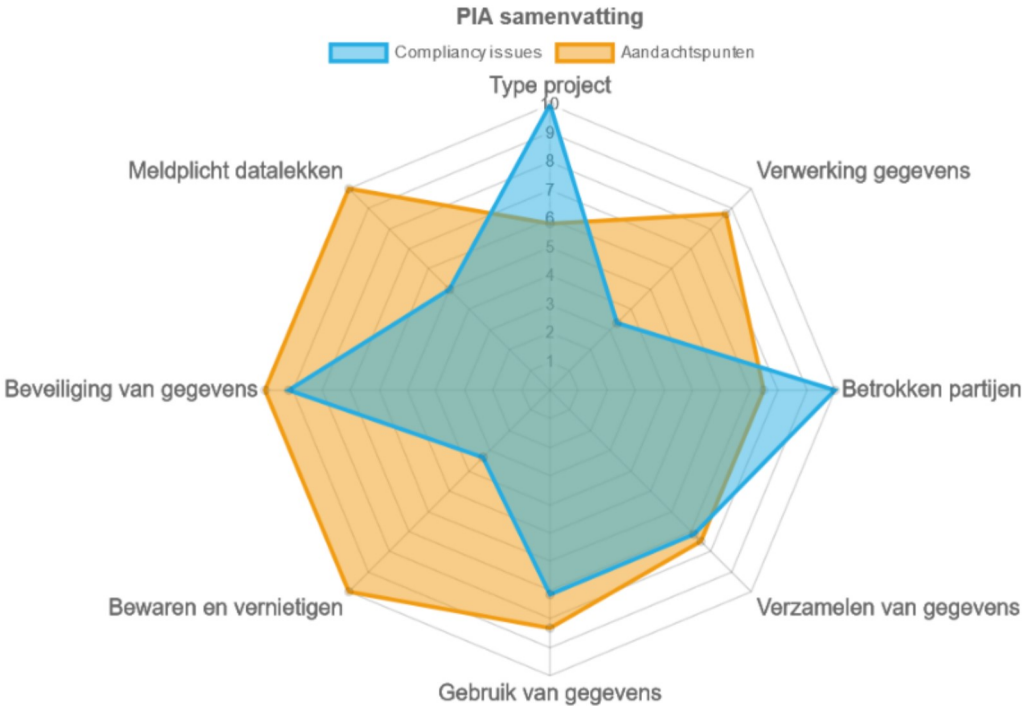
De PIA is gericht op het in kaart brengen van privacyrisico's. Daarnaast helpt het opvolgen van de aanbevelingen uit deze PIA om de kwaliteit van uw gegevens te optimaliseren, uw dienstverlening te verbeteren en het vertrouwen dat uw klanten/medewerkers in u hebben te vergroten / handhaven. Maakt u voor het tot stand brengen van uw product of dienst gebruik van de diensten van derden? Gebruik de onderstaande aanbevelingen dan om gerichte opdrachten te geven aan degene die het product of de dienst verder ontwikkelt. Hierdoor voorkomt u dat in een later stadium kostbare aanpassingen nodig zijn. Bijvoorbeeld dat u een systeem moet herontwerpen of een project moet stopzetten.

Uw project: Uitbreiding website Classity

Verantwoordelijke	Classity
Bewerker	De verwerkingsorganisatie
Privacy Officer	Jan de Groot (Nog aan te melden bij de AP)
Datum PIA	2 mei 2018
Impact analyse door	Jan Pieterse, Jeroen van Hemert, Greet Homa
Monitoring opvolging	Sieb de Vries
Verwerking gerechtvaardigd	Ja, wij hebben met deze PIA de voor ons relevante aandachtspunten en risico's in kaart gebracht en gaan deze adresseren.
Scope	De website wordt uitgebreid met een webshop voor consumenten. Het full fillment van de orders wordt uitgevoerd door een derde partij. Onder de diensterlening valt: Bestelling registreren, Order picken en labellen, Pakket aanmelden bij verzender, Facturatie, Orderstatus versturen, Tevredenheidsonderzoek uitvoeren, After sales service verlenen.

Resultaten Privacy Impact Assessment

In de onderstaande grafiek ziet u in welke mate u rekening hebt gehouden met relevante privacyaandachtspunten. Op de onderwerpen waar de grafiek de buitenrand nadert scoort u beter dan op onderwerpen die de kern van de grafiek naderen. Op een onderdeel dat lager scoort zijn dus meer aandachtspunten of risico's van toepassing.



Type project

Aanbeveling	Risico	Actie	Actiehouder
Controleer of de door u aangepaste wijze van verwerking binnen de wettelijke kaders past (en passen bij het doel waarvoor de gegevens verzameld zijn).A	L	Vermijden / Naleven	Jan Pieterse
Controleer of de door u aangepaste wijze van verwerking binnen de wettelijke kaders past (en of de verwerking proportioneel is).A	L	Vermijden / Naleven	geen
Controleer of de door u aangepaste wijze van verwerking binnen de wettelijke kaders past (en passen bij het doel waarvoor de gegevens verzameld zijn).A	L	Vermijden / Naleven	Jeroen van Hemert
Mogelijk schatten niet alle betrokken partijen de risico's op de juiste wijze in of gaan ze onzorgvuldig om met de persoonsgegevens. Borg via een verwerkersovereenkomst dat er goede afspraken zijn over zaken als het doel van de verwerking, de scope van de verwerking, geheimhouding en beveiliging.A	H	Vermijden / Naleven	Jan Pieterse
Houd een register van verwerkingsactiviteiten bij.A	H	Vermijden / Naleven	Jeroen van Hemert

Verwerking gegevens

Aanbeveling	Risico	Actie	Actiehouder
Beperk de verzamelde gegevens tot die gegevens die nodig zijn om uw doel te bereiken (zie ook artikel 25 AVG). Daarnaast leidt het optimaliseren van de hoeveelheid verwerkte persoonsgegevens ertoe dat u minder gegevens hoeft te onderhouden en wordt de kans op fouten verkleind. Ook leidt het mogelijk tot verwerkingsefficientie (betere prestaties, hersteltijden en service niveaus).C	M	Reduceren	Jan Pieterse
Bied kwetsbare doelgroepen de mogelijkheid om zich aan de verwerking te onttrekken. Besteed extra aandacht aan de beveiliging van de gegevens (zie art 32 AVG).A	M	Reduceren	Jeroen van Hemert
Vraag voor de verwerking van gegevens van kinderen onder de 16 jaar altijd toestemming aan de ouder/voogd en registreer deze toestemming.C		Reduceren	Greet Homa

Betrokken partijen

Aanbeveling	Risico	Actie	Actiehouder
Zorg voor een duidelijke gegevensbeschrijving. Beleg de taken en verantwoordelijkheden voor de verwerking van de gegevens eenduidig (beveiliging, foutafhandeling, foutterugmelding, toetsing). Sluit met externe partijen een verwerkersovereenkomst af.A	M	Reduceren	Jan Pieterse

Verzamelen van gegevens

Aanbeveling	Risico	Actie	Actiehouder
U verwerkt van gegevens zonder dat dit publiekelijk bekend is of gemaakt kan worden. Dit brengt een hoog risico voor de betrokken met zich mee. Stel op basis van een belangenafweging vast of het doel van de verwerking opweegt tegen de risico's voor de betrokkenen.A	H	Reduceren	Greet Homa
Registreer de benodigde details over de gegeven toestemming (waarvoor, waar en wanneer, waarover is geinformeerd en hoe de vraag is gesteld).C	H	Reduceren	Greet Homa
Informeer de betrokkene waarom u gegevens over hem/haar verzameld (zie art 13 AVG).C	H	Vermijden / Naleven	Jeroen van Hemert

Gebruik van gegevens

Aanbeveling	Risico	Actie	Actiehouder
Borg dat u door kwalitatief slechte gegevens geen verkeerde conclusies trekt of verkeerde acties onderneemt (zie ook art. 5 AVG, juistheid). Zorg dat gegevens actueel juist en volledig zijn.C	L	Reduceren	
Bied betrokkenen de mogelijkheid om de door u verwerkte gegevens zonder onredelijke vertraging te laten verwijderen. Dit kunt u alleen weigeren indien hiervoor zwaarwegende redenen zijn, welke u op dat moment dient te delen. Gegevens die nodig zijn voor de administratieve verwerking van een overeenkomst kunnen uiteraard niet verwijderd worden totdat de rechtsgrond voor de verwerking komt te vervallen (opzegging van de overeenkomst).C	H	Vermijden / Naleven	Jan Pieterse
Bied betrokkenen de mogelijkheid om de verwerking van de gegevens te laten beperken (met uitzondering van de opslag ervan).A	H	Vermijden / Naleven	Jan Pieterse

Bewaren en vernietigen van gegevens

Aanbeveling	Risico	Actie	Actiehouder
Stel een passende bewaartermijn vast. Bewaar gegevens niet te kort, maar ook niet te lang omdat daarmee de kans op misbruik toeneemt (art. 25 en 30 AVG).C	H	Vermijden / Naleven	Greet Homa
Zorg dat de vernietiging van gegevens onomkeerbaar is.C	M	Accepteren	

Beveiligen van gegevens

Aanbeveling	Risico	Actie	Actiehouder
Stel een informatiebeveiligingsplan op waarin (op basis van uw beveiligingsbeleid) de maatregelen zijn beschreven die borgen dat de gegevens op passende wijze worden beschermd.C	H	Vermijden / Naleven	Jeroen van Hemert

Meldplicht datalekken

Aanbeveling	Risico	Actie	Actiehouder
Borg dat de verantwoordelijken binnen uw organisatie de handreiking datalekken kennen zodat ze daar waar de situatie zich voor doet op de juiste wijze kunnen handelen.C	M	Reduceren	Jan Pieterse

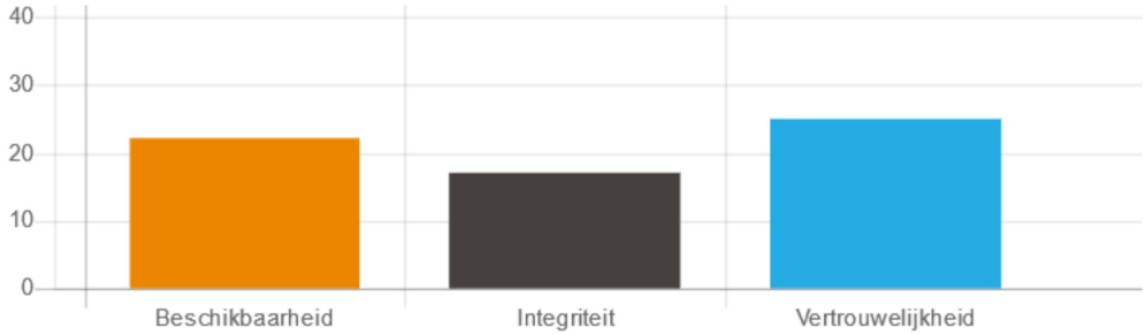
Opvolging

Op basis van deze PIA zijn de onderstaande conclusies en maatregelen vastgesteld. De maatregelen dienen ter reductie van de benoemde risico's en ter naleving van het wettelijke kader.
We gaan ons proces verbeteren en de aanbevelingen gebruiken om onze beveiligings- en privacymaatregelen aan te scherpen.

Op vindt een opvolgingsgesprek plaats. Elke actiehouder bepaalt ter voorbereiding van dit gesprek of er voor de aan hem toegekende risico's maatregelen nader gedetailleerd of toegevoegd moeten worden.

Classificatie en informatiebeveiliging

U heeft uw informatiesysteem of project ter aanvulling op de PIA geclassificeerd op de onderwerpen Beschikbaarheid, Integriteit en Vertrouwelijkheid. De onderstaande tabel geeft de resultaten van deze classificatie weer. Op basis van deze resultaten is er een praktische beveiligingscheclist bij deze PIA gevoegd. Deze checklist kan als aanvulling op uw eigen ISMS en/of de beveiligingsrichtsnoeren van de Autoriteit Persoonsgegevens worden gebruikt. De aandachtspunten uit de checklist helpen u een passend beschermingsniveau te realiseren en datalekken te voorkomen.



Beschikbaarheid

Het door u gewenste beschikbaarheidsniveau is **wezenlijk**
U vraagt een bovengemiddeld beschikbaarheidsniveau van uw informatiesysteem. U doet er verstandig aan extra continuiteitsmaatregelen te treffen.

Integriteit

Het door u gewenste integriteitsniveau is **detecteerbaar**
U stelt geen hoge integriteitseisen aan uw informatiesysteem. Aanvullende maatregelen voor het zekerstellen van de juistheid van gegevens zijn niet noodzakelijk.

Vertrouwelijkheid

Het door u gewenste vertrouwelijkheidsniveau is **vertrouwelijk**
Tref normale beschermingsmaatregelen om misbruik van deze gegevens tegen te gaan en een datalek te voorkomen.

Beveiligingschecklist

De onderstaande beveiligingschecklist helpt u om aan het eind van de ontwerp- of implementatiefase eenvoudig te controleren of de informatiesystemen waar deze PIA betrekking op heeft van de belangrijkste beveiligingsmaatregelen zijn voorzien. De inhoud van deze checklist is gedeeltelijk afhankelijk van de door u bepaalde beschikbaarheids- integriteits- en vertrouwelijkheidsclassificatie.

Beheer van technische kwetsbaarheden	
☐	Processen en procedures voor aanvraag, creatie, hernieuwing, intrekken en beheer van sleutelmateriaal en certificaten zijn opgevolgd.
☐	Er wordt periodiek een kwetsbaarhedenanalyse uitgevoerd.
☐	Er wordt periodiek een penetratietest op de meest bedreigde onderdelen van de infrastructuur uitgevoerd.
☐	De broncode is aan een collegiale toets onderworpen. Tijdens de controle zijn tevens de onderwerpen uit de OWASP Top 10 getoetst.
☐	Er is een patchmanagementproces waarin aandacht is voor het detecteren, beoordelen, inplannen en doorvoeren van beveiligingsupdates.
☐	Beveiligingsupdates met een CVSS score van 8 of hoger worden direct doorgevoerd indien ze vanaf internet toegankelijke kwetsbaarheden verhelpen.
☐	De hier beschreven beveiligingsmaatregelen zijn afgestemd en contractueel vastgelegd met externe leveranciers.
☐	Beheerwerkzaamheden worden uitgevoerd vanaf beveiligde beheerstations. Deze stations bevatten alleen goedgekeurde software, bevatten sterke wachtwoorden, bevatten bijgewerkte antivirus software en zijn voorzien van de laatste beveiligingsupdates. Dit laatste geldt voor alle programmatuur, dus besturingssysteem en applicatiesoftware zoals Java, Acrobat, Flash, Quicktime etcetera. De harde schijven van mobiele beheerwerkplekken zijn volledig versleuteld.
☐	Indien er gebruik wordt gemaakt van mobiele apps, dan bevatten deze Apps geen kwetsbaarheden uit de OWASP Mobile Top 10.
☐	Indien er binnen een webapplicatie externe content of applicatiecode (Javascript) wordt ingeladen, dan zijn er met de hosting partij van deze content of applicatiecode beveiligings- en privacyafspraken gemaakt.

Beleidsdocument voor informatiebeveiliging	
☐	Er is een informatiebeveiligingsbeleid dat expliciet ingaat op de maatregelen die getroffen moeten zijn om de verwerkte persoonsgegevens te beveiligen.
☐	Het informatiebeveiligingsbeleid is goedgekeurd op bestuurlijk c.q. leidinggevend niveau en kenbaar gemaakt aan alle werknemers en relevante externe partijen.