

PRIVACYBELEID

Question Degree als betrouwbare partner



Auteur: Question Degree
Documentnr: 18.0803
Versie: 1.0 / Definitief
Datum: 04-04-2018

Inhoud

1	Inleiding	3
1.1	Wat houdt de AVG in?	3
1.2	Doel van dit document	3
1.3	Leeswijzer	3
2	Wet- en regelgeving	4
3	Rollen en verantwoordelijkheden	5
3.1	Directie	5
3.2	Leidinggevenden en afdelingshoofden	5
3.3	Privacy Officer	5
3.4	Chief Information Security Officer (CISO)	6
3.5	Functionaris gegevensbescherming	6
3.6	Naleving	6
4	Verwerking van persoonsgegevens	7
4.1	Grondslag	7
4.2	Geheimhouding	7
4.3	Doorgifte van persoonsgegevens	7
4.4	Bewaren van persoonsgegevens	8
4.5	Beveiligingsmaatregelen	8
4.6	Vragen en klachten	8
5	Datalek	9
5.1	Melden en registreren	9
5.2	Afhandeling	9
6	Rechten van betrokkenen	10
6.1	Recht op informatie	10
6.2	Recht op inzage	10
6.3	Recht op wijziging, verwijdering en beperking	11
6.4	Bescherming van de rechten	11

1 Inleiding

Dit document geeft weer hoe Question Degree omgaat met persoonsgegevens. Het verwerken van persoonsgegevens dient met een grote zorgvuldigheid te gebeuren omdat misbruik en het uitlekken hiervan schade kan opleveren voor de betrokkenen, maar ook voor Question Degree zelf. Hierom hecht Question Degree veel waarde aan het beschermen van persoonsgegevens die haar worden verstrekt en aan de wijze waarop deze persoonsgegevens worden verwerkt. Het op een juiste manier verwerken van persoonsgegevens is de verantwoordelijkheid van het bestuur van Question Degree. Deze is gevestigd in

Met het beschrijven van de maatregelen in dit privacybeleid beoogt en neemt Question Degree haar verantwoordelijkheid om de kwaliteit van de verwerking en de beveiliging van persoonsgegevens te optimaliseren en daarmee te voldoen aan de relevante privacywet- en regelgeving.

1.1 Wat houdt de AVG in?

De AVG staat voor Algemene Verordening Gegevensbescherming. De Algemene Verordening Gegevensbescherming is op 25 mei 2016 in werking getreden en sinds 25 mei 2018 van kracht gegaan in de hele Europese Unie. Hiervoor had elke lidstaat van de Europese Unie haar eigen nationale wetten gebaseerd op de Europese privacyrichtlijn van 1995, zoals de Wet bescherming persoonsgegevens (Wbp) in Nederland. Door middel van de AVG worden de privacyrechten van mensen versterkt en uitgebreid, is er meer verantwoordelijkheid voor organisaties en gelden dezelfde bevoegdheden voor alle Europese privacytoezichthouders.

1.2 Doel van dit document

Question Degree verwerkt persoonsgegevens van haar klanten. Deze gebruikt zij voor klant wervingscampagnes. Het doel van dit privacybeleid is om te waarborgen dat er zorgvuldig wordt omgegaan met de persoonsgegevens die Question Degree ontvangt en dat zij zich houdt aan de regels en wetgeving hiervoor. Dit privacybeleid is van toepassing op alle betrokkenen die werkzaam zijn bij Question Degree. Question Degree vindt het belangrijk dat persoonsgegevens zorgvuldig verwerkt worden en de verwerkingen rechtmatig plaatsvinden.

1.3 Leeswijzer

In dit document wordt beschreven hoe Question Degree omgaat met persoonsgegevens van haar klanten. In de komende hoofdstukken zal uitgelegd worden voor welke doeleinden Question Degree persoonsgegevens verzamelt, welke rollen en verantwoordelijkheden hierbij naar voren komen en hoe deze persoonsgegevens beveiligd worden. Daarnaast wordt ook het beleid om persoonsgegevens te verwerken toegelicht en beschreven wat de rechten van de betrokkenen zijn.

2 Wet- en regelgeving

Het verwerken van de persoonsgegevens is bij Question Degree gebaseerd op de wettelijke grondslagen die genoemd zijn in de *EU Algemene Verordening Gegevensbescherming*. Kort samengevat houdt dit in dat het verwerken van persoonsgegevens rechtmatig moet zijn, persoonsgegevens alleen verwerkt worden op een manier dat behoorlijk en transparant is ten aanzien van de betrokkene en persoonsgegevens alleen verwerkt worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Daarnaast blijft de hoeveelheid en het soort gegevens beperkt tot de persoonsgegevens die noodzakelijk zijn voor het doeleinde, worden zij niet langer verwerkt dan noodzakelijk is en adequaat beveiligd volgens de geldende beveiligingsnormen.

Question Degree verzamelt persoonsgegevens van haar klanten. De gegevens die zij verzamelen zijn de namen, adressen, postcodes, woonplaatsen, telefoonnummers en e-mailadressen van haar klanten. Deze gegevens zijn nodig om contact te onderhouden over de diensten die zij aanvragen bij Question Degree of om producten naar de klanten toe te sturen. Zonder deze persoonsgegevens is het voor Question Degree niet mogelijk om haar diensten en producten te leveren. Om deze reden dienen klanten deze persoonsgegevens achter te laten wanneer zij een dienst of product aanvragen bij Question Degree. Daarnaast worden de persoonsgegevens 180 dagen bewaard zodat Question Degree diensten en producten kan aanbieden. De persoonsgegevens worden zelf door de klanten achtergelaten via de digitale snelweg. Wanneer zij hun persoonsgegevens achterlaten geven zij hiermee toestemming aan Question Degree om deze gegevens te verwerken. Wanneer zij ervoor kiezen om deze persoonsgegevens niet door te geven kunnen de diensten en producten van Question Degree niet aan de klant geleverd worden.

Naast het implementeren van de wettelijke vereisten die in de *EU Algemene Verordening Gegevensbescherming* benoemd worden, houdt Question Degree zich ook aan de voorschriften uit de Archiefwet en het Archiefbesluit over de wijze waarop omgegaan moet worden met informatie dat is vastgelegd in documenten en informatiesystemen. Dit is onderdeel van de jaarlijkse externe accountantsrapportages.

3 Rollen en verantwoordelijkheden

Om ervoor te zorgen dat er op een betrouwbare manier met persoonsgegevens wordt omgegaan, heeft Question Degree een aantal rollen en verantwoordelijkheden toegewezen aan bestaande medewerkers. Het uitgangspunt van Question Degree is dat het zorgvuldig verwerken van persoonsgegevens een lijnverantwoordelijkheid is. Dit houdt in dat de directie en afdelingshoofden (het lijnmanagement) de primaire verantwoordelijkheid draagt voor een zorgvuldige verwerking van persoonsgegevens op hun afdeling of eenheid. Maar het zorgvuldig omgaan met persoonsgegevens is ieders verantwoordelijkheid. Medewerkers van Question Degree dienen zich integer te moeten gedragen met betrekking tot persoonsgegevens. Wanneer een medewerker opzettelijk een onveilige situatie veroorzaakt wordt dit niet geaccepteerd. Om deze reden zijn er gedragsregels geformuleerd en geïmplementeerd.

3.1 Directie

De directie van Question Degree is de verwerkingsverantwoordelijke en daarmee de eindverantwoordelijke voor de rechtmatige en zorgvuldige verwerking van persoonsgegevens binnen de organisatie. Daarnaast stelt de directie het beleid, de maatregelen en de procedures op het gebied van de verwerking van persoonsgegevens vast.

3.2 Leidinggevenden en afdelingshoofden

Leidinggevenden en afdelingshoofden bij Question Degree zijn verantwoordelijk om bewustwording van het privacybeleid te creëren en ervoor te zorgen dat het privacybeleid wordt nageleefd door de medewerkers. Zij stellen de medewerkers van Question Degree op de hoogte van het beleid en zien toe op de naleving van het beleid. Tevens zijn zij verantwoordelijk om het onderwerp 'Privacy' onder de aandacht te brengen in vergaderingen.

3.3 Privacy Officer

De privacy officer wordt gekozen door de directie en is verantwoordelijk voor het vormgeven en bewaken van het privacybeleid binnen Question Degree. Hij houdt toezicht op de naleving van de privacywetten en –regels. Daarnaast inventariseert en houdt de privacy officer gegevensverwerkingen bij. Wanneer een medewerker een vraag heeft over het verwerken van persoonsgegevens kan hij bij de privacy officer terecht. De privacy officer geeft namelijk medewerkers van Question Degree advies over zaken die gerelateerd zijn aan het verwerken van persoonsgegevens.

Contactgegevens Privacy officer

Naam:	Gerdinand Boerman
Telefoonnummer:	088-7744300
E-mailadres:	opvraagbaar

3.4 Chief Information Security Officer (CISO)

De CISO is verantwoordelijk voor het implementeren van, en toezicht houden op het informatiebeveiligingsbeleid binnen Question Degree. Hij ondersteunt de directie en managers met kennis over informatieveiligheid, zodat zij hun verantwoordelijkheid voor de veiligheid van de informatievoorziening kunnen invullen. De CISO is het aanspreekpunt voor de directie en medewerkers van Question Degree over informatieveiligheid. Hij geeft gevraagd en ongevraagd advies en zal signaleren wanneer zijn functie ongewenste risico's ziet. Om het informatiebeveiligingsbeleid en privacybeleid te controleren op effectiviteit worden er jaarlijks audits gehouden waarbij de CISO betrokken is.

Contactgegevens CISO

Naam:	Gerard Buitenhuis
Telefoonnummer:	088-7744340
E-mailadres:	opvraagbaar

3.5 Functionaris gegevensbescherming

Aangezien Question Degree geen overheidsinstantie of publieke organisatie is, is zij niet verplicht om een functionaris gegevensbescherming aan te stellen. De taken die bij overheidsinstanties of publieke organisaties aan de functionaris gegevensbescherming zijn toegekend worden bij Question Degree door de CISO en privacy officer uitgevoerd.

3.6 Naleving

Iedere medewerker van Question Degree dient in lijn met dit privacybeleid en de daaruit afgeleide maatregelen te handelen. Dit staat beschreven in hun contractuele overeenkomst. De medewerkers dienen zich bewust te zijn over het privacybeleid. Hierom informeert de privacy officer de directie, leidinggevenden en afdelingshoofden hierover. Vervolgens zijn de leidinggevenden en afdelingshoofden verantwoordelijk om de medewerkers van hun afdeling over het privacybeleid in te lichten.

Indien een medewerker opzettelijk de maatregelen uit het privacybeleid overtreedt, wordt hij hierop berispt. Mocht hierna herhaling optreden bij diezelfde medewerker, dan volgt er een sanctie van een minimaal bedrag van €2500,- en de bijbehorende kosten voorkomend uit de schade die door Question Degree of de betrokkene is geleden, en wordt de medewerker volledig uitgesloten van werkzaamheden met Question Degree.

4 Verwerking van persoonsgegevens

Question Degree verwerkt persoonsgegevens die zij ontvangt in overeenstemming met de principes die zijn uitgewerkt in hoofdstuk 2 van dit beleid. In dit hoofdstuk worden deze principes verder toegelicht.

4.1 Grondslag

Question Degree verwerkt persoonsgegevens van haar klanten om haar diensten en producten te kunnen leveren en aan te bieden. Deze persoonsgegevens worden verkregen door de klanten zelf. Door het achterlaten van hun persoonsgegevens geven zij Question Degree toestemming om deze persoonsgegevens te verwerken.

De persoonsgegevens die door Question Degree verzameld worden zijn de namen, adressen, postcodes, woonplaatsen, telefoonnummers en e-mailadressen van haar klanten. Dit houdt in dat er geen bijzondere persoonsgegevens (zoals gegevens over gezondheid, politieke opvattingen of religieuze overtuigingen) worden verzameld.

De persoonsgegevens van de klanten worden door Question Degree verwerkt op een manier die voor haar klanten behoorlijk en transparant is. Zij maakt duidelijk aan haar klanten in hoeverre en op welke manier hun persoonsgegevens verwerkt worden. Wanneer zij de persoonsgegevens achterlaten worden zij ingelicht door middel van een privacyverklaring.

4.2 Geheimhouding

De medewerkers van Question Degree die de persoonsgegevens kunnen inzien hebben een geheimhoudingsplicht. Alle persoonsgegevens die Question Degree ontvangt worden als vertrouwelijk geclassificeerd en alle medewerkers dienen hiernaar te handelen. Dit houdt in dat zij de persoonsgegevens niet verspreiden of misbruiken. Zoals beschreven is in paragraaf 3.6 dienen de medewerkers dit na te leven en vindt er een sanctie plaats wanneer zij dit opzettelijk overtreden.

4.3 Doorgifte van persoonsgegevens

Bij Question Degree worden de persoonsgegevens intern gebruikt. Dit houdt in dat de persoonsgegevens niet worden doorgegeven aan externe partijen tenzij dit wordt gevraagd door de <klant> zelf en hier schriftelijke toestemming voor is gegeven. Wanneer <een klant> zijn persoonsgegevens achterlaat bij Question Degree kunnen deze alleen ingezien worden door de medewerkers die in dienst zijn bij Question Degree.

4.4 Bewaren van persoonsgegevens

Wanneer een <klant> zijn gegevens achterlaat bij Question Degree worden zij bijgehouden in een systeem en minimaal 180 dagen bewaard. De privacy officer houdt toezicht op dit systeem. Na de 180 dagen wordt gekeken of de klant nog een zakelijke relatie heeft met Question Degree en de gegevens nog relevant zijn. Indien Question Degree niet meer diensten of producten levert aan de <klant> worden zijn gegevens na deze 180 dagen verwijderd. Documenten worden geshredderd met een papiervernietiger met als minimale norm DIN P-3. Gegevens die bestemd zijn voor statistische doeleinden worden echter in een archief bewaard dat aanwezig is op het hoofdkantoor van Question Degree. Dit is het geval wanneer de gegevens betrekking hebben op de persoon zijn mening over de kwaliteit van de diensten en producten van Question Degree. Wanneer dit van toepassing is worden de adressen, e-mailadressen en telefoonnummers van deze persoon echter niet meer bewaard.

4.4.1 Verlies van persoonsgegevens voorkomen

Om het verlies van gegevens te voorkomen maakt Question Degree elke dag een back-up van haar informatie en software. Hierbij is er sprake van een mirror back-up in de avonduren zodat alle back-up data exact wordt gekopieerd en niet verloren gaat. Bij het bewaren van back-ups wordt de 3-2-1 regel gehanteerd. Dit betekent dat er minimaal drie kopieën zijn, op minimaal twee verschillende media waarvan één op een andere locatie. Hierdoor veroorzaakt een verstoring op de ene locatie niet voor schade bij de mirror back-up. Daarbij worden back-ups regelmatig getest om te kijken of de back-up leesbaar is. De dagback-up wordt altijd een week bewaard. Tevens wordt de restore procedure minimaal jaarlijks getest of na een grote wijziging om betrouwbaarheid te waarborgen als ze in noodgevallen uitgevoerd moeten worden. Wanneer er een incident voorkomt bedraagt het dataverlies maximaal 25 uur. De hersteltijd van incidenten is maximaal twee werkdagen, oftewel 16 werkuren.

4.5 Beveiligingsmaatregelen

Question Degree is verantwoordelijk om de persoonsgegevens die zij ontvangt te beschermen. Hiervoor zijn passende technische en organisatorische maatregelen genomen. Hierbij hanteert Question Degree het principe 'privacy by design' en 'privacy by default'. Om ervoor te zorgen dat onbevoegden geen inzage krijgen in de verzamelde persoonsgegevens wordt er bijvoorbeeld gebruik gemaakt van een FTP-server. Dit zorgt ervoor dat er een gebruikersnaam en wachtwoord nodig zijn om de persoonsgegevens in te kunnen zien. Daarnaast is het alleen mogelijk om in het systeem in te loggen met een toegestaan IP-adres. Hierdoor kunnen medewerkers de gegevens niet thuis of ergens anders inzien. De precieze maatregelen en de risicoanalyse hiervoor zijn opgenomen in een apart document dat onder toezicht wordt gehouden door de privacy officer en CISO van Question Degree. Er is gekozen om dit niet te publiceren aangezien dit risico's met zich meebrengt.

4.6 Vragen en klachten

Wanneer een betrokkene vragen of klachten heeft in verband met persoonsgegevens kunnen die gemeld worden bij de privacy officer. Van vragen of klachten met een (potentiële) significante impact, wordt een register bijgehouden. De vragen en klachten zullen binnen twee werkdagen behandeld worden. Wanneer de vraag of klacht betrekking heeft op persoonsgegevens die in gevaar zijn wordt dit zo snel mogelijk afgehandeld en wordt de directie ook ingelicht.

5 Datalek

Een datalek houdt in dat er een inbreuk is op de beveiliging van persoonsgegevens. Om een datalek te voorkomen kunnen medewerkers niet buiten het kantoor van Question Degree om inloggen en persoonsgegevens inzien doordat er een IP-adres aan het systeem is toegekend. Mocht er echter alsnog een datalek plaatsvinden doordat er informatie op een USB-stick staat of een e-mail naar een verkeerde persoon is verstuurd, dan gelden de volgende maatregelen.

5.1 Melden en registreren

Wanneer er een datalek plaatsvindt of er een vermoeden van een datalek is, dient hier zo spoedig mogelijk een melding van gemaakt te worden bij de privacy officer. De volgende gegevens dienen hierbij doorgegeven te worden:

Het melden van een datalek

- Wie heeft de melding gemaakt?
- Wat is er gemeld?
- Waar kwam de melding vandaan?
- Welke persoonsgegevens en informatie zijn hierbij betrokken?
- Hoe heeft het incident plaatsgevonden?
- Wanneer heeft het incident plaatsgevonden?
- Wat is er gedaan om het incident op te lossen of te voorkomen?

Alle meldingen die worden gemaakt worden bijgehouden in een register. Wanneer de persoonsgegevens van klanten of de bedrijfsprocessen, financiën of de goede naam van Question Degree in gevaar zijn wordt de directie hiervan op de hoogte gesteld alsook de privacy officer en de CISO. Aangezien Question Degree geen bijzondere persoonsgegevens verwerkt, is zij niet verplicht datalekken door te geven aan Autoriteit Persoonsgegevens.

5.2 Afhandeling

Nadat er een melding heeft plaatsgevonden neemt de directie een advies uit omtrent de verplichting om dit te melden aan de betrokkene. Dit wordt gedaan in combinatie met de privacy officer en wordt door hem doorgegeven aan de betrokkene. Ook vindt er een evaluatie plaats om te kijken hoe een toekomstige datalek voorkomen kan worden. Wanneer de datalek plaatsvond doordat er een fout in het systeem zat dient de CISO dit te verwerken en op te lossen. Alle datalekken die plaatsvinden worden zo snel mogelijk afgehandeld en gerapporteerd.

6 Rechten van betrokkenen

De AVG geeft rechten aan de betrokkenen waarmee zij controle kunnen uitoefenen op de verwerking van hun persoonsgegevens. In dit hoofdstuk wordt er ingegaan op deze rechten.

6.1 Recht op informatie

Wanneer een klant zijn persoonsgegevens worden verwerkt door Question Degree worden zij door Question Degree hierover geïnformeerd. Dit gebeurt wanneer zij hun persoonsgegevens achterlaten. Deze informatie ontvangen zij kosteloos. Er wordt duidelijk gemaakt welke persoonsgegevens Question Degree van haar klanten verwerkt en wat de doeleinden zijn van het verwerken van deze gegevens. Daarnaast worden de klanten ingelicht hoelang de persoonsgegevens bewaard zullen worden en krijgen zij informatie over waar zij een klacht kunnen indienen. Klachten over het verwerken van persoonsgegevens kunnen bij Question Degree aangegeven worden bij de privacy officer, Voornaam Achternaam, zie eerder opgegeven in dit document.

Wanneer een betrokkene het oneens is met het verwerken van zijn persoonsgegevens kan hij ook een bezwaar indienen tegen het verwerken van persoonsgegevens. Dit kan wanneer deze verwerking plaatsvindt op grond van de vervulling van een taak van algemeen belang of in het kader van de uitoefening van het openbaar gezag van Question Degree. Question Degree zal bij bezwaar de verdere verwerking stopzetten. Indien zij kan aantonen dat haar gerechtvaardigde belangen zwaarder wegen dan de belangen of grondrechten van de betrokkene, zal de verwerking worden voortgezet. Question Degree bewaart ook persoonsgegevens voor direct marketing, namelijk om haar producten en diensten aan te bieden aan bestaande klanten. Wanneer een klant zijn gegevens voor dit doeleinde worden gebruikt heeft hij altijd het recht om een bezwaar te maken en dit stop te zetten. Een bezwaar kan ook ingediend worden bij de privacy officer.

6.2 Recht op inzage

Wanneer een klant zijn persoonsgegevens worden verwerkt door Question Degree kan hij deze gegevens inzien. Hij ontvangt een e-mail met zijn aanvraag voor een dienst of product van Question Degree waar de ingevulde persoonsgegevens in vermeld staan. Op deze manier kan hij controleren of deze gegevens correct zijn. Indien dit niet het geval is dient de klant dit aan te geven zodat de gegevens gewijzigd kunnen worden. Zie hiervoor paragraaf 6.3. Wanneer de klant in het systeem staat maar niet op de hoogte is welke persoonsgegevens hierbij vermeld staan kan hij altijd contact opnemen met de privacy officer van Question Degree om een kopie aan te vragen. Vervolgens zal hij een kopie krijgen van de persoonsgegevens die van hem bekend zijn bij Question Degree.

6.2.1 Dataportabiliteit

Een klant kan ook een verzoek indienen om zijn gegevens te verkrijgen per e-mail en deze naar een andere organisatie te laten doorsturen. Voordat persoonsgegevens echter doorgegeven kunnen worden aan een andere organisatie dient de klant hier nadrukkelijk schriftelijke toestemming voor te geven. Question Degree houdt hierbij rekening met de rechten en vrijheden van haar klanten.

6.3 Recht op wijziging, verwijdering en beperking

Klanten van wie de persoonsgegevens door Question Degree worden verwerkt hebben altijd het recht om kosteloos contact op te nemen met de privacy officer van Question Degree om hun gegevens aan te vullen, te wijzigen of te verwijderen. Daarnaast kunnen zij ook kosteloos een verzoek bij de privacy officer indienen om de verwerking van persoonsgegevens te beperken. Wanneer er een verzoek wordt ingediend om gegevens te beperken worden de persoonsgegevens die beperkt zijn afgeschermd.

Wanneer blijkt dat de persoonsgegevens die de klant heeft doorgegeven onjuist zijn, voor het doel van Question Degree onvolledig zijn of in strijd met een wettelijk voorschrift zijn verwerkt, zal de privacy officer deze gegevens verbeteren, permanent verwijderen, aanvullen of beperken. Hierover wordt contact opgenomen met de klant van wie de gegevens wordt verwerkt. De privacy officer zorgt ervoor dat een verzoek tot verbetering, aanvulling, verwijdering of afscherming zo spoedig mogelijk wordt uitgevoerd.

6.4 Bescherming van de rechten

Wanneer een klant van mening is dat de bepalingen in dit privacybeleid niet overeenkomen met de wettelijke bepalingen inzake de privacybescherming, kan hij een schriftelijke klacht indienen bij Voornaam Achternaam zie eerder in dit document. Klachten en verzoeken zullen zo spoedig mogelijk verwerkt worden.

6.4.1 Besluit tot afwijzing van een klacht of verzoek

Mocht een klacht of ingediend verzoek betrekking hebben op het overtreden van de AVG en afgewezen worden door Question Degree en de klant het hier niet mee eens zijn, dan heeft hij de mogelijkheid een verzoekschriftprocedure te starten bij de kantonrechter. Het verzoekschrift dient binnen zes weken na ontvangst van het antwoord op de klacht of het verzoek van Question Degree ingediend te worden bij de kantonrechter. Indien er niet een antwoord is gegeven binnen de gestelde termijn op het verzoek van de klant moet het verzoekschrift binnen zes weken na afloop van die termijn worden ingediend.

Wanneer het besluit is afgewezen en aan te merken is als een besluit van een bestuursorgaan heeft de klant de mogelijkheid een bezwaarschriftprocedure te starten. Een bezwaarschriftprocedure moet altijd gestart worden binnen 6 weken na bekendmaking van een besluit van Question Degree. Tegen de beslissing op bezwaar, staat beroep open bij de rechtbank. Daarnaast kan de klant ook een klacht indienen bij een toezichthoudende autoriteit.