Informatiebeveiligings- en privacy beleid

Ambitie, doel en scope beleid

In dit document wordt beleid en een aanpak vastgesteld om de beschikbaarheid, integriteit en vertrouwelijkheid van informatie op een passende wijze en blijvend te borgen en daarbij te voldoen aan de AVG.

PAO Psychologie vindt dat cursisten, docenten en medewerkers erop moeten kunnen vertrouwen dat PAO zorgvuldig en veilig met hun persoonsgegevens omgaat.

Nieuwe technologische ontwikkelingen, innovatieve voorzieningen en verschillende vormen van samenwerking stellen steeds zwaardere eisen aan de bescherming van gegevens en privacy. PAO is zich hiervan bewust en zorgt dat de privacy gewaarborgd blijft, onder andere door maatregelen op het gebied van informatiebeveiliging, dataminimalisatie, transparantie en gebruikerscontrole.

Door middel van dit beleid wordt een duidelijke richting gegeven aan informatiebeveiliging en privacy en laat PAO zien dat zij de privacy waarborgt, beschermt en handhaaft.

De **ambitie** bij dit beleid is om met behulp van dit beleidsdocument de informatieveiligheid structureel naar een hoog niveau te brengen en daar te houden.

Doelen die daarvoor gesteld worden zijn:

- Het waarborgen van de beschikbaarheid van informatie van het onderwijs en de bedrijfsvoering.
- Het waarborgen dat informatie juist, volledig en actueel is (integriteit) en alleen toegankelijk is voor personen die vanuit hun rol/functie daar toegang tot mogen hebben (beschikbaarheid, integriteit en vertrouwelijkheid).
- Het voorkomen van beveiligings- en privacy-incidenten en de eventuele gevolgen hiervan verminderen.

Deze doelen worden hierna concreet gemaakt.

De **scope** van dit beleid is als volgt:

- Het informatiebeveiligings- en privacybeleid is van toepassing op de gehele organisatie;
- Het beleid is van toepassing op de eigen medewerkers, docenten en cursisten;
- Het informatiebeveiligings- en privacybeleid is van toepassing op alle formeel vastgelegde informatie;
- Het informatiebeveiligings- en privacybeleid is van toepassing op alle instellingsonderdelen en -dienstverlening;
- Het beleid is locatie-onafhankelijk.

Beleidsprincipes

PAO heeft beleidsprincipes voor informatiebeveiliging vastgesteld. Deze helpen om te bepalen welke beveiligingsmaatregelen er nodig zijn

Vijf beleidsprincipes zijn leidend, namelijk:

1. Risico-gebaseerd

We baseren de maatregelen op de mogelijke veiligheidsrisico's van onze informatie, processen en IT-faciliteiten.

2. Iedereen

Iedereen is en voelt zich verantwoordelijk voor een juist en veilig gebruik van middelen en bevoegdheden.

3. Altijd

Informatiebeveiliging zit in het DNA van al onze werkzaamheden en processen.

4. Security by Design

Informatiebeveiliging is vanaf de start een integraal onderdeel van ieder project of iedere verandering m.b.t. informatie, processen en IT-faciliteiten.

5. Security by Default

Gebruikers hebben alleen toegang tot informatie en IT-faciliteiten die zij nodig hebben voor hun werkzaamheden. Het openstellen van informatie is een bewuste keuze.

Verantwoordelijkheid Informatiebeveiliging en Privacy

Ten aanzien van de verantwoordelijkheden onderkent PAO de volgende rollen:

Eigenaar:

De directeur van PAO Psychologie is eindverantwoordelijk voor het informatiebeveiligingsbeleid en daarmee het voldoen aan wetten en normen.

Interne privacy expert:

Binnen PAO houdt de Informatieadviseur zich bezig met de bescherming van persoonsgegevens en is tevens de interne privacy expert. De privacy expert heeft een onafhankelijke rol en is toezichthouder rondom de naleving van de wet- en regelgeving met betrekking tot privacy en gegevensbescherming binnen de organisatie.

Categorieën persoonsgegevens

PAO Psychologie verwerkt persoonsgegevens van cursisten, zodat zij gebruik kunnen maken van onze diensten. PAO verwerkt deze persoonsgegevens alleen als de cursist daar zelf toestemming voor heeft gegeven of als zijn/haar bedrijf de cursist middels een overeenkomst een Incompany cursus van PAO Psychologie aanbiedt. PAO Psychologie verwerkt deze gegevens zorgvuldig en vertrouwelijk volgens de geldende privacyregels. Bij de inschrijving van een cursus kan de cursist een vakje aanvinken waarmee men akkoord gaat met de Algemene Voorwaarden en het verwerken van zijn/haar persoonsgegevens.

Dit is het overzicht van de persoonsgegevens die PAO verwerkt en waarom zij ze verwerkt.

- Voor- en achternaam (voor het kunnen inschrijven voor cursus, webinar of opleiding, deelname en certificering)
- Adresgegevens (opsturen certificaat en factuur)
- Telefoonnummer (ivm vragen die betrekking hebben op de scholing)
- E-mailadres (ivm vragen over de scholing, informeren over cursus en certificering, toegang tot de online leeromgeving, versturen nieuwsbrief)
- Overige persoonsgegevens die men actief verstrekt in correspondentie per email en telefonisch, bijvoorbeeld maar niet uitsluitend:
    - Lidmaatschap en registratienummer bij een beroepsvereniging (voor het invoeren van de presentie en certificering)
    - Functietitel (bepalen of je tot de doelgroep van de cursus behoort)
    - Naam en adres werkgever (om de betaling te kunnen verwerken mits deze via werkgever verloopt)
    - Geboortedatum, doopnamen, meisjesnaam, titel en geboorteplaats (voor het verstrekken van een CPION-diploma van de opleiding Post-HBO zorg en onderwijs aan kinderen en volwassenen met ernstige meervoudige beperkingen)

Verwerkingsdoeleinden

Persoonsgegevens mogen alleen verwerkt worden als het echt niet anders kan. PAO verwerkt persoonsgegevens bij de inschrijving van cursussen die PAO aanbiedt. Dit is nodig om de cursist een factuur en een certificaat te kunnen sturen, toegang te geven tot de leeromgeving, accreditatiepunten te geven, berichten over de cursus te kunnen sturen. Kortom: het is nodig om een cursist een cursus te kunnen laten volgen.

De wettelijke grondslagen voor het verwerken van deze gegevens zijn Toestemming en Uitvoering Overeenkomst.

Grondslag Toestemming

Voor de inschrijving van cursussen is de eerste grondslag van toepassing: PAO heeft toestemming van de persoon om wie het gaat. Voor offertes van Incompany uitvoeringen geldt de grondslag Overeenkomst.

Bij de inschrijving van een cursus op het opleidingsportaal kan een cursist een vakje aanvinken om aan te geven dat hij akkoord gaat met de Algemene Voorwaarden en met het verwerken van zijn persoonsgegevens. De cursist kan vervolgens, door te klikken op de woorden Algemene Voorwaarden en het woord persoonsgegevens, de algemene voorwaarden en de privacyverklaring direct lezen.

Juiste eisen aan toestemming

De toestemming wordt vrijelijk gegeven. Men wordt niet onder druk gezet. De toestemming is specifiek en dient slechts 1 doel: inschrijven voor de cursus. De toestemming is ondubbelzinnig, want het vakje is niet vooraf aangevinkt. Tevens is men geïnformeerd over de identiteit van PAO, het doel van elke verwerking, welke persoonsgegevens verzameld worden en het recht dat men heeft om de toestemming weer in te trekken. Dit staat in de privacyverklaring die op pao.nl eenvoudig te vinden is en waar in de Algemene Voorwaarden naar wordt verwezen.

Grondslag Uitvoering Overeenkomst

Het is voor PAO noodzakelijk om persoonsgegevens te verwerken om een overeenkomst tussen een bedrijf en PAO Psychologie uit te voeren. Dit is het geval als een bedrijf meerdere medewerkers een cursus van PAO aanbiedt op een eigen locatie, een zogenaamde Incompany cursus. De grondslag geldt voor de offerte-fase.

In de offerte worden geen persoonsgegevens gevraagd. In de overeenkomst wel. Dit zijn alleen gegevens die noodzakelijk zijn om de cursus te kunnen volgen en zo de overeenkomst na te kunnen leven. PAO Psychologie gebruikt de gegevens bijvoorbeeld niet om het koopgedrag te analyseren. Het gaat om:

- Achternaam
- Tussenvoegsel

- Voorletter
- Roepnaam
- Titel
- Emailadres zakelijk (om cursisten te kunnen informeren over de cursus)
- Functie (om te bepalen of men voldoet aan de ingangseisen van de betreffende cursus)
- Registratienummer(s) bij de beroepsvereniging(en) (ivm de toekenning van accreditatiepunten aan de cursisten).

Het bedrijf krijgt van PAO een Excel formulier waar men de gegevens invoert. De gegevens op dit formulier worden door een medewerker van PAO in de cursusadministratie geïmporteerd bij de betreffende Incompany cursus. De gegevens zijn daar terug te vinden.

Rechten van betrokkenen

Rechten die cursisten en medewerkers onder de AVG hebben:

- Recht op **inzage**. Dat is het recht om onder meer een kopie te ontvangen van de persoonsgegevens die PAO van hen verwerkt.
- Recht op **vergetelheid**. Mensen hebben het recht om 'vergeten' te worden.
- Recht op rectificatie en aanvulling. Het recht om de persoonsgegevens die PAO verwerkt te laten wijzigen.
- 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 minder gegevens te laten verwerken.
- Het recht met betrekking tot **geautomatiseerde besluitvorming en profilering**. Oftewel: het recht op een menselijke blik bij besluiten.
- Het recht om **bezwaar** te maken tegen de gegevensverwerking.
- Ten slotte hebben mensen recht op **duidelijke informatie** over wat PAO met hun persoonsgegevens doet.

Om gebruik te maken van zijn/haar rechten kan de betrokkene een verzoek indienen. Dit verzoek kan zowel schriftelijk als via de e-mail ingediend worden. PAO Psychologie heeft vier weken de tijd, vanaf de ontvangst van het verzoek, om te beoordelen of het verzoek gerechtvaardigd is. Binnen vier weken zal PAO laten weten wat er met het verzoek gaat gebeuren. Als het verzoek niet wordt opgevolgd is er de mogelijkheid om bezwaar te maken bij PAO Psychologie, of een klacht in te dienen bij de Autoriteit Persoonsgegevens (AP). Aan de hand van een verzoek kan PAO aanvullende informatie opvragen om zeker te zijn van de identiteit van de betrokkene.

Het verzoek dient bij voorkeur te worden ingediend via: info@pao.nl of anders per post.

Betrokkenen worden geïnformeerd met behulp van een privacyverklaring.

Privacy by design & default

Privacy by design

Privacy by design houdt in dat PAO er al *bij het ontwerpen van producten en diensten* voor zorgt dat persoonsgegevens goed worden beschermd. En dat de gegevens *niet langer worden bewaard dan nodig* is voor het doel van de verwerking.

Voorstellen voor nieuwe (of wijzigingen aan bestaande) systemen, apparaten of verwerkingen legt PAO in een vroeg stadium voor aan de interne privacy expert en/of een externe privacy jurist. Hij/zij kan dan meekijken of in het ontwerp voorzien is in passende technische en organisatorische maatregelen.

De persoonsgegevens van de producten en diensten van PAO Psychologie worden volgens het principe Privacy by design met technische en organisatorische maatregelen goed beschermd.

Enkele van deze maatregelen zijn:

- PAO bevordert het beveiligingsbewustzijn door jaarlijks de bestaande medewerkers te informeren over hun rol in de bescherming van persoonsgegevens en door nieuwe medewerkers bij het inwerktraject te informeren over de AVG en hun rol daarin.
- PAO heeft een protocol voor de afhandeling van datalekken en beveiligingsincidenten.
- PAO heeft met de betrokken partijen die persoonsgegevens voor PAO verwerken verwerkersovereenkomsten afgesloten.
- Logische en fysieke beveiliging van apparatuur.
- Technisch beheer van de autorisaties en bijhouden van logbestanden.
- Dedicated servers in gespecialiseerd datacenters met systeem- en databack-ups.
- Betrokkenen worden middels Privacyverklaringen ingelicht.

Bewaartermijnen gegevens

Persoonsgegevens worden niet langer bewaard dan noodzakelijk is voor de doeleinden waarvoor zij zijn verzameld of worden gebruikt. PAO Psychologie controleert jaarlijks de oudst aanwezige data. Persoonsgegevens die ouder zijn dan 5 jaar worden tijdens deze controle waar mogelijk verwijderd of geanonimiseerd.

Privacy by default

Privacy by default houdt in dat de standaardinstellingen van de producten en/of diensten vanuit het perspectief van een buitenstaander privacyvriendelijk zijn. Dit betekent dat PAO technische en organisatorische maatregelen neemt om ervoor te

zorgen dat PAO, als standaard, alléén persoonsgegevens verwerkt die noodzakelijk zijn voor het specifieke doel dat PAO wil bereiken.

De standaardinstellingen van de producten, systemen en diensten die PAO aanbiedt zijn privacyvriendelijk:

- ✓ Er worden nooit meer gegevens gevraagd dan noodzakelijk is.
- ✓ De locatie van gebruikers wordt niet geregistreerd als dat niet nodig is.
- ✓ Er zijn geen vakjes vooraf aangevinkt.
- ✓ Gebruikers hoeven niets aan instellingen en functies te wijzigen om hun privacy te beschermen.

Verantwoordingsplicht

Verwerkingsregister

PAO Psychologie is verwerkingsverantwoordelijke en beschikt over een verwerkingsregister.

Register Datalekken

Als er binnen PAO een datalek optreedt waarbij er kans is op verlies of onrechtmatige verwerking van persoonsgegevens, dan kan PAO verplicht zijn een melding te doen bij de Autoriteit Persoonsgegevens. PAO beschikt over een datalekregister.

Toestemming voor gegevensverwerking

PAO kan aantonen dat een betrokkene daadwerkelijk toestemming heeft gegeven voor een gegevensverwerking wanneer PAO voor deze verwerking toestemming nodig heeft.

Functionaris Gegevensbescherming (FG)

Op grond van artikel 37 van de AVG heeft PAO geconcludeerd dat het aanstellen van een FG niet verplicht is. De genoemde situaties in dit artikel waarbij men wel verplicht is een FG aan te stellen, zijn niet op PAO van toepassing.

Privacyverklaring

Privacyverklaring

Jaarlijkse controle

Jaarlijks, in januari, controleert PAO of de organisatie nog steeds aan een aantal belangrijke onderdelen van de AVG voldoet. Eventuele acties zullen gedurende het jaar worden uitgevoerd.