**Checklist:**

Print

Bewustwording

☑

Jouw organisatie is op de hoogte van de nieuwe privacyregels.

Jouw organisatie is niet op de hoogte van de nieuwe privacyregels.

Je moet kunnen aantonen dat de mensen in jouw organisatie zich bewust zijn van de nieuwe wet- en regelgeving. Bovendien is het van belang dat jouw organisatie op tijd de juiste acties onderneemt en de juiste mensen aanhaakt om te voldoen aan de AVG: De AVG kan aanzienlijke impact hebben op jouw diensten en processen.

☐ Ga naar https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving en lees je in.
☐ Zorg voor bewustwording in de organisatie, bijvoorbeeld door een vergadering over het belang van informatiebeveiliging en privacy te houden.

Verwerkingsregister

☑ Je beschikt over een verwerkingsregister. Je beschikt over een verwerkingsregister.

Een verwerkingsregister is nodig om aan de Autoriteit Persoonsgegevens te kunnen laten zien dat je voldoet aan de AVG. Daarnaast is een verwerkingsregister van belang als een betrokkene zijn of haar privacyrechten wil uitoefenen.

☑ met de categorieën van betrokken partijen

Voeg in je verwerkingsregister een kolom toe met de categorieën van betrokken partijen

☑ met de doelen van de gegevensverwerking

Voeg in je verwerkingsregister een kolom toe met de doelen van de gegevensverzameling

☑ met de grondslag van de gegevensverwerking

Voeg in je verwerkingsregister een kolom toe met de grondslag van de gegevensverwerking

- Al jouw gegevensverwerkingen moeten gebaseerd zijn op een AVG-grondslag. Voeg in je verwerkingsregister een kolom toe met de de op jou van toepassing zijnde grondslagen van gegevensverwerking. Kijk hier voor de zes AVG-grondslagen.

☑ met informatie over hoe lang de gegevens worden bewaard

Let op dat deze niet de wettelijke bewaartermijn overschrijdt! Voeg in je verwerkingsregister een kolom toe met informatie over hoe lang de gegevens worden bewaard

☑ met een overzicht van welke interne en externe partijen de gegevens krijgen te zien Voeg in je verwerkingsregister een kolom toe met informatie over hoe lang de gegevens worden bewaard

☑ waarin het staat genoteerd als gegevens met een land of organisatie buiten de EU worden gedeeld

Noteer in het verwerkingsregister als gegevens met een land of organisatie buiten de EU worden gedeeld

- Achterhaal of gegevens buiten de EU gaan. Voeg in jouw verwerkingsregister een kolom toe waarin je dit zet. Let op! In landen buiten de EU is niet altijd sprake van een aan de AVG gelijke wetgeving. Je bent er echter toe verplicht de data toch AVG-proof te hebben. Informeer bij de bedrijven buiten de EU naar “GDPR compliancy” en of er ISO-certificaten zijn behaald.

☑ met een korte beschrijving van maatregelen die je hebt genomen om de persoonsgegevens te beveiligen
Voeg in je verwerkingsregister een kolom toe met een beschrijving van maatregelen die je hebt genomen om de persoonsgegevens te beveiligen
Je beschikt niet over een verwerkingsregister.
Een verwerkingsregister is nodig om aan de Autoriteit Persoonsgegevens te kunnen laten zien dat je voldoet aan de AVG. Daarnaast is een verwerkingsregister van belang als een betrokkene zijn of haar privacyrechten wil uitoefenen.
☐ Breng in kaart welke gegevens je allemaal verzamelt.
☐ Zet dit in een tabel (het "verwerkingsregister").
☐ Voeg in je verwerkingsregister een kolom toe met de categorieën van betrokken partijen
☐ Voeg in je verwerkingsregister een kolom toe met de doelen van de gegevensverzameling
☐ Voeg in je verwerkingsregister een kolom toe met de grondslag van de gegevensverwerking

- Al jouw gegevensverwerkingen moeten gebaseerd zijn op een AVG-grondslag. Voeg in je verwerkingsregister een kolom toe met de de op jou van toepassing zijnde grondslagen van gegevensverwerking. Kijk hier voor de zes AVG-grondslagen.

☐ Voeg in je verwerkingsregister een kolom toe met informatie over hoe lang de gegevens worden bewaard
☐ Voeg in je verwerkingsregister een kolom toe met informatie over hoe lang de gegevens worden bewaard
☐ waarin het niet staat genoteerd als gegevens met een land of organisatie buiten de EU worden gedeeld

- Achterhaal of gegevens buiten de EU gaan. Voeg in jouw verwerkingsregister een kolom toe waarin je dit zet. Let op! In landen buiten de EU is niet altijd sprake van een aan de AVG gelijke wetgeving. Je bent er echter toe verplicht de data toch AVG-proof te hebben. Informeer bij de bedrijven buiten de EU naar "GDPR compliancy" en of er ISO-certificaten zijn behaald.

☐ Voeg in je verwerkingsregister een kolom toe met een beschrijving van maatregelen die je hebt genomen om de persoonsgegevens te beveiligen
Privacyrechten
☑ Je informeert mensen voldoende over wat je met hun data doet en hun privacyrechten
Mogelijk informeer je mensen onvoldoende over wat je met hun data doet en over hun privacyrechten
Informatievoorziening is cruciaal om te voldoen aan de AVG. Met een privacystatement dat voldoet aan de eisen van de AVG kun je een mooie slag maken. Zet in dit privacystatement welke data je verzamelt, wat je met data doet, welke rechten betrokkenen hebben en ook hoe zij verzoeken bij jou kunnen indienen. Je zult zelf binnen redelijke tijd (uiterlijk 4 weken) aan zo'n verzoek moeten kunnen voldoen
☑ Je beschikt over procedures die je volgt als er een privacyverzoek wordt ingediend.
Je hebt geen procedure die je volgt als er een privacyverzoek wordt ingediend.
Je moet kunnen aantonen dat je in staat bent te voldoen aan privacyverzoeken van personen van wie je persoonsgegevens verzamelt. Met een navolgbare procedure kun je laten zien dat je hierover hebt nagedacht. Misschien moet je ook nog technische aanpassingen doen om in staat te zijn privacyverzoeken in te willigen. Denk hier goed over na. Een overzicht van de privacyrechten vind je hier.
DPIA
☑ Je hebt een Data Protection Impact Assessment uitgevoerd.
Pluform heeft reeds een DPIA voor jou opgesteld waarbij je enkel jouw eigen gegevens nog hoeft aan te vullen.
Je moet nog een Data Protection Impact Assessment uitvoeren.
Voer een DPIA uit. Een DPIA bevat de volgende ingrediënten: een beschrijving van de gegevensverwerkingen en de doeleinden hiervan; een beoordeling van de noodzaak en de proportionaliteit van de verwerkingen; een beoordeling van de privacyrisico's voor de betrokkenen; de

beoogde maatregelen om de risico's aan te pakken en aan te tonen dat u aan de AVG voldoet. Zie hier voor een handreiking voor de uitvoering van een DPIA. Je hoeft geen Data Protection Impact Assessment uit te voeren.
Toelichting: Let op! Bij de verantwoordingsplicht van de AVG hoort ook dat je moet kunnen uitleggen waarom je vindt dat je niet een Data Protection Impact Assessment hoeft uit te voeren. In sommige gevallen is het daarom verstandig om alsnog wel een Data Protection Impact Assessment uit te voeren.
Privacy by design en privacy by default
☑ Je verzamelt niet te veel persoonsgegevens.
Je verzamelt te veel persoonsgegevens.
Volgens de principes van privacy by design en privacy by default moet je erop letten zo weinig mogelijk persoonsgegevens te verzamelen en deze zo kort mogelijk te bewaren. Ga na welke gegevens je ook kunt nalaten te verzamelen. Mogelijk zijn hier technische maatregelen voor nodig. Let in het maken van nieuwe producten ook op het toepassen van deze regels.
☑ Je bewaart de persoonsgegevens niet te lang.
Je bewaart de gegevens langer dan strikt noodzakelijk.
Volgens de principes van privacy by design en privacy by default moet je erop letten zo weinig mogelijk persoonsgegevens te verzamelen en deze zo kort mogelijk te bewaren. Ga na welke gegevens je ook kunt nalaten te verzamelen. Mogelijk zijn hier technische maatregelen voor nodig.
☑ Je hebt het toegangsbeheer op basis van need to know geregeld.
Je hebt het toegangsbeheer niet geregeld op basis van need to know.
Het is van belang dat alleen geautoriseerde personen toegang hebben tot de persoonsgegevens. Je dient dit te regelen en aantoonbaar te maken, bijvoorbeeld door een maandelijks autorisatie-overzicht te maken.
Meldplicht datalekken
☑ Je kunt aantonen dat jouw procedure voor het omgaan met datalekken voldoet aan de AVG.
Pluform heeft een goede procedure voor de meldplicht datalekken.
Je kunt niet aantonen dat jouw procedure voor het omgaan met datalekken voldoet aan de AVG.
Maak een incidentenmanagementhandboek. Zie hier voor meer informatie
☑ Je documenteert datalekken en incidenten volgens de AVG.
Pluform documenteert datalekken en incidenten volgens de AVG.
Als Verwerkingsverantwoordelijke blijf je verantwoordelijk voor het melden en documenteren van datalekken. Je kunt hiervoor de relevante documentatie van Pluform ter inspiratie gebruiken. Je documenteert datalekken en incidenten niet volgens de minimale eisen van de AVG.
Maak een format waarin je zowel gemelde als niet gemelde datalekken, hun feiten, gevolgen en maatregelen kunt gaan documenteren.
Verwerkersovereenkomsten
☑ Je hebt (een) verwerkersovereenkomst(en) met je verwerker(s).
Je hebt al beschikking over, of kunt bij Pluform vragen om, een verwerkersovereenkomst met Pluform. Hierin staat alles wat je nodig hebt.
Je moet nog verwerkersovereenkomsten maken met alle verwerkers.
Maak een verwerkersovereenkomst.
☐ met het onderwerp en de duur van de verwerking
Voeg het onderwerp en de duur van de verwerking toe in de verwerkersovereenkomst.
☐ met de aard en het doel van de verwerking
Voeg de aard en het doel van de verwerking toe in de verwerkersovereenkomst
☐ met het soort persoonsgegevens dat wordt verwerkt
Voeg het soort verwerkte persoonsgegevens toe in de verwerkersovereenkomst
☐ met de categorieën van betrokken partijen
Voeg de categorieën betrokken partijen toe in de verwerkersovereenkomst.
☐ met uw rechten en verplichtingen erin beschreven.
Voeg jouw rechten en verplichtingen toe in de verwerkersovereenkomst
☐ met de rechten en verplichtingen van de verwerker erin beschreven.

Voeg de rechten en verplichtingen van de verwerker toe. Dit zijn tenminste:

- De verwerker verwerkt de persoonsgegevens in principe op basis van schriftelijke instructies van jou
- De verwerker waarborgt dat de gegevens vertrouwelijk en op basis van geheimhouding worden verwerkt
- De verwerker schakelt geen subverwerkers in zonder jouw voorafgaande schriftelijke toestemming
- De verwerker neemt de vereiste maatregelen voor beveiliging van de verwerking,
- De verwerker ondersteunt jou in het uitvoeren van de privacyrechten van betrokkenen
- De verwerker helpt jou bij het nakomen van verplichtingen m.b.t. beveiliging en de meldplicht datalekken,
- Na afloop van de verwerkingsdiensten wist de verwerker de persoonsgegevens, bezorgt hij deze terug, of verwijdert hij kopieën, tenzij anders is aangegeven
- De verwerker stelt jou alles ter beschikking om nakoming van jouw verplichtingen aan te kunnen tonen en werkt mee aan audits.

Je hoeft geen verwerkersovereenkomsten te maken.
Verantwoordingsplicht
☑ Je bent in staat aan te tonen welke technische en organisatorische maatregelen je neemt om de persoonsgegevens te beschermen.
Pluform kan aantonen welke technische en organisatorische maatregelen worden genomen om de persoonsgegevens te beschermen. Zie daarvoor de verwerkersovereenkomst of neem contact op met de servicedesk.
Als Verwerkingsverantwoordelijke blijf je verantwoordelijk voor het aantonen van welke technische en organisatorische maatregelen je neemt om persoonsgegevens te beschermen. Je kunt hiervoor de relevante documentatie van Pluform ter inspiratie gebruiken. Onder de verantwoordingsplicht valt dat je kunt laten zien welke maatregelen jouw organisatie heeft genomen en neemt om persoonsgegevens te beschermen. Ga na welke beveiligingsmaatregelen je neemt en documenteer dit.
Wil je jouw cliëntgegevens veilig op één plek? Ga dan naar Pluform voor een gratis proefaccount.

Naar Pluform