AVG Proof in 15 stappen

Vanaf 25 mei 2018 moeten organisaties voldoen aan de bepalingen uit de Algemene Verordening Gegevensbescherming (AVG) en de invoeringswet. De AVG vervangt de Wet Bescherming Persoonsgegevens (Wbp). Er is geen overgangsrecht van toepassing, dus vanaf 25 mei 2018 gaat de Autoriteit Persoonsgegevens de wet handhaven. Niet voldoen aan de AVG-privacy wetgeving kan sancties en hoge boetes opleveren, tot wel 4% van de wereldwijde omzet.

1. **Bewustwording**
   - Informeer het management, afdelingen, medewerkers en andere betrokkenen.
   - Organiseer kennissessies en laat alle betrokkenen meedenken in het proces.
   - Wie, wat, waar, wanneer, hoe en waarom verwerken we privacygevoelige informatie?

2. **Inventarisatie**
   - Inventariseer waar privacygevoelige informatie wordt opgeslagen (dataopslag én papier).
   - Inventariseer wie de privacygevoelige informatie verwerkt (verwerkers én bewerkers).
   - Inventariseer met wie de privacygevoelige informatie wordt gedeeld (leveranciers e.d.).
   - Maak een stroomschema vanaf de invoer van data, via informatiebeheer naar dataopslag (Wie? Wat? Waar? Wanneer? Hoe? Waarom?).

3. **Register**
   - Maak een verwerkingsregister aan om de verantwoordingsplicht duidelijk te krijgen.
   - Wie is de verwerker van de gegevens? Wie is de verwerkingsverantwoordelijke?
   - Controleer of er verwerkersovereenkomsten zijn gesloten met leveranciers e.d.
   - Welke beveiligingsmaatregelen zijn genomen om de gegevens te beschermen?
   - Welke beveiligingsrisico's zijn nog niet (volledig) gedekt?

4. **Verantwoording**
   - De gegevensverwerking moet niet alleen aan de AVG-beginselen voldoen, maar organisaties moeten dit ook volledig en transparant kunnen aantonen.
   - Dit betekent in veel gevallen dat er kritisch gekeken moet worden naar juridische documentatie, onderbouwing en argumentatie van gegevensverwerking.
   - Het verdient aanbeveling een periodieke review of internal audit uit te (laten) voeren.

5. **Communicatie**
   - Controleer of de (juridische) documentatie van de organisatie voldoet aan de inhoudelijke eisen uit de AVG wet- en regelgeving.
   - Denk hierbij aan statuten & reglementen, procedures, protocollen en richtlijnen zoals de Code of Conduct en Social Media gedragsregels.
   - De AVG geeft een opsomming van de informatie die beschikbaar moet zijn voor alle betrokkenen, zodat duidelijk is hoe het recht op privacy wordt gewaarborgd.
   - De verwerkingsdoeleinden: waarom verwerken we deze gegevens?
   - De rechtsgrond van de verwerking: wat is het gerechtvaardigde belang van verwerking?
   - De bewaartermijnen en de criteria of voorwaarden die hierbij worden gehanteerd.

6. **Rechten van betrokkenen**
   - Beoordeel of de rechten van betrokkenen voldoende duidelijk worden gecommuniceerd.
   - Geef duidelijk aan wat de meldingsprocedure is en wie de vertrouwenspersoon is.
   - Neem deze procedures op in het klachtenregelement en/of het privacy statement.
   - Betrokkenen hebben niet alleen recht op inzage en correctie van hun privacygevoelige informatie, maar ook recht op vergetelheid en dataportabiliteit.
   - Recht op vergetelheid: het recht om privacygevoelige informatie te laten wissen op eerste verzoek van de betrokkene wiens privacy is geschonden.
   - Recht op dataportabiliteit: het recht om privacygevoelige informatie te laten overdragen naar een andere organisatie of systeem.

7. **Verzoek tot toegang**
   - Het recht op inzage is uitgebreid met vereisten welke informatie moet worden verstrekt bij een inzageverzoek.
   - Denk hierbij aan bewaartermijnen, toegangsautorisatie en het recht om een klacht in te dienen bij de toezichthoudende autoriteit.
   - Dossiervorming vindt soms op meerdere niveaus plaats, waardoor er sprake kan zijn van toegangsautorisatie bij het inzien van privacygevoelige informatie.
   - Maak duidelijk afspraken over welke informatie op welk niveau gedeeld mag worden en met wie deze informatie gedeeld mag worden.
   - Denk goed na over de manier waarop er voldaan kan worden aan een inzageverzoek, zonder dat de privacy van personen verder wordt aangetast.
   - Een inzageverzoek kan alleen gedaan worden door een geïdentificeerd persoon, waarvan duidelijk is dat deze recht heeft op inzage of toegang tot de gegevens.

8. Grondslag of doelstelling van gegevensverwerking

- Organisaties moeten zich bewust zijn van de grondslag en de doelstelling van gegevensverwerking.
- Het gerechtvaardigd belang van gegevensverwerking moet door de organisatie helder en duidelijk worden omschreven.
- Welke gegevens hebben wij nodig bij de uitvoering van onze functie?
- Welke gegevens hebben wij nodig om personen zo goed mogelijk van dienst te kunnen zijn?
- Bij deze overweging is het goed te beseffen welke belangen er zijn voor de organisatie, maar ook alle betrokkenen binnen én buiten de organisatie (stakeholders e.d.).
- Is er sprake van een commercieel belang, een dienstverlenend belang of een noodzakelijk belang bij gegevensverwerking van privacygevoelige informatie?

9. Toestemming

- Toestemming voor gegevensverwerking van privacygevoelige informatie en persoonsgegevens moet voortaan expliciet worden gevraagd.
- De toestemming moet hierna kunnen worden aangetoond door vastlegging van welke toestemming precies is verleend (gebruik persoonsgegevens, publicatie foto's, e.d.).
- De toestemming moet door de persoon kunnen worden ingetrokken en persoonsgegevens moeten op eerste verzoek worden verwijderd.
- Het verwerken van bijzondere gegevens (ras, etnische afkomst, gezondheidsgegevens, etc.) is in beginsel verboden.
- Bijzondere gegevens mogen alleen worden verwerkt als dit noodzakelijk is voor de uitvoering van de overeenkomst, taak of functie.
- Het moet voor de persoon duidelijk zijn waarom deze bijzondere gegevens benodigd zijn (medisch specialist, vertrouwenspersoon, e.d.).

10. Kinderen

- Voor verwerking van privacygevoelige informatie of persoonsgegevens van kinderen is de uitdrukkelijke toestemming van ouders of wettelijke vertegenwoordigers nodig tot 16 jaar.
- Ga na of uw huidige systemen de leeftijd van het kind kunnen controleren en op welke wijze toestemming aan ouders of wettelijke vertegenwoordigers kan worden gevraagd.
- De organisatie heeft hierin een verantwoordingsplicht en moet de toestemming van ouders of wettelijke vertegenwoordigers vastleggen.
- Bij internetdiensten of toegang tot digitale systemen voor kinderen is deze toestemming lastig te realiseren, want kinderen zijn al jong digitaal vaardig.
- Het verdient daarom aanbeveling hierbij gebruik te maken van een disclaimer, privacy statement of toestemmingsverklaring.
- Geef duidelijk aan dat ouders of wettelijk vertegenwoordigers verantwoordelijk zijn voor het waarborgen van de privacy van het kind tot 16 jaar.

11.Datalek

- Controleer of u een sluitende procedure heeft bij een datalek.
- Wie is verantwoordelijk voor de opsporing van datalekken?
- Wie is verantwoordelijk voor het onderzoeken van het datalek?
- Wie is verantwoordelijk voor de interne melding en de externe melding?
- Wie is verantwoordelijk voor het informeren van betrokkenen?
- Hoe worden datalekken in de toekomst voorkomen?
- Welke procedures moeten worden herzien?

12.Gegevensbescherming (Privacy by Design / Privacy by Default)

- De organisatie is juridisch aansprakelijk voor het naleven van de AVG-privacy wetgeving, nu en in de toekomst.
- Beschrijf de processen die te maken hebben met de administratieve organisatie en interne beheersing van privacy risico's.
- Kijk daarbij kritisch naar de toegangsautorisatie, het niveau van informatiebeveiliging en de waarborging van de privacy van betrokkenen.
- Op beleidsmatig niveau verdient het aanbeveling vooraf te bepalen welke keuze(s) er worden gemaakt bij aanschaf, ontwerp op ontwikkeling van nieuwe systemen.
- Privacy by Design: we slaan alleen noodzakelijke privacygevoelige gegevens op en gaan zorgvuldig om met de persoonsgegevens van de gebruiker.
- Privacy by Default: we houden rekening met privacy vriendelijke instellingen en de gebruiker bepaalt zelf welke gegevens hij/zij aan ons wil geven.

13.Functionaris Gegevensbescherming (FG) / Data Protection Officer (DPO)

- Stel vast of uw organisatie een vertrouwenspersoon moet aanstellen, om toe te zien op naleving van de AVG-privacy wetgeving
- De AVG geeft voorwaarden aan voor de positie, het kennisniveau en de taak- en functieomschrijving van de (interne) vertrouwenspersoon FG of DPO.
- Een interne vertrouwenspersoon valt onder de klokkenluidersregeling. In sommige gevallen wordt daarom gekozen voor een externe vertrouwenspersoon.
- Dit vanwege de eventuele complicaties die kunnen optreden bij belangenverstrengeling en het kunnen waarborgen van transparantie en integriteit (compliance vereisten).

14.Toezichthoudende Autoriteit

- Bij de keuze voor de toezichthoudende autoriteit, moet rekening worden gehouden met de jurisdictie waaronder de organisatie valt, en het vestigingsadres van de (moeder)organisatie.
- Vooral bij grensoverschrijdende verwerkingen is het van belang te bepalen welke wet- en regelgeving van toepassing is.
- Valt de verwerking onder Nederlands recht, Europees Recht of Internationaal Recht?

15.Bestaande contracten

- De AVG stelt eisen aan de contractuele bepalingen in de overeenkomst tussen de organisatie, de verwerkingsverantwoordelijke en de verwerker.
- In een verwerkingsovereenkomst of privacyverklaring moet duidelijk worden aangegeven wie juridisch aansprakelijk en verantwoordelijk is.
- Het verdient aanbeveling bestaande contracten en overeenkomsten met leveranciers te reviewen op de AVG-privacy wetgeving.
- Sommige contracten en overeenkomsten hebben een bepaalde looptijd en kunnen daarom niet tussentijds worden opgezegd of beëindigd (extra kosten).
- Hierdoor kunnen aanvullende maatregelen nodig zijn om te kunnen voldoen aan de AVG (contractbespreking of kiezen voor een ander alternatief).

Voor vragen of advies?
Neem contact op met IDA Interim Development Advice
Dit kan via onze contactpagina of mail mij rechtstreeks

Bron: Autoriteit Persoonsgegevens

**Disclaimer*
Aan deze informatie kunnen geen rechten worden ontleend.
Wij adviseren een ICT-jurist te consulteren bij een dispuut of schending van uw privacy.
Desgewenst kunnen wij u doorverwijzen naar een juridisch specialist in ons netwerk.