ICTRECHT

Checklist

De Algemene verordening gegevensbescherming

Ter implementatie van de Algemene verordening gegevensbescherming (AVG) dient er binnen organisaties het een en ander te worden geregeld. Zo moet er grip worden gekregen op de omgang met persoonsgegevens, dient de awareness van medewerkers te worden verhoogd, behoren er diverse (beleids-) documenten te worden opgesteld en moeten er daarnaast diverse procedures worden ingericht. Hieronder volgt een vijfstappenplan van de hoofdpunten die een organisatie moet regelen om in lijn te handelen met de AVG.

Stap 1: Inventarisatie

Voor het implementeren van de AVG dient er een overzicht te worden verkregen van de huidige situatie met betrekking tot de omgang met persoonsgegevens. Hiervoor dient het volgende in kaart te worden gebracht:

Breng in kaart	Bijvoorbeeld	Check
Via welke wegen persoonsgegevens uw organisatie binnenkomen.	Website, cookies, klantopdracht of arbeidscontract.	○
Welke persoonsgegevens er precies worden verwerkt.	Naam, adres, contactgegevens, financiële gegevens of salarisgegevens.	○
Of er bijzondere persoonsgegevens worden verwerkt, en zo ja, welke?	Medische gegevens, gegevens over seksuele voorkeur of religie.	○
Van welke soort betrokkenen deze (bijzondere) persoonsgegevens afkomstig zijn.	Websitebezoekers, klanten of medewerkers.	○
Voor welke doeleinden deze gegevens worden gebruikt.	Het leveren van producten en diensten of uitbetalen van salaris.	○
Op basis van welke grondslagen er persoonsgegevens worden verwerkt.	Uitvoering van de overeenkomst of toestemming.	○
Waar en hoelang persoonsgegevens worden opgeslagen en waarom die termijn wordt gehanteerd.	CRM-systeem – tot zeven jaar na einde (koop)overeenkomst.	○
Aan wie en op welke wijze deze persoonsgegevens weer worden doorgegeven.	ICT-dienstverleners, salarisadministratiekantoor of andere entiteiten binnen de groep.	○
Hoe de persoonsgegevens zijn beveiligd.	Wachtwoorden, beveiligde verbindingen of encryptie.	○
In welke landen de persoonsgegevens worden verwerkt (en dus ook inzichtelijk zijn).	Nederland, Duitsland of de Verenigde Staten.	○

Stap 2: Beoordeling

Nadat er een overzicht is gemaakt van wat er met persoonsgegevens gebeurt, is het van belang om te beoordelen of dit in lijn is met de AVG. Met betrekking tot persoonsgegevens die jouw organisatie in haar rol als verwerkingsverantwoordelijke verwerkt, dienen de volgende vragen te worden gesteld en moet het antwoord worden beoordeeld:

Beoordeel	Toelichting	Check
Wat is ons doel en welke gegevens verzamelen wij hiervoor?	*Doelbinding:* persoonsgegevens mogen alleen worden gebruikt voor het doel waarvoor ze zijn verzameld, of een doel dat daar heel nauw mee samenhangt.	○
Hebben wij een rechtmatige grondslag voor de gegevens die wij verzamelen?	*Rechtmatige grondslag:* persoonsgegevens mogen alleen verwerkt worden daar een rechtmatige grondslag voor is.	○
Hebben wij betrokkenen adequaat over onze gegevensverwerking geïnformeerd via bijvoorbeeld een privacyverklaring?	*Informatieplicht:* alle betrokkenen dienen over de verwerking van hun persoonsgegevens te worden geïnformeerd. Hierbij moet ten minste informatie worden gegeven over het soort persoonsgegevens, de doeleinden, de grondslagen en de rechten van betrokkenen.	○
Verzamelen we enkel de gegevens die noodzakelijk zijn?	*Dataminimalisatie:* er mogen niet meer persoonsgegevens worden verwerkt dan nodig om de vastgestelde doelen te bereiken.	○
Kloppen de persoonsgegevens die wij verwerken nog wel, of zijn ze (mogelijk) verouderd?	*Juistheid:* persoonsgegevens moeten juist zijn en zo nodig worden geactualiseerd.	○
Bewaren wij persoonsgegevens enkel zo lang als nodig voor het doel waarvoor ze zijn verzameld en hebben wij daar beleid voor opgesteld?	*Opslagbeperking:* persoonsgegevens mogen niet langer worden bewaard dan nodig. Voor bepaalde gegevensverwerkingen volgt de bewaartermijn uit de wet (zoals de fiscale bewaarplicht van de Belastingdienst). Wanneer er geen bewaartermijn uit de wet volgt, moet je zelf een passende bewaartermijn vaststellen.	○
Hebben wij met alle partijen met wie we persoonsgegevens delen goede afspraken gemaakt over de omgang hiermee?	*Afspraken:* tussen verwerkingsverantwoordelijken en verwerkers, en tussen verwerkers en sub-verwerkers dient een (sub)verwerkersovereenkomst te worden gesloten. Tussen twee gezamenlijk verwerkingsverantwoordelijken een data-uitwisselingsovereenkomst.	○
Zijn er passende waarborgen getroffen wanneer persoonsgegevens buiten de Europese Economische Ruimte (EER) worden verwerkt?	*Doorgifte:* voor de verwerking van persoonsgegevens buiten de EER dienen passende waarborgen te worden getroffen.	○
Beveiligen wij persoonsgegevens op passende wijze?	*Adequate beveiliging:* er dienen passende technische en organisatorische maatregelen te worden genomen.	○
Kunnen wij persoonsgegevens op verzoek laten inzien, wijzigen, wissen, de verwerking beperken en overdragen en bieden wij betrokkenen de mogelijkheid om bezwaar te maken?	*Rechten van betrokkenen:* betrokkenen hebben verschillende rechten onder de AVG. Hoofdregel is dat aan een verzoek hiertoe binnen één maand moet worden voldaan.	○

Beoordeel	Toelichting	Check
Leven wij de principes *privacy by design* en *privacy by default* na?	*Privacy by design:* bij het ontwerp of bij de inkoop van systemen wordt nagedacht over het naleven van de privacyregels. *Privacy by default:* standaardinstellingen zijn privacyvriendelijk ingesteld.	○
Kunnen we de naleving van alle bovengenoemde punten aantonen?	*Verantwoordingsplicht:* jouw organisatie dient aan te kunnen tonen dat zij aan de AVG voldoet, o.a. via haar verwerkingsregister en de bij stap drie genoemde documenten.	○
Hebben wij een intern aanspreekpunt (*privacy officer*) aangewezen voor de naleving van de AVG, of een (verplichte) Functionaris Gegevensbescherming (FG)?	*Aanspreekpunt:* intern dient duidelijk te zijn wie voor de naleving van de AVG zal zorgdragen (de zogenoemde *privacy officer(s)*). Daarnaast is het voor sommige organisaties verplicht om een FG aan te stellen.	○

Stap 3: Documentatie

Om te kunnen voldoen aan de AVG, en aan te kunnen tonen dat uw organisatie hier inderdaad aan voldoet, dienen de volgende documenten te worden opgesteld:

Op te stellen document	Wat is het?	Check
Verwerkingsregister	Een overzicht van alle gegevensverwerkingen binnen de organisatie. Er moet een verwerkingsregister worden opgesteld en bijgehouden voor gegevensverwerkingen waar jouw organisatie verwerkingsverantwoordelijke en/of verwerker is.	○
Datalekkenregister	Een overzicht van alle datalekken die binnen jouw organisatie hebben plaatsgevonden.	○
Verwerkersovereenkomst(en) en een overzicht van alle gesloten/nog te sluiten verwerkersovereenkomsten	Schriftelijke afspraken tussen de verwerkings-verantwoordelijke en de verwerker, en tussen de verwerker en een subverwerker over de zorgvuldige omgang met persoonsgegevens. De AVG schrijft een aantal verplichte onderwerpen voor, die in de verwerkersovereenkomst terug moeten komen.	○
Data- uitwisselingsovereenkomst	Schriftelijke afspraken tussen twee (gezamenlijk) verwerkingsverantwoordelijken die gegevens uitwisselen, over onder andere de omgang met de rechten van betrokkenen en de informatieplicht.	○
Beveiligingsbeleid	Een overzicht van de genomen passende technische en organisatorische beveiligingsmaatregelen en een overzicht van de beveiligingsmaatregelen die medewerkers dienen op te volgen (zoals bijvoorbeeld een wachtwoordbeleid).	○
Beleid inzake bewaartermijnen	Een beleidsstuk waarin de bewaartermijnen voor de verschillende soorten persoonsgegevens staan opgesomd.	○
Privacybeleid	Een beleidsstuk over de wijze waarop medewerkers met persoonsgegevens moeten omgaan. Zoals wat ze moeten doen als een betrokkene zijn/haar rechten wil uitoefenen, of wat ze moeten doen alvorens een nieuw IT-systeem wordt aangeschaft.	○
Interne privacyverklaring	Een document waarin is uitgelegd welke persoons-gegevens een werkgever van haar werknemers verwerkt, en wat daar vervolgens mee gebeurt.	○

Op te stellen document	Wat is het?	Check
Privacy- (en cookie)verklaring (extern)	Een document waarin een organisatie richting alle externe betrokkenen, zoals klanten en websitebezoekers uitlegt welke persoonsgegevens worden verwerkt en wat daar vervolgens mee gebeurt. Vaak wordt ervoor gekozen om de informatie voor alle externen in één privacy- (en cookie)verklaring op de website van de organisatie te plaatsen.	○
Calamiteitenplan datalekken	Een document met informatie over datalekken en over de interne procedure bij datalekken. Het doel van dit document is om ervoor te zorgen dat medewerkers weten wat een datalek is, dat datalekken intern bij de juiste persoon uitkomen en dat iedereen weet wat zijn/haar rol is bij een datalek.	○

Stap 4: Procedures

Niet alleen is het nodig om te weten wat jouw organisatie met persoonsgegevens doet en om de juiste documenten op orde te hebben, ook tijdens de dagelijkse werkzaamheden moet aan de AVG worden voldaan. De volgende fase is daarom: het inrichten van de procedures. Zo zorg je ervoor dat opgestelde beleidsstukken ook daadwerkelijk worden opgevolgd.

In te richten procedures	Waarom?	Check
Kennisdeling	Het is belangrijk dat medewerkers weten wat privacy is, wanneer sprake is van de verwerking van persoonsgegevens en waarom het belangrijk is om aan de regels uit de AVG te voldoen. Zorg dat de kennis up-to-date blijft en dat elke nieuwe werknemer wordt geïnstrueerd over beleid inzake privacy. Waarborg daarnaast dat werknemers vooral hun dagelijkse werkzaamheden kunnen blijven uitvoeren. Het te veel en onnodig hinderen van werknemers in hun dagelijkse werk voor privacy doeleinden kan ervoor zorgen dat medewerkers er net omheen gaan werken.	○
Inschakelen derde partijen	Wanneer een derde partij wordt ingeschakeld, zoals een ICT-dienstverlener, moet worden beoordeeld of deze partij persoonsgegevens voor jouw organisatie verwerkt. Indien dat het geval is, moeten schriftelijke afspraken worden gemaakt met deze partij over de omgang met persoonsgegevens. Intern dient duidelijk te zijn wie dit moet regelen en hoe ervoor wordt gezorgd dat deze persoon op tijd wordt betrokken.	○
Wijze van inrichting nieuwe gegevensverwerkingen	Als er een nieuwe gegevensverwerking wordt opgestart (bijvoorbeeld het versturen van een nieuwsbrief) moet deze nieuwe verwerking weer in lijn met de AVG worden ingericht. Het verwerkingsregister en de privacyverklaring dienen aangevuld te worden, en wanneer het software betreft moet het volgens de principes van privacy by design en default worden ingericht. De privacy officer/FG dient op tijd bij nieuwe verwerkingen te worden betrokken.	○

In te richten procedures	Waarom?	Check
Uitvoering geven aan rechten van betrokkenen	Op een verzoek van een betrokkene moet binnen een korte periode worden gereageerd. Het verzoek dient in principe binnen uiterlijk één maand te worden opgelost. Daarom dient intern een procedure te worden ingericht zodat duidelijk is wie de verzoeken van betrokkenen beoordeelt, hoe de verzoeken naar deze persoon moeten worden doorgezet en hoe deze persoon deze moet afhandelen.	○
Communicatie rondom datalekken	Het calamiteitenplan datalekken moet ook in de praktijk functioneren. Duidelijk moet zijn dat het plan er is, dat iedereen begrijpt wanneer er sprake is van een (mogelijk) datalek en dat de benodigde medewerkers goed bereikbaar zijn.	○
Beoordeling noodzaak DPIA	Voor risicovolle verwerkingen is een Data Protection Impact Assessment (DPIA) vereist. Beslis wie beoordeelt of er een DPIA moet worden uitgevoerd, wie dit uiteindelijk moet gaan doen en zorg ervoor dat de beoordelaar op tijd wordt geïnformeerd.	○
Up-to-date houden van de documenten	Een organisatie staat nooit stil en dus zullen de privacydocumenten ook regelmatig moeten worden aangepast. Zorg ervoor dat hiervoor verantwoordelijke personen worden aangewezen en dat procedures op zijn plek zijn zodat deze personen (en/of de privacy officer of FG) tijdig worden geïnformeerd.	○

Stap 5: Awareness en controle

Als de organisatie in lijn is gebracht met de AVG is het noodzaak dat ook de medewerkers weten wat zij moeten doen om te zorgen dat dit zo blijft en waar nodig hun werkwijze aan te passen. Het is van belang om kennis over privacy in de gehele organisatie te verspreiden en de kennis, documenten, procedures en beveiliging regelmatig te (laten) controleren en waar nodig bij te stellen. De AVG is niet iets dat eenmalig wordt geïmplementeerd, het is een doorlopend proces dat continu moet worden bijgehouden en waar nodig moet worden aangevuld.

Dit laatste benadrukt het belang van het aanwijzen van interne verantwoordelijke stakeholders (privacy officers) en/ of een FG. Zodra jouw organisatie verandert, of er nieuwe activiteiten worden ondernomen, zullen ook de AVG-documenten moeten worden aangepast/aangevuld. Daarnaast zal er bij (nieuwe) activiteiten of ontwikkelingen mogelijk actie moeten worden ondernomen, zoals bijvoorbeeld het sluiten van een verwerkersovereenkomst of het uitvoeren van een DPIA.