FLINN

Avocats ▪ Advocaten

IS UW ONDERNEMING GDPR-CONFORM? – EEN INLEIDENDE VRAGENLIJST (*)

☐ De Commissie voor de Bescherming van de persoonlijke levenssfeer (op 25.05.2018 wijzigt de naam naar Gegevenbeschermingsautoriteit) raadt alle Verwerkingsverantwoordelijken en Verwerkers aan om een register van hun verwerkingsactiviteiten bij te houden – zelfs al zijn ze hiertoe niet verplicht volgens art. 30 GDPR.

☐ Het is hierbij nodig dat u een beeld vormt van de gegevensstromen binnen uw onderneming. Stel uzelf de vraag – voor welk(e) doel(en) worden persoonsgegevens opgevraagd, gebruikt en bijgehouden? Met wie worden ze gedeeld? Er kunnen eventueel verschillende einddoelen zijn – analyseer hierbij elk doel afzonderlijk.

☐ **OVERZICHT VAN DE VERWERKING – Analyseer de gegevens waarover u beschikt**

- **Waarom** worden er persoonsgegevens verwerkt? (bijv. personeelsadministratie, wettelijke verplichtingen, levering van goederen of diensten, marketing, profilering…)

- Van **wie** worden persoonsgegevens verwerkt? (bijv. personeel, klanten, zakelijke contacten, leveranciers, kinderen… Bron van de gegevens: de betrokkenen zelf, een externe bron…)

- **Welke** persoonsgegevens worden verwerkt? (bijv. persoonlijke details zoals naam, adres, e-mail, IP-adres, telefoon, geboortedatum, rijksregisternummer…; financiële details zoals nummer van de bankrekening of kredietkaart; arbeidsgegevens; speciale categorieën van gegevens zoals gezondheid, biometrische gegevens, strafblad…)

- **Wanneer** worden er persoonsgegevens verwerkt? ("Verwerken" betekent onder meer het verkrijgen, openbaar maken, opslaan, verwijderen… Wanneer worden ze verkregen? Aan wie worden ze meegedeeld en waarom? Hoe lang worden ze bijgehouden?)

- **Waar** worden de persoonsgegevens verwerkt? (bijv. elektronische opslag – gebeurt dit intern of wordt het extern uitbesteed? Staan de servers in de EER, USA of ergens anders? Cloud – waar staan de servers? Manuele opslag – locatie?)

☐ **VERWERKINGEN BINNEN DE ONDERNEMING**

- Hebt u uw personeel opgeleid in verband met de bescherming van persoonsgegevens (DP)? Wie is de verantwoordelijke voor de DP? Hebt u enige richtlijnen/verklaringen omtrent DP opgesteld, zowel intern (werknemers) als extern (cliënten, klanten, leveranciers)? Wanneer werden deze het laatst herzien? Welke DP/Cookies verklaringen staan er op uw website?

☐ **DERDEN**

- Bent u een Verwerkingsverantwoordelijke, werkt u samen met een externe Verwerker? Hebt u een kopie van de contracten? Hebt u deze herzien in het kader van GDPR-verplichtingen zoals veiligheid, integriteit en vertrouwelijkheid?

☐ **TRANSPARANTIE**

- Hebt u de informatie die u verstrekt aan betrokkenen bijgewerkt in een duidelijke taal en heeft u hierbij rekening gehouden met de informatie die gevraagd wordt in de artikelen 13 en 14 GDPR?

☐ **RISICO-INSCHATTING**

- Beschikt u over een systeem dat uw gegevensbeheersysteem controleert en de veiligheid en bescherming tegen zowel interne als externe aanvallen inschat?

☐ **PARAATHEID**

- Bestaat er een interne procedure voor het beoordelen en bijhouden (en de rapportering ervan indien nodig) van enige inbreuken in verband met de persoonsgegevens?

☐ **INTERNATIONAAL**

- Indien u persoonsgegevens overdraagt over de grenzen van de EER heen; heeft u geverifieerd op welke juridische basis u dergelijke doorgiften uitvoert?