Tips voor een goed opgestelde Privacy verklaring

De GDPR vereist immers dat je openheid hanteert naar alle betrokkenen, met andere woorden naar alle personen van wie je gegevens gebruikt. Het is hun recht op de hoogte te zijn van de verwerkingen die er met hun gegevens gebeuren. Een tekst waarin je als organisatie deze informatie publiek maakt, noemen we een 'Privacy verklaring'.

De GDPR legt vast welke informatie de betrokkene moet krijgen. Een goed opgestelde Privacy verklaring moet dus elk van deze items behandelen.

- De **verantwoordelijke voor de gegevensverwerking** moet zichzelf duidelijk kenbaar maken, met de exacte naam van de firma of de organisatie en met het volledige adres van de zetel. Als de organisatie een Data Protection Officer (DPO) heeft aangesteld, moet de Privacy verklaring ook vermelden hoe deze gecontacteerd kan worden. Het is niet nodig de naam van deze persoon te geven, maar wel minstens een adres, telefoonnummer of mailadres waarmee hij kan bereikt worden. Als er geen DPO is, moet evenzeer verwezen worden naar een contactpunt.
- Het belangrijkste deel van de verklaring is **de opsomming van de verwerkingen** van persoonsgegevens die je organisatie doet. Dit moet voldoende in detail gebeuren, apart per doelstelling. Je geeft telkens aan met welke **bedoeling** bepaalde gegevens verzameld worden, welke **categorieën** van gegevens je verwerkt en over welke categorieën van personen het gaat, welke **verwerkingen** er gebeuren en op welke **rechtsgrond** je je beroept om de verwerking te kunnen doen. Hiervoor kun je uiteraard putten uit het interne register, zodat je niets vergeet.
- Er moet ook duidelijkheid zijn over de **bestemmelingen**. Wie heeft toegang tot deze informatie? Aan wie wordt ze doorgegeven? Geef aan welke categorieën medewerkers intern bij de verwerking betrokken zijn en dus inzage kunnen hebben in de informatie. Vermeld of er externe partijen aan de verwerking deelnemen. Als de verzamelde informatie voor verder gebruik doorgegeven wordt aan derden, moet je dit zeker expliciet aangeven. Meestal gebeurt dit in algemene bewoordingen als 'zustermaatschappijen' of 'partners'. De GDPR gaat uit van zoveel mogelijk transparantie. Het is immers belangrijk dat de betrokkenen begrijpen waar hun gegevens terechtkomen. Uiteraard kan men niet verwachten dat je elke partner of leverancier met naam en toenaam opsomt.
- Vervolgens toon je aan dat er **voldoende beveiligingsmaatregelen** genomen zijn om de vertrouwelijkheid en integriteit van de data te verzekeren. Ook hier is het niet nodig alle technologie en procedures in detail uit de doeken te doen. Dat zou natuurlijk juist de beveiliging ondergraven. Maar de gevolgde principes en de manier waarop je deze intern kunt waarborgen, vermeld je best wel.
- Een specifieke vereiste is informatie over **de bewaartermijn van gegevens**. De GDPR zegt immers dat je persoonsgegevens enkel voor het gestelde doel mag gebruiken en dus ook niet langer mag bewaren dan nodig is voor dat doel. Bovendien moet je als verantwoordelijke instaan voor de kwaliteit van de gegevens. Dat houdt ook in dat ze niet verouderd zijn. Info over de bewaartijd vermeld je best specifiek per doel.
- Verder moet de Privacy verklaring ook de **rechten van de betrokkene** duidelijk opsommen.
    - Hij kan altijd een klacht indienen bij de Privacy Commissie als hij van oordeel is dat gegevens onrechtmatig verwerkt worden.

- Hij kan bij de verantwoordelijke informatie opvragen over de verwerkingen van zijn gegevens en je moet hem uitleggen welke procedure hij daarvoor kan volgen.
- Hij kan inzage krijgen in de beschikbare informatie en deze desgewenst laten wijzigen of wissen.