

Privacy Checklist.

Persoonsgegevens verwerken brengt verantwoordelijkheden met zich mee. Met deze Privacy Checklist krijg je snel inzicht in de belangrijkste aandachtspunten voor jouw organisatie. Ontdek waar je rekening mee moet houden en zorg ervoor dat je privacybeleid aansluit op de geldende vereisten.

Persoonsgegevens

JA NEE

- ☐ ☐ Weten we welke persoonsgegevens wij verwerken?
- ☐ ☐ Verwerken we bijzondere categorieën persoonsgegevens (zoals gezondheid, religie of biometrie), of strafrechtelijke gegevens?
- ☐ ☐ Beschikken we over een geldige grondslag voor de verwerking van deze persoonsgegevens en (bij bijzondere gegevens) een wettelijke uitzondering?
- ☐ ☐ Hebben betrokkenen toestemming gegeven wanneer dat nodig is? En kan deze net zo makkelijk worden ingetrokken?
- ☐ ☐ Is het doel van de verwerking duidelijk bepaald? En als we de persoonsgegevens verder verwerken, is het nieuwe doeleinde dan verenigbaar?
- ☐ ☐ Kan de verwerking met minder inbreuk op de privacy plaatsvinden? En staat ons doel in verhouding tot de privacyinbreuk?
- ☐ ☐ Weten we hoe lang we persoonsgegevens (mogen) bewaren en vernietigen we deze ook daadwerkelijk op tijd?
- ☐ ☐ Delen we persoonsgegevens met derde partijen (ook buiten de Europese Economische Ruimte)? Weten we of dat mag, bijvoorbeeld dankzij een adequaatheidsbesluit of SCC's?

Organisatie

JA NEE

- ☐ ☐ Zijn de interne rollen, taken en verantwoordelijkheden duidelijk vastgelegd?
- ☐ ☐ Zijn wij verplicht een FG aan te stellen? Is deze onafhankelijk gepositioneerd? Is de FG aangemeld bij de toezichthouder?
- ☐ ☐ Hebben we een privacybeleid en -procedures?
- ☐ ☐ Krijgen medewerkers genoeg ondersteuning bij privacyvraagstukken?
- ☐ ☐ Zijn medewerkers voldoende getraind? Zijn medewerkers bekend met privacybeleid en -procedures?
- ☐ ☐ Hebben we een duidelijk proces voor het omgaan met datalekken? Melden we datalekken op tijd bij de toezichthouder?
- ☐ ☐ Hebben we een proces voor het uitoefenen van rechten van betrokkenen ingericht? Denk aan: inzage, rectificatie, verwijdering, beperking, bezwaar en het recht om niet te worden onderworpen aan geautomatiseerde besluitvorming en profilering.
- ☐ ☐ Behandelen we verzoeken op tijd (binnen een maand) en inhoudelijk voldoende? Verifiëren we de identiteit van de verzoeker voordat we gegevens verstrekken?

Beheer

JA NEE

- ☐ ☐ Kunnen we aantonen dat we voldoen aan de AVG? Denk aan alle onderwerpen op deze checklist.
- ☐ ☐ Hebben we zicht op de risico's voor betrokkenen en leggen we die analyse vast, bijvoorbeeld met een pre-DPIA?
- ☐ ☐ Hebben we een DPIA uitgevoerd voor verwerkingen met een hoog risico voor betrokkenen?
- ☐ ☐ Hebben we een verwerkingsregister en is dat up-to-date?
- ☐ ☐ Beveiligen we de persoonsgegevens voldoende? En hebben we een informatiebeveiligingsbeleid?
- ☐ ☐ Houden we rekening met privacyafwegingen bij het ontwerpen van nieuwe diensten en producten (privacy by design en by default)?
- ☐ ☐ Hebben we verwerkersovereenkomsten gesloten met leveranciers? Zijn deze actueel en volledig?

Communicatie

JA NEE

- ☐ ☐ Hebben we een privacyverklaring voor de website, voor sollicitanten en voor werknemers?
- ☐ ☐ Informeren we betrokkenen op tijd over de verwerking van hun persoonsgegevens en verstrekken we alle verplichte informatie?
- ☐ ☐ Hebben we informatie over privacy in ons jaarverslag opgenomen?
- ☐ ☐ Weten we hoe we moeten communiceren met de toezichthouder, de media of betrokkenen over hoe we omgaan met persoonsgegevens, bijvoorbeeld bij een datalek?

Heb je vragen over de begrippen, vereisten of grondslagen die in deze checklist aan bod komen?
Neem dan vrijblijvend contact met ons op via info@privacycompany.nl

Ben je al bekend met onze Privacy Management software?

PRIVACYNEXUS  Vraag een gratis demo aan

PRIVACYCOMPANY 

WIJ WERKEN SAMEN MET **PURASEC**

BC **ISO 27001:2022**
Certified by
Brand Compliance



Dit werk valt onder een
Creative Commons-licentie
CC BY-ND 4.0

