

Houd bij het verwerken van persoonsgegevens vanaf het begin rekening met privacy. We hebben per onderwerp acht formulieren toegevoegd zodat je aan kunt tonen welke maatregelen je getroffen hebt. Het is sterk aangeraden om een privacy en security professional erbij te betrekken.

Uitgangspunt is altijd: anonimiseren en aggregeren!

Zorg dat de gegevens niet herleidbaar, koppelbaar en deduceerbaar zijn. Als het goed gebeurt en het is onomkeerbaar dan zijn geen extra maatregelen nodig, er zijn namelijk geen persoonsgegevens meer aanwezig. Je kunt dan stoppen met het framework.

Als je niet anonimiseert en er is sprake van grondslag en doelbinding volg dan onderstaand Privacy by Design framework.

1

Dataminimalisatie

Alleen strikt noodzakelijke gegevens verzamelen of overbodige direct verwijderen, (web) invulformulieren aanpassen

Waar mogelijk deel van de gegevens anonimiseren /aggregeren

art. 5 lid 1 sub c AVG

2

Pseudonimiseren

Vervangen van direct identificerende kenmerken door een pseudoniem.

art. 4 lid 5 AVG

3

Bescherming

Toegangsbeheer, fysieke toegangscontrole, logische toegangscontrole, authenticatie en autorisatie. Afdwingen sterke wachtwoorden. Bijhouden autorisatiematrix en logging. Houd principie van need to know als uitgangspunt (art. 32 lid 1, art. 5 lid 1 sub f AVG).

Encryptie (versleuteling)
Gegevens of apparaten beveiligen door ze onleesbaar te maken voor onbevoegden (TLS, HTTPS, AES) (art. 6 lid 4 sub e, art. 32 lid 1 sub a AVG).

Scheid de verwerking van persoonsgegevens zo veel mogelijk van elkaar.

4

Standaardinstelling (privacy by default)

Stel je standaardinstellingen privacy vriendelijk in.

art. 25 lid 2 AVG

5

Verwijderen en bewaartermijn

Zorg ervoor dat je een bewaartermijn vaststelt en dat die gegevens daadwerkelijk worden verwijderd.

Richt daarom je system zo in dat gegevens daadwerkelijk kunnen worden verwijderd en waar mogelijk op een geautomatiseerde wijze.

art. 5 lid 1 sub e AVG

6

Rechten van betrokkenen

Faciliteer de volgende rechten van betrokkenen:

- Informeer over de verwerking
- Inzage
- Correctie
- Vergetelheid (verwijderen)
- Beperking van de verwerking
- Dataportabiliteit
- Bezwaar
- Recht om niet te worden onderworpen aan geautomatiseerde individuele besluitvorming/profiling

art. 12 t/m 22 AVG

ANONIMISEREN

Wat heb je gedaan om de persoonsgegevens te anonimiseren?

Hoe heb je dat gedaan

DATAMINIMALISATIE ART. 5 LID 1 SUB C AVG

Wat heb je gedaan op het gebied van dataminimalisatie?

Hoe heb je dat gedaan

PSEUDONIMISEREN ART. 4 LID 5 AVG

Wat heb je gedaan om de gegevens te pseudonimiseren?

Hoe heb je dat gedaan

BESCHERMING ART. 32 AVG

Wat heb je gedaan aan de bescherming van persoonsgegevens?

Hoe heb je dat gedaan

STANADAARDINSTELLING (PRIVACY BY DEFAULT) ART. 25 LID 2 AVG

Wat heb je gedaan met de standaardinstelling?

Hoe heb je dat gedaan

VERWIJDEREN EN BEWAARTERMIJN ART. 5 LID 1 SUB E AVG

Wat heb je gedaan met de verwijdering en bewaartermijn van persoonsgegevens?

Hoe heb je dat gedaan

RECHTEN VAN BETROKKENEN ART. 12 T/M 22 AVG

Wat heb je gedaan om de rechten van betrokkenen te kunnen faciliteren?

Hoe heb je dat gedaan