Privacy by Design Framework

Governance:
Omvat algemene privacy awareness binnen organisatie, intern beleid, beleggen van verantwoordelijkheden, transparantie naar betrokkenen, samenwerking met derde partijen en bewerkers (incl. contracten, bewerkersovereenkomsten)

Onderdeel / Invulling	**Anonimiseren**	**1. Dataminimalisatie** (art. 5 lid 1 sub c)	**2. Pseudonimiseren** (art. 4 lid 5)	**3. Encryptie** (art. 6 lid 4 sub e, art. 32 lid 1 sub a)	**4. Access control** (art. 32 lid 1, art. 5 lid 1 sub f)	**5. Data protection by default** (art. 25 lid 2)	**6. Verwijderen / bewaartermijnen** (art. 5 lid 1 sub e)	**7. Faciliteren rechten van betrokkenen** (artt. 12 t/m 22)
Techniek	Anonimiseren en aggregeren (bijv. differential privacy)	Alleen strikt noodzakelijke gegevens verzamelen of overbodig direct verwijderen, (web) invulformulieren aanpassen	Ontdoen van direct identificerende kenmerken, hashing, polymorfe pseudo-id	Bijvoorbeeld public key encryptie, disk encryptie	Digitale gegevenskluis, fysieke toegangscontrole, logische toegangscontrole, authenticatie en autorisatie	Privacyvriendelijke settings als uitgangspunt, transparante user-interface, permission management	Automatisch vernietigen, 'flaggen' data na verstrijken bewaartermijn, sticky policies, data fading	Privacy dashboard, communicatie / support (art. 5 lid 1 sub a)
Onderliggende documentatie	Geen extra maatregelen nodig, want geen persoons-gegevens	Doelomschrijving met opsomming noodzakelijke gegevens	Beleid voor gescheiden houden van identificerende gegevens en overige gegevens, contracten	Informatie-beveiliging standaarden (art. 32 lid 1)	Bijhouden autorisatiematrix en logging, op basis van *need to know* en *need to access*	Registraties opt-in en opt-out en van permissies	Beleid en overzicht bewaartermijnen, omgang met e-waste (oude documenten en devices)	Privacy statement, beleid bij verzoeken tot inzage/correctie/ verwijderen gegevens
Alternatief	Als je niet anonimiseert: het schema volgen	Waar mogelijk deel gegevensset anonimiseren/ aggregeren, data fading	Andere beveiligings-maatregelen	Andere beveiligings-maatregelen (bijv. stand-alone server)	Access logs met controle achteraf	Geen alternatief, gewoon doen, is verplicht	Anonimiseren en aggregeren, (archiveren indien wettelijk toegestaan)	Geen alternatief, wettelijke plicht

Privacy Audit

Een privacy impact assessment kan de onderdelen toetsen en helpt inzichtelijk maken wat nodig is

De verwijzingen naar artikelen betreffen de artikelen uit de Algemene Verordening Gegevensbescherming (Verordening 2016/679 (AVG))

Mede mogelijk gemaakt door het SIDN Fonds.

www.privacycompany.eu

Privacy by Design Framework

Waarom dit framework?

In de *Algemene Verordening Gegevensbescherming* wordt *Privacy by Design* expliciet vereist bij het verwerken van persoonsgegevens. *Privacy by Design* betekent dat organisaties bij de ontwikkeling van (nieuwe) producten en diensten zo vroeg mogelijk aandacht besteden aan het beschermen van persoonsgegevens. Door privacybeschermende maatregelen aan het begin mee te nemen in de ontwikkeling is men eerder compliant met privacyregelgeving en worden kosten bespaard doordat deze maatregelen niet later alsnog moeten worden genomen. *Het is onduidelijk wanneer is voldaan aan het vereiste van Privacy by Design.*

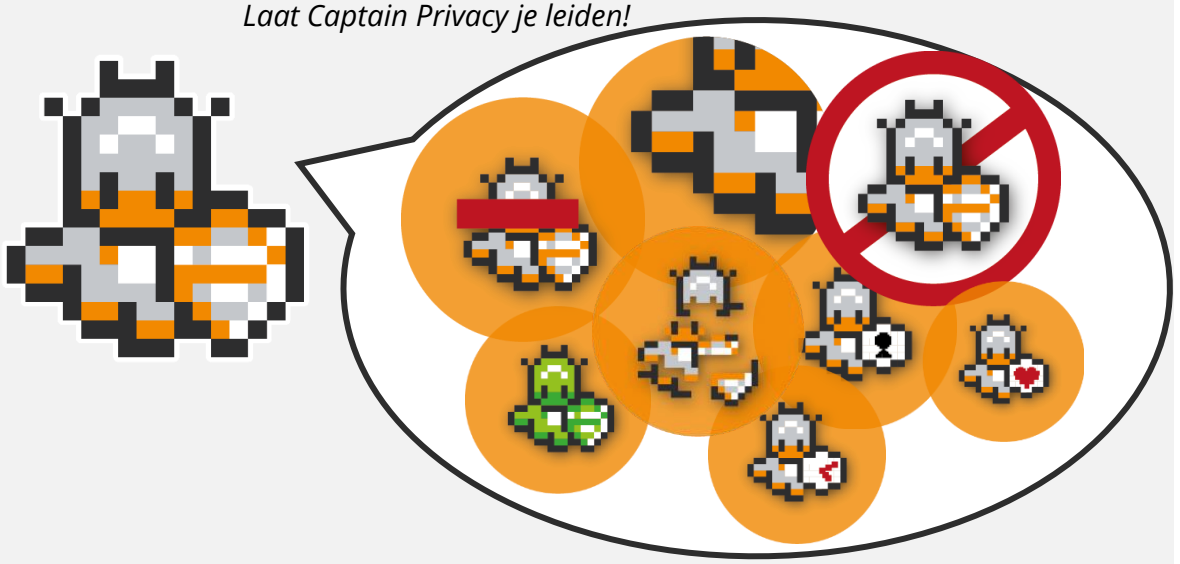
Hoe gebruik je dit framework?

Dit framework geeft invulling aan *Privacy by Design* op basis van vereisten die door de *Algemene Verordening Gegevensbescherming* verspreid zijn opgenomen.

Indien mogelijk kun je werken met anonieme gegevens. Als dat niet mogelijk is doorloop je de overige kolommen. Steeds is er een technische component met ondersteunende documentatie of organisatorische maatregelen. Door het schema te doorlopen en te registreren welke aspecten zijn meegenomen ontstaat een overzicht van de manier waarop jouw organisatie aan *Privacy by Design* voldoet.

Omdat mogelijk niet altijd alle aspecten technisch ingevuld kunnen worden is ook gekeken naar alternatieve waarborgen.

Laat Captain Privacy je leiden!



Maak het onderdeel van je organisatie

Het framework kan binnen een organisatie gebruikt worden als onderdeel van de algehele privacy governance. Om te borgen dat de organisatie compliant blijft bevelen wij je aan regelmatig een privacy audit uit te voeren aan de hand van het framework. Daarnaast kan een privacy impact assessment helpen inzichtelijk maken welke maatregelen vereist zijn bij het ontwerpen van een nieuwe dienst of gegevensverwerking.