

CHECKLIST

Privacy by Design voor productteams

Gebruik deze checklist om privacy en security vanaf discovery tot beheer mee te nemen in concrete productkeuzes. Bespreek open punten met de verantwoordelijke specialisten; de checklist vervangt geen formele DPIA, audit of juridische beoordeling.

Product / feature

Product owner

Datum

FASE 01 Discovery & scope

- ☐ 01 Is het beoogde gebruik helder, inclusief gebruikers, processen en de waarde die het product moet leveren?
- ☐ 02 Is duidelijk welke privacy- of juridische beoordeling door de verantwoordelijke specialist nodig is?
- ☐ 03 Zijn betrokkenen en mogelijke gevolgen van het gebruik in beeld gebracht?
- ☐ 04 Is expliciet onderscheid gemaakt tussen noodzakelijke informatie en nice-to-have gegevens?

Open punt, notitie of besluit

FASE 02 Gegevens & ontwerp

- ☐ 05 Is per gebruiksdoel het minimaal noodzakelijke gegevenspakket bepaald?
- ☐ 06 Zijn bewaartermijnen, verwijdering en relevante uitzonderingen meegenomen in het ontwerp?
- ☐ 07 Zijn rollen en toegangsrechten gekoppeld aan werkzaamheden en minimaal noodzakelijke toegang?
- ☐ 08 Zijn exports, koppelingen, back-ups en andere gegevenskopieën onderdeel van dezelfde ontwerpkeuzes?

Open punt, notitie of besluit

FASE 03 Development & integraties

- ☐ 09 Zijn privacy- en securityeisen opgenomen in backlog, ontwerp en acceptatiecriteria?
- ☐ 10 Worden in ontwikkel- en testomgevingen bij voorkeur synthetische of geminimaliseerde gegevens gebruikt?
- ☐ 11 Zijn koppelingen ingericht met passende authenticatie, autorisatie en gegevensbeperking?
- ☐ 12 Ondersteunen logging en monitoring aantoonbare controle zonder onnodig extra persoonsgegevens te verzamelen?

Open punt, notitie of besluit

CHECKLIST

Van ontwerp naar aantoonbaar beheer

Privacy by Design | Fasen 4 tot en met 6

FASE 04 Test & acceptatie

- ☐ 13 Zijn toegestane én verboden autorisatiescenario's aantoonbaar getest?
- ☐ 14 Zijn bewaartermijnen, verwijdering, export en andere kritieke gegevensfuncties getest?
- ☐ 15 Zijn relevante fout-, uitval- en incidentscenario's beoordeeld of getest?
- ☐ 16 Is acceptatiebewijs opgeslagen en is duidelijk welke bevindingen livegang blokkeren?

Open punt, notitie of besluit

FASE 05 Livegang

- ☐ 17 Zijn benodigde privacy-informatie, gebruikersinstructies en procesbeschrijvingen bijgewerkt?
- ☐ 18 Zijn relevante leveranciers- en verwerkingsafspraken afgerond voordat productie start?
- ☐ 19 Zijn resterende relevante risico's benoemd en door de juiste eigenaar geaccepteerd?
- ☐ 20 Zijn beheer, support, incidentroute en verantwoordelijkheden klaar voor gebruik?

Open punt, notitie of besluit

FASE 06 Beheer & wijziging

- ☐ 21 Zijn periodieke toegangsreviews en andere terugkerende controles ingepland en belegd?
- ☐ 22 Leiden nieuwe functionaliteit, koppelingen, doelen of incidenten tot herbeoordeling waar nodig?
- ☐ 23 Hebben bevindingen en incidenten een eigenaar, herstelactie en hertoetsmoment?
- ☐ 24 Wordt periodiek beoordeeld of maatregelen nog passend zijn en aantoonbaar blijven werken?

Open punt, notitie of besluit

Eerste vervolgactie

Actie en beoogd resultaat

Eigenaar

Afgesproken datum