Workshop “Privacy by Design door architecten”

Inleiding:

Bijna elke architect komt in zijn werk vraagstukken tegen die raken aan Privacy. Met de implementatie van de Avg neemt dat alleen maar toe en hoort Privacy by Design (PbD) in de gereedschapskist van iedere architect. Dat is snel gezegd, maar hoe ga je het borgen van Privacy inbouwen in je architectuur, hoe neem je dat aspect mee in de complexiteit waar we vaak middenin zitten? Waar begin je dan?

Doelgroep*: architecten en collega’s uit de publieke sector die actief moeten zijn met privacy / PbD*

Doelstelling van de workshop:
De doelstelling van de workshop is tweeledig:

1. Het delen van ervaring en kennis met de deelnemende architecten over hoe architecten de Avg wetgeving mee nemen in hun architectuurbeschrijvingen.

2. Het in kaart brengen kennisbehoefte voor de doorontwikkeling thema Privacy in de NORA.

We willen daarvoor graag weten welke architectuurprincipes jullie toepassen om te voldoen aan de Avg / te komen tot PbD en wat jullie ervaring daarbij is. Mogelijk kunnen de privacy criteria uit de Privacy Baseline van CIP (Centrum voor Informatiebeveiliging en Privacybescherming) helpen om als architect sturing te geven aan PbD .

Door jullie kennis en ervaring te delen kan de kennis worden meegenomen in een NORA-thema Privacy.

De case

Je bent lead-architect en in die rol verantwoordelijk voor één of meerdere verwerkingen van persoons-gegevens. Je heeft hierbij steeds aandacht gehad voor de belangen van de organisatie. De organisatie maakt zich echter zorgen of wel aan de AVG voldaan wordt en laat een audit uitvoeren op één van de gegevens-verwerking waar je verantwoordelijk voor bent. Uit de audit komen 10 bevindingen.

De 10 bevindingen:

1. Privacy by Default is niet toegepast.
2. De noodzaak van de verwerking en de opslag van de gegevens liggen niet vast.
3. Van de doorgiften liggen de wettelijke grondslag en de waarborgen niet vast.
4. De complexiteit van de gegevensverwerking is te hoog, waardoor het corrigeren van foutieve gegevens niet mogelijk is.
5. De levenscyclus van persoonsgegevens is niet meegenomen in het ontwerp.
6. Het hoe en waarom de betrokkenen wel of niet worden geïnformeerd over verwerkingen ligt niet vast.
7. De persoonsgegevens zijn niet overdraagbaar.
8. De architectuur benut niet of beperkt de mogelijkheden van encryptie.
9. Bij het maken van ontwerpkeuzen is men zich niet bewust geweest van hoe keuzen de persoonlijke levenssfeer van betrokkenen kunnen beïnvloeden.
10. Om aan te kunnen tonen dat de verwerking aan de Avg voldoet vraagt om dure audits.

Je vraagt af of je als leadarchitect de belangen van de organisatie ten aanzien van privacy afdoende hebt geborgd.

1. Heb ik voldoende sturing gegeven in de vorm van gehanteerde principes?
2. Heb ik daarbij voldoende duidelijkheid gegeven aan de ontwerpers?
3. Heb ik dat op het juiste moment gedaan?

Je bent op de hoogte van het bestaan van de AVG en weet van de Privacy Baseline van het CIP. Hierdoor heb je de kennis voorhanden om te weten wat er geregeld moet worden.

Hoe zou je, als architect, reageren op de bevindingen:

1. Door per bevinding:
    a. De bevinding te weerleggen of
    b. De bevinding in de toekomst te voorkomen, door:
        i. Het doen van verbetervoorstellen voor de gehanteerde principes of
        ii. Het geven van extra uitleg bij de te hanteren principes

2. Gebruik je bij i of ii :
    a. de NORA (afgeleide) principes of anders
    b. De binnen de organisatie gehanteerde principes

3. Kun je aangeven aan waar/hoe de keuzen in het design-proces het best kunnen worden ingebracht of binnen de organisatie kunnen worden belegd?

Opdracht aan de groepen:

Formuleer als groep een reactie de bevindingen en presenteer deze plenair. Het gaat niet zozeer om de oplossingen, als wel om het leren van elkaars overwegingen.