Van: [redacted]@drechtsteden.nl>
Verzonden: donderdag 17 september 2020 13:02
Aan: [redacted]@nijmegen.nl>; [redacted]@nijmegen.nl>
CC: [redacted]@dordrecht.nl>
Onderwerp: Re: DPIA vraag voor AWS verwerking (+ overeenkomst gezamenlijke verwerking)

Helemaal top [redacted]! Dit is precies wat ik zocht.
Het is een technisch verhaal, maar ik kon het prima lezen als leek dus dit biedt een transparante beschrijving wat er met welke gegevens gebeurt in de AWS omgeving.

Puur voor de bevestiging, je zegt op een gegeven moment “die verwerkt alleen de dtfm code en een secret” dat moet DTMF zijn denk? Of gaat het hier toch om een andere code?

Bedankt, ik ga dit bijvoegen.

Groet!
[redacted]

Van: [redacted] <[redacted]@nijmegen.nl>
Datum: donderdag 17 september 2020 om 12:22
Aan: "[redacted])" <[redacted]@drechtsteden.nl>, [redacted] <[redacted]@nijmegen.nl>
CC: "[redacted]" <[redacted]@dordrecht.nl>
Onderwerp: RE: DPIA vraag voor AWS verwerking (+ overeenkomst gezamenlijke verwerking)

Ha,

De korte beschrijving is er niet, maar bij deze. Hoop dat het kort genoeg is ;-).

Nadat een gebruiker zijn/haar IRMA atttributen (waaronder het BSN) heeft onthuld haalt de backend-server die gegevens op bij de IRMA server die gebruikt is voor het onthullen, op basis van het IRMA sessie id, en slaat die gegevens op in een database. We gebruiken een IRMA server die gehost en beheerd wordt door de Gemeente Nijmegen, voor deze omgeving is een aparte DPIA gemaakt.
De telefooncentrale die het gesprek afhandelt wisselt de binnenkomende DTMF code om voor een secret (via een aanroep naar de backend). Het secret bevat geen informatie, het is alleen een op een cryptografisch veilige manier gegenereerde unieke string. Dat secret wordt meegegeven aan het agent portaal waar een kcc medewerker op ingelogd is. Via de browser van de kcc medewerker wordt de backend aangeroepen en op basis van het secret worden de onthulde gegevens uit de database gelezen en getoond aan de kcc medewerker.
De onthulde gegevens worden niet verwerkt door de telefooncentrale component, die verwerkt alleen de dtfm code en een secret.
Wanneer een gesprek beëindigd is heeft een kcc-medeweker ‘nawerktijd’, waarin ze aan verslaglegging doen. Zodra ze daarmee klaar zijn klikken ze in hun portaal op ‘clear contact’ om aan de telefooncentrale aan te geven dat ze beschikbaar zijn voor een nieuwe beller. Op dat moment

wordt het record met de persoonsgegevens van de beller verwijderd uit de database.
De persoonsgegevens worden in ieder geval ook 1 uur na het aanmaken verwijderd.
Er blijven dus geen persoonsgegevens achter in de database. Er blijft ook geen ander record achter in de database.
Na aanleiding van de pentest/audit is de automatische backup van de database uitgezet. Er worden geen backups of andere kopieën van de database gemaakt.

De persoonsgegevens worden op geen andere plek opgeslagen dan in de database. Ze worden ook niet getoond in logging. Het is ook niet mogelijk om ze te tonen in logging, er is geen code aanwezig in de backend waarmee de logging op een niveau gezet kan worden dat er persoonsgegevens gelogd worden.

De credentials waarmee toegang tot de database verkregen kan worden zijn opgeslagen in een 'AWS parameter store', en daarin encrypt opgeslagen. De toegang tot deze paramater, en de toegang tot de gebruikte encryptiesleutel zijn beperkt. In een apart AWS account specifiek voor audit-trails wordt alle toegang tot de paramater en de encryptie key gelogd.
Ook toegang tot de database wordt gelogd naar het audit-trail account (alle acties binnen de AWS omgeving op AWS resources worden opgeslagen in het audit account).

Groeten,
[redacted]

Van: [redacted] <[redacted]@drechtsteden.nl>
Verzonden: donderdag 17 september 2020 10:45
Aan: [redacted] <[redacted]@nijmegen.nl>; [redacted] <[redacted]@nijmegen.nl>
CC: [redacted] <[redacted]@dordrecht.nl>
Onderwerp: Re: DPIA vraag voor AWS verwerking (+ overeenkomst gezamenlijke verwerking)

Hoi [redacted]

Het gaat vooral om de persoonsgegevens die op de AWS omgeving ergens worden opgeslagen, getoond, verwerkt. Wat ik me kan voorstellen is dat het alleen gaat om wat de agent toont aan de KCC medewerker, dan 'moet' het dus ergens staan. Ik weet alleen niet of die gegevens ook ergens bewaard blijven of opgeslagen zijn. Daar zoek ik een korte beschrijving van, dan kunnen we dat aanvullen in de DPIA en samen met de overeenkomst voor gezamenlijke verwerkingsverantwoordelijken hebben we dat stukje gedekt.

De plaat zal ik aanpassen thanks!
Groet,
[redacted]

Van: [redacted] <[redacted]@nijmegen.nl>
Datum: donderdag 17 september 2020 om 10:09
Aan: "[redacted] <[redacted]@drechtsteden.nl>, [redacted] <[redacted]@nijmegen.nl>
CC: "[redacted] <[redacted]@dordrecht.nl>

Onderwerp: RE: DPIA vraag voor AWS verwerking (+ overeenkomst gezamenlijke verwerking)

Ha,

Mijn kantoordagen zijn weer achter de rug, dus ik ben weer lekker rustig thuis aan het werk ☺.

Ik herken de 2 gele punten, maar weet niet zo goed wat er nu van mij verwacht wordt om te doen…

Ik zie wel dat de plaat op pagina 23 niet de meest recente is. Die is hier te vinden: https://old.sharepoint.com [redacted]

Van: [redacted], [redacted] <[redacted]@drechtsteden.nl>
Verzonden: donderdag 17 september 2020 09:59
Aan: [redacted] <[redacted]@nijmegen.nl>; [redacted] <[redacted]@nijmegen.nl>
CC: [redacted] <[redacted]@dordrecht.nl>
Onderwerp: DPIA vraag voor AWS verwerking (+ overeenkomst gezamenlijke verwerking)

Hoi [redacted] en [redacted],

[redacted] ik weet dat je deze week verminderd bereikbaar bent voor ID bellen, misschien dat jullie er samen antwoord op kunnen geven. Uit de DPIA kwamen vanuit de FG Drechtsteden nog een paar opmerkingen, waaronder de verwerkingen van persoonsgegevens die in AWS in Nijmegen plaatsvinden. Dit is ook belangrijk voor de overeenkomst voor gezamenlijke verantwoordelijkheid (dat zit hem puur in dat kleine stukje namelijk). Kunnen jullie daar kort iets over toelichten?

@[redacted] ik had [redacted] gevraagd om een concept overeenkomst voor gezamenlijke verwerkingsverantwoordellijkheid op te stellen, hij is nu offline begrijp ik. Zou jij kunnen helpen om dat concept op te stellen en te delen?

Hieronder het betreffende stuk van de FG:

De zaken die nu vanuit deze DPIA opvallen zijn de volgende:
-Verwerking van de gegevens door Nijmegen en AWS wordt niet genoemd
-Gebru k van BSN wordt niet genoemd.-Gebruik voor evaluatie wordt niet genoemd
-Hoe wordt aan de aantoonbaarheidsverplichting uit de AVG voldaan indien na het project alle gegevens/aanmeldingen direct verwijderd worden?

De DPIA is raadpleegbaar via deze link: https://teams.microsoft.com [redacted]