

Belangenafweging SOC aanbesteding

18 juli 2024

Vertrouwelijkheid: Openbaar



INHOUDSOPGAVE

1. BELANG VAN HET WATERSCHAPSHUIS	3
2. BELANG VAN DE BETROKKENE	3
3. CONCLUSIE	4

1. Belang van het Waterschapshuis

Het doel van het ontvangen en verwerken van de persoonsgegevens is:

- Het door het Waterschapshuis kunnen uitkiezen van een betrokkene om te interviewen ten behoeve van het controleren van de door de werkgever (de inschrijver van de aanbesteding) aangeleverde informatie.

Het belang voor het Waterschapshuis is hierbij:

- Ervoor zorgen dat het gunnen van de opdracht op de juiste wijze verloopt, door de informatie die is aangeleverd door de inschrijvers te controleren bij de betrokkene.
- Het interview draagt bij aan het gunnen van de, door ons als opdrachtgever beschikbaar gestelde, opdracht aan de juiste inschrijver die voldoet aan de door ons als opdrachtgever gestelde wensen en eisen.

Wijder publiekelijk belang:

- Het SOC draagt bij aan het beveiligen van de systemen en informatie die de primaire processen van de waterschappen uitvoeren. Om dit van goede kwaliteit en borging te voorzien, dient de aanbesteding met extra aandacht voor het beoordelen op de gestelde wensen en eisen te worden doorlopen.

2. Belang van de betrokkene

De persoonsgegevens die worden gedeeld van de betrokkenen zijn:

Type persoonsgegevens	Beoordeling bij het delen van deze gegevens
Voornaam en Achternaam	Namen staan veelal al op internet gedeeld. Deze informatie zal voor een kwaadwillende dus vaak al op een andere plaats vindbaar zijn. Daarnaast kan een kwaadwillende nog niet veel met alleen een naam. Er is een verwaarloosbaar risico op phishing, spam en identiteitsfraude als een kwaadwillende de naam van een betrokkene onderschept. De kans is klein dat de naam verkeerd wordt gedeeld en de impact is ook relatief klein voor de betrokkene. Het risico is dus Laag.
SOC certificeringsniveau 1,2 of 3	Het SOC certificeringsniveau is vergelijkbaar met een opleidingsniveau. Deze informatie wordt door veel SOC-analisten openbaar gedeeld via social media. De informatie wordt door bedrijven opgevraagd om te bepalen of de betrokkene de juiste kwalificaties heeft. Voor een kwaadwillende is er weinig wat deze kan doen met de informatie. De kans is klein dat de naam verkeerd wordt gedeeld en de impact is ook relatief klein voor de betrokkene. Het risico is dus Laag.
Type certificering en instituut	Het type certificering dat wordt gebruikt om het SOC certificeringsniveau aan te tonen, inclusief daarbij het instituut wat de certificering heeft afgegeven, is informatie die vaak al openbaar wordt gedeeld. Deze informatie zal voor een kwaadwillende dus vaak al op een andere plaats vindbaar zijn. Daarnaast kan een kwaadwillende nog niet veel met alleen het type certificering en instituut. Er is een verwaarloosbaar risico op identiteitsfraude als een kwaadwillende het type certificering en instituut dat de certificering heeft afgegeven van een betrokkene onderschept. De kans is klein dat het type certificering met instituut naam verkeerd worden gedeeld en de impact is ook relatief klein voor de betrokkene. Het risico is dus Laag.
Type screening & POB	Het type screening dat wordt gebruikt om de integriteit van de SOC-analist te waarborgen, inclusief daarbij het Particulier Onderzoeksbureau (POB) dat de screening heeft uitgevoerd, is erg

	beknpte informatie, gezien niet gevraagd wordt om de screening in te zien. Deze informatie zal voor een kwaadwillende nauwelijks/geen waarde hebben gezien die niet gebruikt kan worden tegen de betrokkene. De kans is klein dat het type screening en POB verkeerd worden gedeeld en de impact is ook relatief klein voor de betrokkene. Het risico is dus Laag.
Datum start binnen converged OT- en IT-SOC	De startdatum geeft aan sinds wanneer een SOC-analist werkt binnen het converged OT- en IT-SOC. De kans dat de startdatum wordt gelekt is laag. De impact is beperkt. Met een startdatum is alleen te weten sinds wanneer een SOC-analist binnen het converged OT- en IT-SOC werkt. Een kwaadwillende kan hier niet veel mee. Het risico is dus laag.

Deze persoonsgegevens vallen niet onder de categorie bijzondere persoonsgegevens of strafrechtelijke persoonsgegevens. Sterker nog, de meeste van deze persoonsgegevens zijn zakelijke gegevens, die door de betrokkene met regelmaat worden gedeeld op sites zoals LinkedIn.

Maatregelen die worden genomen om het risico voor de betrokkenen verder in te perken:

- De inschrijvingen van de werkgevers van de betrokkenen worden vertrouwelijk behandeld. Dat wil zeggen dat alleen het beoordelingsteam, de betrokken inkoopadviseur(s) en de betrokken juristen kennis kunnen nemen van de persoonsgegevens van de betrokkenen. Daarmee is de toegang tot de persoonsgegevens beperkt.
- De persoonsgegevens die worden gedeeld worden alleen gebruikt om de SOC-analist te interviewen.
- De persoonsgegevens worden, na de bewaartermijn van 3 jaar na tekenen van de overeenkomst op basis van de aanbestedingswetgeving, gepseudonimiseerd.

Kan het doel ook op andere manier bereikt worden?

Nee, het is niet mogelijk om op een andere manier een betrokkene (SOC-analist) te interviewen met het oog op het beoordelen van de inschrijving van de werkgever van de SOC-analist. Het is nodig om een naam te hebben gekoppeld aan de gegevens, zodat een betrokkene gericht uitgenodigd kan worden.

Het risico voor de betrokkene is dus laag, met ook een lage impact op de persoonlijke levenssfeer van de betrokkene.

Het belang van de SOC-analist ligt in een zo laag mogelijke impact op de persoonlijke levenssfeer.

3. Conclusie

Het belang van de betrokkene ligt in een zo laag mogelijke impact op de persoonlijke levenssfeer. Dit is voor deze belangenafweging gekwantificeerd in risico's. Het risico voor de betrokkenen is laag. Daarnaast zijn maatregelen genomen om de risico's nog verder in te perken, wat het risico nog verder verlaagt.

Het belang voor het Waterschapshuis is hoog. Het belang is niet alleen voor het Waterschapshuis, maar ook de deelnemers, de waterschappen, en nog verder het publiek, omdat deze verwerking bijdraagt aan het beschermen van de primaire processen die worden uitgevoerd door de waterschappen.

Het belang van het Waterschapshuis weegt hierbij zwaarder dan dat van de betrokkene, het Waterschapshuis zal dus om de benoemde persoonsgegevens vragen bij de aanbesteding.