Veiligheids- en Gezondheidsregio Gelderland-Midden

ADVIESMEMO

Datum : 05-10-2020
Aan : (MZ)[redacted]
CC: **:** [redacted]
Van : [redacted] Functionaris Gegevensbescherming)
Betreft : Privacy bij coronawerkzaamheden

Aanleiding
In mijn rol als Functionaris Gegevensbescherming heb ik oa. de taak om *toezicht te houden op de gegevensverwerkingen en (on)gevraagd te adviseren over privacy-aangelegenheden bij de ontwikkeling van beleid en systemen*. De afgelopen weken heb ik geprobeerd om me een beeld te vormen van de activiteiten die nu uitgevoerd worden in deze Coronacrisis en wat dit betekent voor de gegevensbescherming.

Inventarisatie
De volgende onderwerpen hebben hierin de aandacht gekregen
- proces van nieuwe medewerkers
- De processen in CoronIT
- De processen in HP Zone (Lite)
- BCO

Omdat nieuwe medewerkers in een systeem werken met vertrouwelijke gegevens die *niet kunnen worden afgeschermd vanwege de uit te voeren werkzaamheden*, is het dus erg belangrijk om stil te staan bij de organisatorische aspecten om dit goed te borgen.
In z'n algemeenheid kan gesteld worden dat men zich bewust is van het werken met privacy gevoelige informatie, maar ook dat het moeilijk is om van nieuwe collega's te verwachten dat ze hierin op hetzelfde niveau werken. Het is duidelijk dat er met name voor de nieuwe medewerkers veel aandacht moet zijn in het werken met privacy informatie. Tijdens het uitvoeren van de analyse werd al actief werk gemaakt van een introductieboekje waarin extra stilgestaan wordt bij integriteit en het tekenen van de bijbehorende gedragscode. Toch zijn er nog verschillende aspecten die aandacht behoeven. Deze zijn in 10 verbeterpunten uitgewerkt.

Bevindingen
Rondom het proces van nieuwe medewerkers zijn er verschillende uitdagingen. Zo gaat het hierbij om het verstrekken van middelen en het geven van een instructie om de middelen goed te gebruiken. Nieuwe medewerkers tekenen een gedragscode. Er is een informatieboekje voor nieuwe medewerkers, er is een masterclass voorafgaand aan de werkzaamheden en op de werkvloer wordt actief gecoacht op een zorgvuldige omgang met vertrouwelijke informatie.

Verbeterpunt:
1. **Vast programma bij introductiebijeenkomst:** In de masterclass wordt aandacht besteed aan het vertrouwelijke karakter van de (persoons)gegevens. De inhoud van de masterclass is nu echter niet of beperkt beschreven. Advies is om alle te bespreken onderwerpen middels een gestructureerde agenda te beschrijven en deze te volgen, zodat geborgd is dat er voldoende aandacht gegeven wordt aan het werken met vertrouwelijke informatie.

In CoronIT worden de gegevens van de mensen vastgelegd die zich aanmelden voor een coronatest.

Op de website van GGD GHOR https://ggdghor.nl/privacyverklaring-coronit/ kan in de privacyverklaring achterhaald worden welke gegevens worden vastgelegd.

Verbeterpunt

2. **Transparantie over gegevensverwerking in CoronIT**: Verwijs op de website van VGGM naar de privacy verklaring CoronIT van GGD GHOR. Op deze manier blijft het ook voor mensen die willen weten wat er gebeurt met hun gegevens ook transparant als ze hier meer informatie over zoeken.

Zodra de uitslag van het lab binnen is, wordt deze zichtbaar in CoronIT; de uitslag van een positieve coronatest gaat naar HP Zone Lite. In HP Zone is een aparte afgeschermde omgeving gemaakt voor de verwerking van gegevens inzake corona. Hier worden de gegevens vastgelegd van degene die positief getest is en wordt ook gestart met het vastleggen van de gegevens van het bron- en contactonderzoek. Op de website van GGD GHOR https://ggdghor.nl/wp-content/uploads/2020/08/privacystatement-bco.pdf wordt hierover veel meer beschreven.

Verbeterpunt

3. **Transparantie over gegevensverwerking voor BCO**: Verwijs op de website van VGGM naar de privacy verklaring BCO van GGD GHOR. Op deze manier blijft het ook voor mensen die willen weten wat er gebeurt met hun gegevens voor BCO transparant als ze hier meer informatie over zoeken.

4. **Transparantie over gebruik gegevenslijsten:** Verschillende (horeca)bedrijven en instellingen houden lijsten bij met gegevens van bezoekers zodat hiermee aansluiting gevonden kan worden met het BCO. Het helpt om als GGD uit te leggen aan burgers dat deze gegevens alleen worden opgevraagd indien er sprake is van een besmetting die te herleiden is naar het specifieke (horeca)bedrijf of instelling. Tevens dient duidelijk te worden wat er met de gegevens gebeurt die wij als GGD op dat moment ontvangen.

5. **Uitbreiding FUBE**: Het functioneel beheer van CoronIT is belegd bij een persoon. Dit wordt nadrukkelijk als een risico benoemd. Er zijn immers veel veranderingen en voorkomen moet worden dat werkzaamheden in het geding komen. Overweeg zodoende om het functioneel beheer over in ieder geval twee personen te verdelen. Zo is er meer tijd voor alle gevraagde aspecten van beheer (gebruikersbeheer, logging en monitoring, instructie etc).

Aangezien de werkdruk bij GGD'en toeneemt, wordt gekeken naar alternatieve manieren om gegevens voor BCO te verwerken. Een van de manieren is om mensen zelf een deel van de administratieve werkzaamheden van het BCO te laten uitvoeren. Dit kan bijvoorbeeld door de betrokkene te vragen om alle contacten inclusief NAW, BSN en contactgegevens in kaart te laten brengen en deze aan de GGD te versturen. Ook wordt gedacht aan een webformulier zodat middels een beveiligde omgeving de juiste gegevens kunnen worden opgevraagd.

Verbeterpunt:

6. **Gebruik beveiligde mailverbinding**: Indien mensen wordt gevraagd om gegevens aan te leveren aan de GGD, dan gaat dit idealiter via een beveiligde omgeving. Onderzocht moet worden op welke manier de gegevens veilig aan de GGD verstuurd kunnen worden (via Zivver?).
7. **Zorg voor een transparante communicatie:** Wederom wordt verwezen naar de uitleg over dit proces in een privacy statement of andere uitleg op de website zodat betrokkenen weten hoe de gegevens aangeleverd kunnen worden en wat er met de gegevens gebeurt.

8. **Beveiligd webformulier:** Er wordt mogelijk een webformulier ontwikkeld. Dit webformulier dient voorzien te zijn van passende beveiligingsmaatregelen zodat de informatie veilig verstuurd kan worden van betrokkene aan de GGD.

Verwerkingsregister
De GGD is verplicht om al haar verwerkingen met persoonsgegevens vast te leggen in een verwerkingsregister. Dit verwerkingsregister dient actueel te zijn en wordt in samenspraak met de Functionaris Gegevensbescherming opgesteld.

Verbeterpunt

9. **Actualiseer verwerkingsregister**: Het verwerkingsregister dient opgesteld te worden en periodiek geactualiseerd te zijn. Vanwege de snel veranderende inzichten wordt voorgesteld om dit beter te borgen zodat de Functionaris Gegevensbescherming vroegtijdig op de hoogte is van veranderingen en zo in staat wordt gesteld om het verwerkingsregister te actualiseren.

Rol Gegevensbescherming
Binnen VGGM is er binnen vrijwel ieder team een aandachtsfunctionaris voor privacy aangesteld. In de gesprekken met verschillende mensen is er duidelijk veel aandacht voor het werken met persoonsgegevens en andere vertrouwelijke informatie. Toch mag niet verwacht worden dat nieuwe mensen in het team al op een zelfde manier (on)bewust bekwaam zijn met het werken met vertrouwelijke gegevens.

Verbeterpunt

10. **Aandachtsfunctionaris privacy in coronateam:** Om privacy een permanente plek in de werkzaamheden te geven, wordt voorgesteld om een aandachtsfunctionaris privacy aan te stellen die als taak heeft om toe te zien op het zorgvuldig borgen van de privacy aspecten van betrokkene. Deze aandachtsfunctionaris staat in nauw contact met de Functionaris Gegevensbescherming en in het team is bekend dat deze persoon hier extra op toeziet. (Deze taak is niet in workload in uren uit te drukken, het gaat vooral om een aanspreekpunt voor het team die alert is op privacy aspecten en extra gespitst is op de manier waarop met vertrouwelijke informatie wordt omgesprongen).

Door bovenstaande verbeterpunten opvolging te geven ontstaat een betere privacyborging. Betrokkenen zijn beter geïnformeerd, nieuwe medewerkers zijn bewust en nieuwe (en bestaande) verwerking worden zorgvuldig getoetst.

[redacted]

Functionaris Gegevensbescherming
Veiligheids- en Gezondheidsregio Gelderland-Midden.