

Bijlage 7.0

Beantwoording vraag AB m.b.t. gegevensveiligheid



Memo Algemeen Bestuur

Onderwerp	Beantwoording vraag AB m.b.t. gegevensveiligheid
Versie	1.0
Bijlagen	-
Datum	06-07-2023
Van	Dagelijks Bestuur RUD Limburg Noord
Aan	Algemeen Bestuur RUD Limburg Noord

Voorstel

- Kennisnemen van de informatie rondom gegevensveiligheid bij de samenwerking.

Aanleiding

In uw Algemeen Bestuur van 22 december 2022 is het verzoek neergelegd om in het Dagelijks Bestuur het aandachtspunt (data)beveiliging en privacy in relatie tot (onderlinge) uitwisseling van gegevens te bespreken.

Vandaar dat deze notitie is opgesteld en u ter kennisname wordt aangeboden.

Inleiding

Medewerkers die in dienst zijn bij de gemeenten en die belast zijn met VTH (basis)taken werken waar mogelijk in de gemeente RX-Mission en daar waar het noodzakelijk is in de RUD omgeving van RX-Mission. Dat de basistaken waar nodig in de RUD omgeving uitgevoerd zouden worden was bekend tijdens de aanbesteding van RX-mission. Een specifiek voorbeeld van 'waar nodig' is het plannen, registreren, uitvoeren en afhandelen van toezicht- en handhavingcontroles bij bedrijven die onder de basistaken vallen. Deze controledata leveren wij naar de viewer Inspectieview milieu. Deze verplichting is net zoals het door omgevingsdiensten uit te voeren basistakenpakket vastgelegd in de Wabo.

Gegevensveiligheid

Kan het samenwerken in de RX-Mission omgeving zonder risico's voor de gegevensveiligheid is de vraag?

Het antwoord op deze vraag: Het risico kan nooit volledig worden weggenomen. Zodra een applicatie gekoppeld is aan het internet is er altijd sprake van risico.

Door kiezen van een leverancier die beveiligingsmaatregelen biedt zoals SSL/TLS versleuteling, firewalls, regelmatige updates van de hard- en software, het volgen van een wachtwoord procedure en die ook nog eens gecertificeerd is op het gebied van informatiebeveiliging en kwaliteit wordt het risico tot een minimum beperkt.

Op de website van onze leverancier is te lezen dat Visma Roxit beschikt over de volgende certificeringen:

- ISO 27001 (Certificaat Informatiebeveiliging);
- ISO27017 (beveiligingsstandaard die is ontwikkeld voor cloudserviceproviders en gebruikers om een veiligere cloud omgeving te creëren en het risico op beveiligingsproblemen te verkleinen);
- ISO27018 (de beveiligingsstandaard die deel uitmaakt van de ISO/IEC 27000-familie van normen. Het was de eerste internationale standaard over de privacy in de cloud)
- NEN7510 (NEN 7510 is een managementsysteemnorm, die een kader stelt voor het organiseren en borgen van informatiebeveiliging binnen een zorginstelling of toeleverancier);
- ISO9001 (ISO 9001 is een norm die eisen stelt aan het kwaliteitsmanagementsysteem van een organisatie).en ISO 14001 (de internationaal geaccepteerde standaard met eisen voor een milieumanagementsysteem) .

Verder zijn in de aanbesteding eisen gesteld aan de locatie van datacenters en de gebruikte servers waardoor de data altijd moet worden behandeld en opgeslagen volgens Europese regelgeving.

Het samenwerken op zich

Het samenwerken in de RUD RX-Mission vereist in de meeste gevallen geen uitwisseling van persoonsgegevens. De RUD adviseert een casemanager van een gemeente over activiteiten in de fysieke leefomgeving. Wie de activiteit uit voert is bij de beoordeling van een verzoek of bij een controle meestal niet relevant voor de RUD. Het toetsen van de integriteit van ondernemers is en blijft een taak van de gemeenten (BIBOB).

De applicatie RX-Mission is ontwikkeld op basis van het principe AVG by design. Zo worden in een omgevingsdossier (met partners deelbare onderdeel) geen persoonsgevoelige informatie opgenomen. Bij een natuurlijk persoon (burger) wordt alleen vermeld 'Natuurlijk persoon'.

Bij bedrijven (Niet natuurlijk persoon) maken we gebruik van openbare via de KVK verkrijgbare informatie (zogenaamde brongegevens).

In de logging van de KVK koppeling en audit trail (logboek) wordt exact vastgelegd welke gebruiker gegevens heeft opgehaald en toegevoegd. (On)geautoriseerd gebruik wordt gemonitord.

Documenten die gekoppeld worden in omgevingsdossiers moeten ten alle tijden geanonimiseerd worden alvorens men deze bestanden mag delen.

Samengevat

De applicatie, de leverancier, de servers en het datacenter moeten voldoen aan de geldende standaarden op het gebied van informatiebeveiliging te weten:

Certificaat Informatiebeveiliging ISO 27001, ISO27017, ISO27018 en NEN7510

Omdat wij bijna dagelijks te maken hebben met vertrouwelijke en privacygevoelige informatie willen wij de zekerheid hebben dat onze leverancier zorgvuldig met de gegevens van onze klanten omgaan. Visma-Roxit meldt op hun website "Informatiebeveiliging is dan ook een cruciaal aspect in onze bedrijfsvoering".

Deze leverancier is dan sinds 2017 ISO 27001 gecertificeerd (actuele Verklaring van Toepasselijkheid). Deze certificering moeten zij periodiek (3 jaar) hernieuwen.

Verder vragen monitoren wij de certificering van de RX-mission applicatie op ISO27017, ISO27018 en NEN7510.

De vraag of medewerkers van de RUD toegang moeten krijgen tot gemeentelijke data is een vraag die zowel in een netwerk alsook in een fysieke dienst met ja beantwoord moet worden. In onze netwerkorganisatie is de discipline om wijzigingen in de status van de medewerkers extreem belangrijk om er voor zorg te dragen dat er geen onbevoegde toegang kan plaats vinden tot gevoelige data.

Verder is de gegevensveiligheid in de RX-Mission omgeving van de RUD gelijk aan de RX-mission omgeving van de gemeenten.