Gemeenteraad van Ridderkerk
p/a griffie

Uw brief van:		Ons kenmerk:	301038
Uw kenmerk:		Contact:	R. de Rooij
Bijlage(n):		Doorkiesnummer:	0180 45 14 03
		E-mailadres:	r.d.rooij@bar-organisatie.nl
		Datum:	11 juni 2021

Betreft: RIB Uitvoeringsplan RKC onderzoek informatieveiligheid

Geachte raadsleden,

In 2019 is door de Rekenkamercommissie een onderzoek uitgevoerd naar de uitwerking en implementatie van de Algemene verordening gegevensbescherming (AVG) bij de gemeente Ridderkerk.

Het Dagelijks Bestuur van de BAR-organisatie heeft naar aanleiding van dit onderzoeksrapport en de rapporten van de gemeenten Albrandswaard en Barendrecht een Uitvoeringsplan laten opstellen. Na bespreking van het Uitvoeringsplan heeft het Dagelijks Bestuur op 17 februari 2021 besloten op welke onderdelen verdere stappen nodig zijn om de informatieveiligheid en privacy te versterken. En tevens is afgesproken u daarover te infomeren. Via deze brief informeren wij u over dit besluit en het vervolgproces.

Uitvoering
Het Uitvoeringsplan richt zich conform de opdracht op de aanbevelingen uit de onderzoeksrapporten. De centrale conclusie van het Uitvoeringsplan is dat er op een aantal terreinen nadere inspanningen nodig zijn. Daarbij is ook geconcludeerd dat het niet lukt alle verbeteringen binnen de bestaande formatie uit te voeren. Daarom heeft het Dagelijks Bestuur prioriteiten gesteld en aangegeven dat voor de uitvoering extra budget moet worden vrijgemaakt. De benodigde extra middelen worden geschat op € 200.000. Dit betekent voor onze gemeente in 2021 circa € 81.000,-. De lasten zijn meegenomen in de eerste tussenrapportage 2021.

De extra maatregelen richten zich op twee invalshoeken. Enerzijds preventie, zodat het risico op dataverlies wordt verkleind en anderzijds op het daadwerkelijk implementeren van maatregelen bij geconstateerde tekortkomingen binnen de uitvoerende processen. De werkzaamheden worden als pilot uitgevoerd voor de duur van 1 jaar.

Koningsplein 1
Postbus 271
2980 AG Ridderkerk

Maatregelen

- *Logging en monitoring*
  - We gaan de wijze waarop we volgen op welke manier dreigingen zich manifesteren, verbeteren. Hiervoor wordt specialistische beveiligingssoftware ingezet om te monitoren, loggen en beoordelen (AI). Daarbij kan 24/7 geautomatiseerd worden geacteerd wanneer er dreigingen ontstaan.
  - Er worden extra interne “branddeuren“ gecreëerd om de data extra te beveiligen.

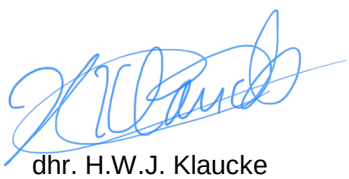
- *Implementeren maatregelen processen met risicovolle persoonsgegevens*
  - Deze processen worden aangepast op basis van de bevindingen uit de (lopende) interne audits. Het werken met decentrale aanspreekpunten en een rapportagestructuur, waarbij periodiek gerapporteerd wordt over risico’s in de processen en systemen, zal er voor zorgen dat de aanbevelingen worden opgevolgd. De CISO en de Privacy Officer ondersteunen hierbij.

- *Versterking Auditing volgens ENSIA systematiek*
  - De ENSIA (Eenduidige Normatiek Single Information Audit) is het verantwoordingsproces over informatieveiligheid bij de gemeente. Dit levert een rapportage en een collegeverklaring op waarin staat in hoeverre de beheersmaatregelen aan de van kracht zijnde beveiligingsnormen voldoen. Hierdoor heeft het gemeentebestuur meer inzicht in de stand van zaken van de informatieveiligheid en kan het hier ook beter op sturen. Een gecertificeerde IT Auditor (RE) zal jaarlijks de opgestelde en de door ons ondertekende collegeverklaring toetsen. Dit resulteert in een Assurance rapport bij de collegeverklaring. Met de collegeverklaring en het assurancerapport, afgegeven door de gecertificeerde IT Auditor (RE), kan de gemeente zich via de ENSIA omgeving verantwoorden naar Logius (DigiD) en het Ministerie van Sociale Zaken en Werkgelegenheid (Suwinet). De CISO continueert zijn rol als centrale ENSIA coördinator.

- *Onderzoek Continuïteit*
  In het onderzoek worden de volgende vragen beantwoord:
  - Hoe continueren we de maatregelen uit de pilot. Daarbij zal ook inzicht gegeven worden in eventueel structureel te verwachten extra kosten.
  - Wat moet er de komende jaren naast de prioritering ook gebeuren om tot een voldoende niveau van veiligheid te komen/ blijven. Gegevensbescherming en het borgen van informatieveiligheid is een doorlopend proces. Omdat dit breder is dan de aanbevelingen uit de onderzoeksrapportages en het Uitvoeringsplan is door het Dagelijks Bestuur ook een aanvullende opdracht aan de organisatie gegeven om dit in kaart te brengen.
  - Welke risico’s zijn er aangaande de bedrijfscontinuïteit en hoe beperken we die.

Hoogachtend,
het college van burgemeester en wethouders van Ridderkerk,

de secretaris | de burgemeester,



dhr. H.W.J. Klaucke | mw. A. Attema