Onderwerp: Beantwoording vragen ex art. 36 RvO van de VVD en D66 over datalek AddComm en beveiliging persoonsgegevens van inwoners
ter informatie

De leden van de raad van de gemeente Groningen
te
GRONINGEN

Telefoon	14 050	Bijlage(n)	1	Ons kenmerk	196425-2024
Datum		Uw brief van		Uw kenmerk	

Geachte lezer,

Hierbij doen wij u de antwoorden toekomen op de door mevrouw I. Jacobs-Setz van de VVD fractie en mevrouw M. Martinez Doubiani van de D66 fractie gestelde vragen ex art. 36 RvO over datalek AddComm en beveiliging persoonsgegevens van inwoners. De brief van de vraagstellers treft u als bijlage aan.

Aanleiding tot het stellen van de vragen is het recente datalek bij AddComm. AddComm maakt voor de gemeente Groningen van digitale data gepersonaliseerde brieven, facturen en aanmaningen. Nadat wij in kennis zijn gesteld van het datalek zijn betrokken inwoners en uw raad geïnformeerd. De fracties van de VVD en D66 hebben over het datalek vijf schriftelijk vragen gesteld. Twee van de vijf vragen waren van technische aard en de antwoorden zijn al met de vragenstellers zelf gedeeld. Middels deze brief willen wij de antwoorden op de overige drie vragen met u delen.

Beantwoording van de vragen:

Bent u van mening dat de verwerkers of leveranciers die toegang hebben tot gemeentelijke gegevens en die van onze inwoners u op een adequate wijze en met gepaste voortvarendheid op de hoogte heeft gesteld van het desbetreffende datalek?

De partij AddComm, had en heeft geen directe toegang tot het netwerk van de gemeente Groningen. Op het moment van het datalek beschikte AddComm alleen over data die door de gemeente Groningen was geüpload binnen de beveiligde AddComm omgeving. Na de eerste melding van het datalek door AddComm is het vervolg in goed overleg en in goede samenwerking verlopen.

Volgvel 1

Middels verschillende berichten in de media zijn onze inwoners op de hoogte gesteld van het datalek. Dit betrof vrij summiere informatie met berichten zoals pas op phishingberichten of oplichting per telefoon. Deze mededeling heeft tot veel onrust geleid, welke mail is nog te vertrouwen en welke niet. Heeft deze onrust uw college ook bereikt en hoe wilt u in de toekomst specifieker communiceren? Waarom is er niet voor gekozen om een brief te sturen in plaats van een mail?

Uit onderzoek van AddComm bleek dat klantdata van de gemeente Groningen zijn buitgemaakt. Op dat moment was nog niet bekend om welke gegevens het ging, of het persoonsgegevens betrof en van welke personen. Dat moest op dat moment nog onderzocht worden. Persoonlijk informeren van onze inwoners heeft de voorkeur, maar omdat niet bekend was wat en wie het betrof en wij toch zo snel mogelijk mensen wilden attenderen hierop, is gekozen voor een algemeen nieuwsbericht met daarin o.a. de oproep om nog meer dan anders goed op te letten op phishingberichten of oplichting per telefoon en bij twijfel aan de echtheid contact op te nemen met de gemeente via ons algemene informatienummer 14050. Wij begrijpen dat dit tot onrust kan leiden, phishing en oplichting aan de telefoon is immers aan de orde van de dag.

Na verder intern onderzoek is duidelijk geworden dat maar een klein deel van de records daadwerkelijk persoonsgegevens bevatte. Snel bleek dat 1 dataset (gevoelige) persoonsgegevens bevatte van 102 inwoners. Het ging in dit geval om cliëntnummers, NAW-gegevens, BSN en het indexeringsbedrag. Deze inwoners zijn op 4 juni per brief geïnformeerd door ons.
Van drie datasets was de inhoud nog onbekend. Nadat de dienstverlening was hervat konden deze drie datasets volledig inzichtelijk worden gemaakt. Daaruit bleek dat deze gegevens van nog 122 andere inwoners bevatte. Het betreft hier inwoners waarbij een brief is verstuurd over betalingsherinneringen, betalingsregelingen en incasso. Deze inwoners zijn op 25 juni per brief geïnformeerd door ons.

Hoe beoordeelt u het ontstaan van het desbetreffende datalek bij deze externe partners en welke maatregelen worden in de toekomst genomen om dit zoveel mogelijk te voorkomen?

Onze externe partner AddComm, is het slachtoffer geworden van cybercriminelen waarbij data zijn ontvreemd. Helaas hebben de security specialisten binnen AddComm dit niet kunnen voorkomen. Onder begeleiding van externe cyber security experts zijn er afspraken gemaakt met de cybercriminelen over het niet publiceren en verwijderen van buitgemaakte klantdata. Deze experts hebben ervaring met dit soort aanvallers en zijn ervan overtuigd dat de afspraken nagekomen worden. AddComm heeft bovendien bewijs ontvangen dat de gegevens zijn gewist.
Voor AddComm weegt het privacybelang van hun klanten heel zwaar. De securityspecialisten van AddComm hebben met externe cyberexperts een nieuwe digitale omgeving gebouwd. Deze nieuwe beveiligde omgeving voldoet aan de gestelde eisen van de gemeente Groningen.

Wij vertrouwen erop u hiermee voldoende te hebben geïnformeerd.