Waarom is toentertijd gekozen om een bedrijf dit te laten doen?

Gemeente Maastricht is in juli 2017 gestart met automatisch cameratoezicht met kentekenherkenning op drie plekken in Randwyck (de Johan Willem Beyenlaan, het Endepolsdomein en de Joseph Bechlaan). Dit ter vervanging van de inzinkbare palen. Het project is via een Europese aanbesteding volgens de openbare procedure op de markt gezet, omdat externe partijen een dergelijk specialistisch systeem meer efficiënt kunnen uitvoeren.
Zoals bekend heeft ARS Traffic deze aanbesteding gewonnen.

Wat is in de overeenkomst afgesproken over informatiebeveiliging?

Binnen de overeenkomst is verklaard dat de kentekengegevens vallen onder de toen geldende Wet Bescherming Persoonsgegevens. Het verzenden en opslaan van kentekens is daarom niet zondermeer toegestaan. Het ANPR-systeem dient te voldoen aan de wettelijke eisen, daartoe dienen de richtlijnen van het (toen nog) College Bescherming Persoonsgegevens in acht te worden genomen. Ook is beschreven dat de data alleen gebruikt mag worden voor de beschreven doelen, niet zijnde een testsysteem, en alleen via beveiligde inlog toegankelijk mag zijn.

Controleert de gemeente daarop? Hoe heeft de gemeente dat gedaan de afgelopen jaren (bijv. door lijfelijk bezoek bij het bedrijf)?

Wij hebben het product na de inbedrijfstelling functioneel gecontroleerd.

De foto's die inzichtelijk zijn geweest vallen niet onder de productieomgeving waarin wij werken, maar onder een testomgeving die bij ARS Traffic parallel draait en die nooit in hun ISO-certificeringstesten en security checks is meegenomen.

Het bestaan van dit testsysteem was de gemeente Maastricht onbekend.

Bij alle huidige ICT aanbestedingen voor geautomatiseerde informatiesystemen, stelt de gemeente security eisen die er voor zorgen dat de gemeente kan voldoen aan de baseline informatiebeveiliging overheid. Een van de eisen betreft het jaarlijks door de leverancier overleggen van een zogenaamde Third Party Memorandum. Een onafhankelijke partij controleert dan of er wordt voldaan aan de gestelde eisen in opzet, bestaan én werking. Als persoonsgegevens verwerkt worden, wordt met leveranciers tevens de verplichte standaard verwerkersovereenkomst van de VNG afgesloten. Hiermee worden de verantwoordelijkheden van betrokken partijen eenduidig vastgelegd. Overigens kan op basis van de nu (door ARS) verkregen informatie niet worden gesteld dat deze omissie dan eerder (door ons) had kunnen worden gedetecteerd.

Hoe nu verder? Welke stappen gaan jullie ondernemen?

Wij hebben een beperkte melding gedaan bij de Autoriteit Persoonsgegevens. Hierbij verwijzende naar de hoofdmelding die door ARS Traffic is gedaan bij de Autoriteit Persoonsgegevens.

Het onderzoek van ARS Traffic naar de volledige impact is nog bezig. Wij beraden ons nog op de te nemen vervolgstappen en de verdere samenwerking met ARS binnen dit project. De uitkomsten van dit onderzoek zullen hierin medebepalend zijn.

Wat is jullie reactie hierop? Vele inwoners zijn vermoedelijk jarenlang kwetsbaar geweest door dit datalek?

Evenals ARS Traffic zijn wij geschrokken. Dit is een ernstige fout. Tegelijkertijd constateren we dat het niet gaat om verrijkte data die eenvoudig te herleiden zijn naar individuele personen en waarbij identiteitsfraude mogelijk is. Ook zijn er geen aanwijzingen dat de data die benaderbaar waren ook daadwerkelijk benaderd zijn door andere derden.

Het systeem van ARS Traffic staat volkomen separaat van het gemeentelijk netwerk. Overige (camera)systemen van de gemeente Maastricht zijn dus niet bij deze specifieke kwetsbaarheden betrokken geweest.