Beantwoording technische vragen

Document:	Jaarrapportage 2020 Bescherming persoonsgegevens (AVG)
Onderwerp:	162. Jaarrapportage 2020 Bescherming persoonsgegevens (AVG)
Portefeuillehouder:	Wethouder J. Schoone
Datum:	4 juni 2021
Van:	Christen Unie

Op 27 mei 2021 heeft de fractie Christen Unie technische vragen gesteld. Hieronder herhalen wij eerst de vraag en vervolgens ons antwoord.
De beantwoording van de vragen 1 t/m 3 is in overleg met de CISO (Chief Information Security Officer) opgesteld. De beantwoording van de overige vragen is door de FG (Functionaris Gegevensbescherming) gedaan.

Vraag 1: Welke (technische) extra maatregelen zijn geïmplementeerd nadat het grootste gedeelte van de gemeente vanuit huis moest werken?
Beantwoording vraag 1: De techniek om de gemeentelijke werkplek vanuit huis te benaderen was al aanwezig ruim voor de corona-pandemie. Dit op basis van Citrix, inclusief two-factor authenticatie. Ook de bandbreedte bleek afdoende. Hierdoor waren er geen aanvullende maatregelen nodig.
Wel was er behoefte aan het op afstand kunnen vergaderen. Om aan deze behoefte te voldoen is eerst Zoom en later Teams beschikbaar gesteld.
Om aandacht te vragen voor de informatiebeveiliging vanuit huis, is er in juni 2020 een artikel op intranet geplaatst. “Informatiebeveiliging anno 2020, ook vanuit huis” met daarin o.a

- het overzicht van de top 10-regels m.b.t. informatiebeveiliging
- een verwijzing naar de strategische en tactische beleidsregels
- een verwijzing naar de praktische operationele regels
- een verwijzing naar Privacy en Informatieveiligheid

Daarbij is ‘Veilig omgaan met informatie’ als speerpunt opgenomen in het concernplan 2021. Het gevolg hiervan is dat dit als input heeft gediend bij het opstellen van de teamplannen.

Vraag 2: Hoeveel applicaties waar persoonsgegevens in verwerkt worden maken nog geen gebruik van two-factor authenticatie?
Beantwoording vraag 2: Doordat de gemeentelijke werkplek alleen toegankelijk is met two-factor authenticatie zijn er geen applicaties met persoonsgegevens benaderbaar zonder deze vorm van beveiliging. Voor cloudapplicaties met persoonsgegevens wordt dit ook afgedwongen. Wanneer een cloudapplicatie geen two-factor-toegang ondersteunt, dan is de mitigerende maatregel dat deze applicatie alleen benaderbaar mag zijn vanuit het gemeentelijke netwerk (waardoor two-factor tot de gemeentelijke werkplek de authenticatie-zekerheid biedt).
Voor twee applicaties bleek deze mitigerende maatregel niet mogelijk, te weten: RAET (HR processen) en een WIZ-Rapportage (sociaal domein). Dit is aanhangig gemaakt bij RAET die zijn systemen daarop recentelijk geschikt gemaakt heeft voor two-factor authenticatie. M.i.v. 01-07-2021 geldt zodoende two-factor authenticatie voor al haar klanten waaronder gemeente Lelystad.

De tweede applicatie is een WIZ-rapportagetool die niet two-factor authenticatie ondersteunt. Momenteel wordt deze applicatie omgezet naar een andere rapportagetool (PowerBI) mét two-factor authenticatie. 16 juni 2021 is opleverdatum.

Vraag 3: Is het college van plan two-factor authenticatie te verplichten bij deze applicaties?
Beantwoording vraag 3: Ja, dat heeft het college in 2020 al impliciet verplicht gesteld, door het strategische informatiebeveiligingsbeleid vast te stellen. De basis voor dit strategisch beleid is de NEN-ISO/IEC 27002:2017 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO). De BIO is het normenkader voor de gehele overheid. Een standaard maatregel uit deze BIO: “Als vanuit een onvertrouwde zone toegang wordt verleend naar een vertrouwde zone, gebeurt dit alleen op basis van minimaal two-factor authenticatie.“

Vraag 4: Welke datalekken zijn gemeld aan betrokkenen?
Beantwoording vraag 4: Dat zijn Cliëntervaringsonderzoek Jeugd, brief Jeugdwet, mail Omgevingsvisie, indieners bezwaarschriften, hack hotmail en TOZO. Per datalek wordt door de FG een afweging gemaakt of het gemeld gaat worden bij betrokkene(n).

Vraag 5: Welke datalekken zijn gemeld bij de AP?
Beantwoording vraag 5: Cliëntervaringsonderzoek Jeugd. Per datalek wordt door de FG een afweging gemaakt of het gemeld gaat worden bij de AP.

Vraag 6: Hoe komt het dat we 1,5 jaar na dato pas het jaarverslag aangeboden krijgen?
Beantwoording vraag 6: U hebt het jaarverslag 2020 aangeboden gekregen, in dezelfde maand als de voorgaande jaren. In de aanbiedingsbrief stond abusievelijk 2019; dit is inmiddels gecorrigeerd.

Vraag 7: Wanneer kunnen we de rapportage over 2020 verwachten?
Beantwoording vraag 7: U hebt voor de vergadering van 22 juni 2021 de jaarrapportage 2020 aangeboden gekregen.