



De heer Mijnders
p/a griffie

Uw brief van: 14 maart 2025
Uw kenmerk: -
Bijlage(n): -

Ons kenmerk: 2025-027682
Contact: Walter van den Berg
Doorkiesnummer: 0180-451234
E-mailadres: Walter.v.d.Berg@DeBedrijfsvoeringsPartner.nl
Datum: 4 april 2025

Betreft: Antwoordbrief schriftelijke vragen (RvO, art. 41) over ICT, privacy en informatieveiligheid

Geachte heer Mijnders,

Op 14 maart 2025 heeft u schriftelijke vragen (RvO, art. 41) gesteld over ICT, privacy en informatieveiligheid. Hieronder worden de antwoorden gegeven.

Vraag 1

Op blz. 11 van begroting van De BedrijfsvoeringsPartner (DBP) uit 2025 wordt het volgende aangegeven *“er is sprake van een verschuiving van kosten richting ICT bijvoorbeeld door het automatiseren van processen verschuiven kosten van personele kosten naar ICT-kosten”*.

Kan het college een paar voorbeelden geven van personele kosten die doormiddel van automatisering zijn vervangen door ICT-kosten?

Antwoord:

Verschuiving van kosten naar ICT (inclusief ICT-personeel) is een gevolg van de steeds verdergaande digitalisering. Voorbeelden:

Digitalisering algemeen

- Digitalisering zorgt voor vermindering van fysieke post- en papierstroom. Effect: (1) minder fysieke distributie van documenten binnen en tussen de gemeentelijke locaties; (2) het opzoeken van documenten in het fysieke papieren archief vereiste een fulltime medewerker; opzoeken is nu digitaal en vereist geen fysieke ophaalactie. Voorbeeld: gedigitaliseerde bouwdoSSIers.
- Digitalisering van processen zorgt voor verschuiving van werk naar ICT-functies. Voorbeeld: handmatig invoeren van facturen wordt in toenemende mate vervangen door software en automatische eFacturatie. Softwaretoepassingen vereisen echter wel ICT-functies zoals applicatiebeheer.

Vervangen en/of versnellen van handmatig werk

- Software robots (ook RPA ofwel Robotic Process Automation) *vervangen* repetitieve handmatige handelingen zoals het overtikken van informatie. Effecten variëren: het niet vervangen van vertrekkende medewerker; minder inhuur; meer tijd voor meer waarde-toevoegend werk. Voorbeelden: RPA oplossingen voor WMO-aanvragen (reductie van 1 fte gerealiseerd); aanvraag levensonderhoud; het proces voor inhuren van externe medewerkers.
- Slimme toepassingen *versnellen* bestaande activiteiten. Voorbeelden: gebruik van softwaretool voor het geautomatiseerd anonimiseren van documenten bij WOO-verzoeken; gebruik van sjablonentool voor het sneller kunnen maken van documenten.

Moderne dienstverlening (extern en intern)

- eDiensten voor onze inwoners zorgen voor moderne dienstverlening én leiden tot (1) minder vragen aan het callcenter; (2) minder papieren aanvragen; (3) minder administratieve afhandeling. Voorbeelden: (1) via de gemeentelijke website onder het kopje *Direct regelen en informatie*. (2) Het digitaal melden – via de kaart – van meldingen openbare ruimte (MOR).
- De gemeenteapp van Ridderkerk leidt tot minder belasting van het KCC. Voorbeeld: veel telefoontjes door inwoners voor het maken of controleren van afspraken worden nu door inwoners zelf geregeld met de gemeente-app.

Betere informatiepositie door dashboards

- Het beschikbaar stellen van dashboards en rapportages met stuur- en managementinformatie vermindert zoektijd en het zelf bijhouden van schaduwadministratie. Effect: minder tijdverlies, hogere kwaliteit. Voorbeelden: de financiële dashboards voor jeugd, participatie, WMO.

Vraag 2

Op blz. 12 wordt het volgende aangegeven *“op het gebied van wet- en regelgeving krijgen we de komende jaren te maken met de “digital decade”. Dit is een set van in eerste instantie 13 wetten die in 2026 geïmplementeerd moeten zijn wat kosten geeft.”*

Kan u het volgende per wet aangeven (indien mogelijk, want de VNG moet als het goed is over verschillende wetten nog adviseren):

- a. Kort wat de wet inhoudt;
- b. Welke acties er verricht moeten worden om aan de wet te voldoen;
- c. Wat de status is van de implementatie van de wet;
- d. Welke kosten er gemoeid zijn bij de implementatie van de wet (hoeveel bekostigd moet worden door Ridderkerk en hoeveel er vanuit het rijk betaald wordt);
- e. Is er voldoende capaciteit om de wetten te implementeren en vanaf 2026 ook toe te passen.

Antwoord:

Om digitalisering te bevorderen, stelt de Europese Unie beleid en wetgeving op, bijvoorbeeld op het vlak van digitale toegankelijkheid, cybersecurity, privacy en gegevensuitwisseling, gebruik van digitale producten en AI. Deze regels zijn ook voor Nederlandse gemeenten van belang.

De VNG heeft de wetgeving onderverdeeld in zes wetgevingsclusters en voert, samen met gemeentelijke vertegenwoordigers, impactanalyses uit. In deze zes clusters worden ook bestaande en in werking getreden verordeningen benoemd (zoals de AVG). Dit om de nieuwe verordeningen in samenhang met de bestaande wet- en regelgeving te kunnen analyseren.

De zes wetgevingsclusters zoals door VNG gehanteerd bij de impactanalyses zijn:

1. Kunstmatige intelligentie, Privacy & Data bescherming:

- Algemene Verordening Gegevensbescherming (AVG).
- ePrivacy directive - ePrivacy richtlijn (Cookiewet).
- AI Act – AI Verordening.
- Machine regulation – Machine Verordening.

2. Cybersecurity:

- Cyber Resilience Act (CRA) - Cyberweerbaarheid Verordening.
- Cybersecurity Act – Cyberbeveiligingsverordening.
- NIS Directive 2.
- Critical Entities Resilience Directive (CER) - Weerbaarheid kritieke entiteiten richtlijn.
- Radio Equipment Directieve.
- Digital Operational Resilience Act (DORA).

3. Datastrategie:

- Interoperability Act – Interoperabiliteitsverordening.
- Open Data Directive (ODD) - Open Data Richtlijn.
- Single Digital Gateway (SDG).
- Data Governance Act (DGA) - Datagovernanceverordening (Dgv).
- EU Data Act - Dataverordening (Dv).
- European Data Spaces - Europese dataruimten.
- High Value Data List (HVDL) - Uitvoeringsverordening High Value Datasets (HVD).

4. Elektronische identificatie:

- European digital identity act (eIDAS - Portemonnee voor de digitale identiteit).

5. Urban Air Mobility:

- Regulations on UAS operations and a regulatory framework for the U-space - Regels voor Unmanned Aerial System (UAS) en richtlijnen voor onbemande luchtvaart.

6. Consumentenbescherming & Regulering van platforms:

- Digital Services Act (DSA) - Digitale Dienstenwet.
- Digital Markets Act (DMA) - Wet Digitale Markten.

De VNG voert met behulp van expertgroepen impact analyses uit op deze wetgeving. Wij participeren vanuit DBP in deze expertgroepen. Voor drie van de wetgevingsclusters (Cybersecurity, Datastrategie en AI) zijn impact analyses opgeleverd. Wij maken gebruik van de beschikbare impact analyses.

Ad 1) Kunstmatige intelligentie, Privacy & Data bescherming

De impact analyse omvat: Machineverordening; ePrivacy richtlijn; ePrivacy verordening; AI-aansprakelijkheid richtlijn; AI-verordening; Algemene verordening gegevensbescherming (AVG).

- Machine Verordening: van toepassing op bedrijven die machines bouwen; geen directe gevolgen voor onze gemeente.
- ePrivacy Verordening & AI Aansprakelijkheidsrichtlijn: op 11 februari 2025 door de Europese Commissie ingetrokken.
- De AVG en de ePrivacy richtlijn (de z.g. Cookiewet) zijn al enkele jaren van kracht.

De beantwoording van uw vragen is daarom gericht op de AI-verordening:

AI Act – AI Verordening

- a. De AI Verordening is gericht op het reguleren van het gebruik van kunstmatige intelligentie in de EU. Het stelt verschillende risicocategorieën vast voor AI-toepassingen en legt strengere eisen op voor toepassingen die een hoog risico met zich meebrengen.
- b. Mogelijke acties:
 - Inventariseer AI-systemen en bepaal risicocategorieën.
 - Organiseer AI-geletterdheid bij medewerkers door trainingen en bewustwordingscampagnes.
 - Richt AI-compliance in binnen de organisatie (bijvoorbeeld via de aanstelling van een AI Compliance Officer) en borg naleving van ethische normen en risicobeoordelingen.
 - Zorg voor registratie van AI-systemen in EU-databank (hoog risico systemen vanaf aug. 2026).
 - Neem maatregelen voor menselijk toezicht en naleving gebruiksinstructies, en zorg voor transparantie door duidelijk te maken dat content gegenereerd is door AI.
 - Verhoogde rapportageverplichtingen voor AI-systemen met hoog risico.
- c. De wet is per 1 augustus 2024 in werking getreden. Algemene verplichtingen en AI-geletterdheid gelden sinds 2 februari 2025. Specifieke verplichtingen voor nieuwe hoog risico AI-systemen worden verplicht vanaf 2 augustus 2026.

- d. Exacte kosten zijn nog niet goed vast te stellen. Wel wordt verwacht dat gemeenten extra capaciteit, expertise en financiële middelen nodig hebben. Op dit moment is het nog niet bekend hoe de kosten verdeeld worden tussen Ridderkerk en het Rijk. De VNG adviseert om snel duidelijkheid te krijgen over adequate financiële compensatie vanuit het Rijk.
- e. De exacte benodigde capaciteit is nog niet goed vast te stellen. Wel wordt verwacht dat gemeenten extra capaciteit, expertise en financiële middelen nodig hebben.

Ad 2) Cybersecurity

Cybersecurity Act (CSA) - Cyberbeveiligingsverordening

- a. De Cybersecurity Act is een Europese wet die de veiligheid van digitale systemen versterkt door een gezamenlijk kader voor certificering van cyberbeveiligingsproducten en -diensten te creëren. Hiermee wordt de digitale weerbaarheid binnen de EU verbeterd.
- b. Mogelijke acties:
 - Gemeenten moeten mogelijk investeren in gecertificeerde cyberbeveiligingsoplossingen.
 - Striktere beveiligingsnormen voor gemeentelijke IT-infrastructuur.
 - Gemeenten moeten voldoen aan nieuwe rapportageverplichtingen bij cybersecurity-incidenten.
 - Mogelijk meer samenwerking met nationale cyberbeveiligingsinstanties.
 - Behoeftte aan extra training op gebied van cyberbeveiliging.
- c. De CSA werd in 2019 van kracht en in 2022 was het jaar van ingaan van de verplichting.
- d. Exacte kosten zijn nog niet goed vast te stellen. Wel wordt verwacht dat gemeenten extra capaciteit, expertise en financiële middelen nodig hebben. Op dit moment is het nog niet bekend hoe de kosten verdeeld worden tussen Ridderkerk en het Rijk. De VNG adviseert om snel duidelijkheid te krijgen over adequate financiële compensatie vanuit het Rijk.
- e. De exacte benodigde capaciteit is nog niet goed vast te stellen. Wel wordt verwacht dat gemeenten extra capaciteit, expertise en financiële middelen nodig hebben.

NIS Directive 2

- a. De NIS 2-richtlijn (Network and Information Security Directive 2) is de vernieuwde Europese wetgeving die de cyberbeveiliging van essentiële en belangrijke sectoren versterkt. Deze richtlijn breidt de reikwijdte van de oorspronkelijke NIS-richtlijn uit, legt strengere beveiligings- en rapportageverplichtingen op voor bedrijven en overheidsinstanties, en bevordert samenwerking tussen EU-lidstaten.
- b. DBP en de gemeente Ridderkerk zijn al in 2024 begonnen met het voorbereiden op deze wet. In deze wet staan de volgende 10 punten (overeenkomstig met de 8 punten van NCSC, zie vraag 3).
 - Zorg ervoor dat het management bedrijfsdoelen en risicobereidheid definieert.
 - Zorg ervoor dat uw NIS2-nalevingskader de bedrijfsdoelen ondersteunt.
 - Betrek, stem af met en houd belanghebbenden op de hoogte - en iedereen die een belang heeft bij de operaties van het bedrijf en de naleving van NIS2.
 - Wijs nalevingsverantwoordelijkheden in het bedrijf aan.
 - Zorg ervoor dat het management toezicht houdt op en goedkeuring geeft voor de implementatie van de cybersecurity-maatregelen.
 - Borg regelmatige beoordeling van het kader.
 - Benut inzichten uit eerdere nalevingsinitiatieven in andere domeinen.
 - Zorg ervoor dat de beveiligingsniveaus geschikt en proportioneel zijn om de toepasselijke risico's te beheren.
 - Houd rekening met de technische, operationele en organisatorische maatregelen.
 - Zorg ervoor dat het management en relevante medewerkers de vereiste cybersecurity-training volgen.
- c. De uit te voeren punten uit deze wet zijn in 2024 in opzet beschreven. In 2025 zal dit worden omgezet naar bestaan van de punten en in 2026 zal dit ook volledig geïmplementeerd zijn. In 2027 zal er een eerste externe audit plaatsvinden.

- d. Exacte kosten zijn nog niet goed vast te stellen. Er is geen bijdrage van het Rijk beschikbaar gesteld.
- e. Voor de volledige implementatie en borging hiervan zal binnen DBP en de gemeente Ridderkerk onvoldoende capaciteit beschikbaar zijn.

Samenvattend betreffende kosten: De exacte kosten voor gemeenten zijn nog niet bekend, maar ze omvatten:

- Implementatie van informatiebeveiliging.
- Uitvoeren van risicoanalyses.
- Nemen van risicomatregelen.
- Opleidingen en rapportage/verantwoording.

Het is nog niet duidelijk hoeveel hiervan door het Rijk zal worden gefinancierd. De VNG meldt dat gemeenten aangeven dat ze extra financiële middelen nodig hebben om aan de verplichtingen te voldoen.

De aanvullende, aan cybersecurity gerelateerde, verordeningen zijn voor de gemeente Ridderkerk van minder direct belang. Voor de volledigheid:

- **Weerbaarheid kritieke entiteiten richtlijn** (Critical Entities Resilience Directive): Europese wetgeving die is ontworpen om de veerkracht van kritieke infrastructuren te verbeteren en omvat sectoren zoals energie, transport, gezondheidszorg en waterbeheer.
- **Cyberweerbaarheid Verordening** (Cyber Resilience Act): Europese verordening en legt fabrikanten, distributeurs en importeurs van hardware en software de verplichting op om te voldoen aan essentiële cybersecurity-eisen.
- **Radio Equipment Directive**: Europese wet die de veiligheid, gezondheid, elektromagnetische compatibiliteit en efficiënt gebruik van het radiospectrum regelt voor draadloze apparaten binnen de EU. De richtlijn stelt eisen aan fabrikanten
- **Digital Operational Resilience Act**: Europese wet die de digitale weerbaarheid van de financiële sector versterkt door strenge eisen te stellen aan ICT-risicobeheer, incidentrapportage en cyberbeveiliging. Dit geldt voor financiële instellingen zoals banken, verzekeraars en beleggingsondernemingen.

Ad 3) Datastrategie

De deelvragen a, b en c beantwoorden we per verordening, de deelvragen d en e gezamenlijk voor de onder dit cluster vallende verordeningen.

Datagovernanceverordening (Data Governance Act (DGA))

- a. Het gebruik van en de toegang tot data worden steeds belangrijker. De DGA zorgt ervoor dat we die data veilig kunnen delen en dat er voldoende ruimte is voor innovatie. Dit gebeurt door nieuwe regels op te stellen voor het delen van gegevens tussen organisaties en individuen, met aandacht voor privacy en veiligheid. De Autoriteit Consument en Markt (ACM) wordt de toezichthouder.
- b. Mogelijke acties:
 - Gemeenten moeten mogelijk hun processen aanpassen voor het hergebruik van data.
 - Toename van verzoeken voor gegevensuitwisseling via databemiddelingsdiensten.
 - Noodzaak om richtlijnen op te stellen voor data-altruïsme en vrijwillig delen van gegevens.
 - Verplichting om transparantie en bescherming van gegevens te waarborgen.
 - Mogelijke extra kosten voor IT-aanpassingen om aan de regelgeving te voldoen.
 - Gemeenten moeten ervoor zorgen dat ze geen exclusieve overeenkomsten aangaan voor het gebruik van data.
- c. Status: datum van ingaan: 23-9-2023.

Dataverordening (Data Act)

- a. De Dataverordening stelt regels op voor het delen en gebruik van gegevens tussen bedrijven, overheden en individuen.
- b. Mogelijke acties:
 - Gemeenten moeten mogelijk overstappen naar nieuwe dataverwerkingsdiensten.
 - Verplichting om gegevens via API's beschikbaar te stellen.
 - Gemeenten moeten afspraken maken over de beschikbaarheid van sensordata.
 - Verplichting om te voldoen aan interoperabiliteitsnormen.
 - Gemeenten moeten reageren op verzoeken van bedrijven en burgers voor toegang tot gegevens.
 - Verhoogde eisen aan datagovernance en beveiliging.
- c. Status: ingetreden op 11-1-2024, van toepassing vanaf 12-9-2025.

Europese dataruimten (European Data Spaces)

- a. De totstandbrenging van gemeenschappelijke, interoperabele dataruimten in de hele EU in strategische sectoren is gericht op het wegnemen van juridische en technische belemmeringen voor het delen van gegevens. Gemeenschappelijke Europese dataruimten zullen de ontwikkeling van nieuwe datagestuurde producten en diensten in de EU bevorderen en de kern vormen van een onderling verbonden en concurrerende Europese data-economie.
- b. Mogelijke acties:
 - Mogelijke kosten voor het upgraden van IT-systemen voor gegevensuitwisseling.
 - Gemeenten moeten personeel trainen in nieuwe protocollen voor gegevensuitwisseling.
 - Samenwerking met regionale en nationale gezondheidsinstanties vereist.
- c. Status: momenteel worden gemeenschappelijke Europese dataruimten ontwikkeld in 14 sectoren/domeinen, denk aan Landbouw, Gezondheid, Financiën en Overheidsdiensten.

Wet implementatie Open data richtlijn (Open Data Directive)

- a. De ODD richt zich op het bevorderen van het hergebruik van overheidsinformatie. Het legt verplichtingen op voor de openbaarmaking van overheidsdata, inclusief onderzoeksdata, en stelt dat deze gegevens beschikbaar moeten zijn via API's. Aan de Open Data Richtlijn wordt met de Wet implementatie Open data Richtlijn (Wiodr) binnen de Wet hergebruik van overheidsinformatie (Who) uitvoering gegeven in Nederland.
- b. Mogelijke acties:
 - Gemeenten moeten hun inkoopvoorwaarden aanpassen om exclusieve datagebruiks-overeenkomsten te vermijden.
 - Gemeenten moeten data via API's beschikbaar stellen.
 - Verhoogde eisen aan de transparantie van gegevensverwerking.
 - Mogelijk meer verzoeken om hergebruik van overheidsinformatie.
 - Gemeenten moeten voorbereid zijn op de verplichting om onderzoeksdata te delen.
 - Mogelijk extra training en ondersteuning nodig voor medewerkers.
- c. Status: op 19 juni 2024 is de Wiodr in werking getreden binnen de Who.

Single Digital Gateway

- a. De Single Digital Gateway (SDG) geeft burgers en bedrijven makkelijk toegang tot digitale overheidsdienstverlening in de Europese Unie. Dat gebeurt met het portaal (gateway) Your Europe. Deze centrale toegangspoort verwijst gebruikers door naar de juiste websites in de verschillende lidstaten. Via Your Europe kunnen burgers en bedrijven op een eenvoudige manier betrouwbare informatie vinden over overheidsdiensten, -producten en -procedures in Europa.
- b. Mogelijke acties:
 - Gemeenten moeten hun diensten en informatie digitaal beschikbaar stellen via het SDG-portaal.
 - Verplichting om administratieve procedures te digitaliseren en toegankelijk te maken voor EU-burgers en bedrijven.
 - Gemeenten moeten zorgen voor een vertaling van cruciale informatie in meerdere EU-talen.

- Verhoogde IT-kosten voor de integratie van gemeentelijke systemen met het SDG-portaal.
 - Gemeenten moeten hun website-inhoud en digitale diensten evalueren en waar nodig aanpassen om te voldoen aan SDG-standaarden.
 - Verplichting om te zorgen voor de toegankelijkheid van online diensten voor mensen met een handicap.
 - Gemeenten moeten waarborgen dat alle benodigde informatie up-to-date en accuraat is.
 - Gemeenten krijgen te maken met verhoogde eisen voor de verwerking van grensoverschrijdende aanvragen en verzoeken.
- c. Status: 1-10-2018 in EU aangenomen, binnen de gemeente Ridderkerk is SDG geïmplementeerd.

Verordening interoperabel Europa (Interoperability Act)

- a. Deze verordening betreft de digitale interoperabiliteit tussen overheden: het vermogen van overheidsdiensten om samen te werken en op elektronische wijze informatie uit te wisselen.
- b. Mogelijke acties:
- Gemeenten moeten mogelijk interoperabiliteitsbeoordelingen uitvoeren bij nieuwe IT-initiatieven.
 - Delen en hergebruiken van softwareoplossingen wordt bevorderd.
 - Gemeenten moeten zorgen voor naleving van Europese interoperabiliteitsstandaarden.
 - Impact op gemeentelijke IT-infrastructuur en digitale samenwerking.
 - Gemeenten moeten deelnemen aan Europese interoperabiliteitsprojecten.
 - Mogelijke kosten voor IT-aanpassingen en trainingsbehoeften.
- c. Status: ingegaan op 2-4-2024, gehandhaafd vanaf 12-6-2024. Artikel 3 wordt per 12-1-2025 gehandhaafd. Artikel 3 van deze verordening bepaalt dat openbare lichamen een interoperabiliteitsbeoordeling moeten doen alvorens zij een besluit neemt met betrekking tot een digitale overheidsdienst met mogelijke gevolgen voor grensoverschrijdende operabiliteit. Hier zullen dus ook gemeenten rekening mee moeten houden vanaf begin 2025.

Uitvoeringsverordening High Value Datasets (High Value Data List)

- a. Deze verordening bepaalt welke datasets als hoogwaardig worden beschouwd en stelt verplichtingen voor het beschikbaar stellen van deze data door overheidsinstanties.
- b. Mogelijke acties:
- Gemeenten moeten hoogwaardig geachte datasets beschikbaar maken voor het publiek.
 - Verplichting om te voldoen aan specifieke eisen voor het delen van data.
 - Gemeenten moeten mogelijk hun IT-systemen aanpassen voor dataverwerking en -publicatie. Mogelijke kosten voor de implementatie van nieuwe gegevensbeheersystemen.
 - Gemeenten moeten samenwerken met nationale en Europese instanties om data te delen.
 - Gemeenten moeten zorgen voor de naleving van transparantie en beveiligingsnormen.
- c. Status: 21-12-2022 is de HVD van de EU gepresenteerd. In samenwerking met o.a. de VNG is er gewerkt aan een high value dataset voor gemeenten, deze is in 2016 samengesteld. Zie ook de Open Data Richtlijn.

Deelvragen d en e:

- De impact van de onderzochte EU-dataregelgeving lijkt beperkt, omdat de onderzochte EU-dataregelgeving in het bijzonder randvoorwaardelijke verplichtingen voor, met name, commerciële partijen stelt. We zien de meeste impact voor gemeenten bij de herziene Who (Wet Hergebruik van Overheidsinformatie).
- Het voldoen aan de verplichtingen uit EU-dataregelgeving vraagt van gemeenten een aantal aanpassingen/ veranderingen. De belangrijkste gaan over het stellen van kaders voor hergebruik van beschermde gegevens, inspanningsverplichtingen voor het vergemakkelijken van hergebruik bij ontwerp en vervaardigen van documenten, bij het stellen van voorwaarden bij financiering van specifieke activiteiten in relatie tot hergebruik en bij de verstrekking van gegevens voor hergebruik.

Mogelijke acties:

- Aanpassen processen voor het hergebruik van data.
- Noodzaak om richtlijnen op te stellen voor data-altruïsme en vrijwillig delen van gegevens.
- Acties gericht op het waarborgen van transparantie en bescherming van gegevens.
- Mogelijke IT-aanpassingen en/of upgraden van systemen om aan de regelgeving te kunnen voldoen bijvoorbeeld op het gebied van gegevensuitwisseling door middel van APIs.
- Borgen dat er geen exclusieve overeenkomsten worden aangegaan voor het gebruik van data.
- Voorwaarden vaststellen aan de algemene wijze van beschikbaarstelling van data en bij specifieke gegevens voor hergebruik (verstrekking) van die data.
- Trainen medewerkers in nieuwe protocollen voor gegevensuitwisseling.
- Voorbereiden op de verplichting om onderzoeksdata te delen.
- Diensten en informatie digitaal beschikbaar stellen via het SDG-portaal.
- Verplichting om te zorgen voor de toegankelijkheid van online diensten voor mensen met een handicap.

Indien het aantal verzoeken voor hergebruik van data na de invoering van de EU- dataregelgeving net als in de huidige situatie laag blijft, dan zullen de kosten niet sterk verschillen van de kosten die op basis van de huidige regelgeving gemaakt moeten worden. Hierbij moet wel in acht genomen worden dat er door de 'hernieuwde' aandacht voor hergebruik van data en communicatie over de EU-data regelgeving mogelijk meer hergebruik verzoeken komen. Dan moeten de gestelde voorwaarden ingevuld worden om hieraan te kunnen voldoen.

Er zijn geen financiële afspraken vanuit het Rijk over eventuele kosten volgend uit deze wetgeving.

Ad 4) Elektronische identificatie**European digital identity act (eIDAS)**

- a. eIDAS staat voor Electronic Identities and Trust Services en omvat elektronische identificatiemiddelen. Via eIDAS kunnen inwoners uit andere Europese landen met hun nationale inlogmiddel ook inloggen bij Nederlandse overheden. Daarnaast kan eIDAS gebruikt worden voor aanbestedingen.
- b. Gemeenten hebben de volgende verplichtingen:
 - Aansluiten op eIDAS infrastructuur.
 - Implementeren van eIDAS.
 - eIDAS betrouwbaarheidsniveau vaststellen.Hieraan wordt gewerkt voor de gemeente Ridderkerk.
- c. Status: Deze wet is sinds mei 2024 van kracht, lidstaten zijn verplicht om hier tegen 21 november 2025 systemen voor op te zetten. Per 1-7-2023 is de Wet Digitale Overheid (Wdo) gefaseerd in werking getreden. Deze wet regelt dat Nederlandse burgers en bedrijven veilig en betrouwbaar kunnen inloggen bij de (semi-)overheid. De Wdo bouwt voort op Europese ontwikkelingen en de eIDAS-verordening inzake elektronische identiteitsstelsels.
- d. De kosten zijn nog niet bekend.
- e. Er is voldoende capaciteit aanwezig om hier uitvoering aan te geven.

Ad 5) Urban Air Mobility

- a. Deze verordening richt zich op het reguleren van stedelijke luchtmobiliteit in de EU, met inbegrip van drones en andere onbemande luchtvaartuigen. Het doel is om veilig en efficiënt gebruik van luchtruim te waarborgen en innovatie in stedelijke mobiliteit te stimuleren.
- b. Impactanalyse van de VNG is nog niet aanwezig. Op de gemeente Ridderkerk zal de impact naar verwachting klein zijn. We kunnen daarbij denken aan de noodzaak om beleid te ontwikkelen voor het veilig gebruik van drones binnen de gemeente.
- c. Voor de stedelijke luchtmobiliteit zijn er verschillende regels opgesteld. De regels voor U-space gelden vanaf 22-4-2021, de volgende set aan regels gaan in op 22-2-2026.

- d. Op dit moment verwachten wij geen kosten.
- e. Mogelijk is capaciteit nodig om beleid te ontwikkelen.

Ad 6) Consumentenbescherming en regulering van platforms

Wet Digitale Markten (Digital Markets Act)

- a. Deze wet moet zorgen voor een concurrerende en eerlijke digitale sector, met meer innovatie, hoogwaardige digitale producten en diensten en eerlijke prijzen voor consumenten. Het grootste deel van de markt is in handen van een klein aantal grote online platforms, ook wel Poortwachters genoemd. De wet legt beperkingen op aan het gedrag van deze platforms om monopolies te voorkomen en de rechten van consumenten te beschermen. Met de Uitvoeringswet digitale marktenverordening wordt de Autoriteit Consument en Markt (ACM) aangewezen als de bevoegde nationale autoriteit in Nederland.
- b. Impactanalyse van de VNG is nog niet aanwezig. Op de gemeente Ridderkerk zal de impact naar verwachting klein zijn.
- c. De Wet Digitale Markten is ingegaan op 2-05-2023. De Uitvoeringswet digitale marktenverordening is ingegaan op 8-3-2025.
- d. Op dit moment verwachten wij geen of weinig kosten.
- e. We verwachten weinig impact op de capaciteit.

Digitale Dienstenwet (Digital Services Act)

- a. De DSA reguleert digitale diensten in de EU, met de focus op het verbeteren van de transparantie en het beperken van illegale inhoud op online platforms. De wet legt verantwoordelijkheden op aan online dienstverleners om ervoor te zorgen dat hun platforms veilig zijn voor gebruikers. Deze wet organiseert gemeenschappelijke regels omtrent verplichtingen en verantwoordelijkheden van digitale intermediairs in de EU. Met de DSA worden er maatregelen getroffen tegen illegale onlinegoederen, -diensten en -inhoud. Ook beschermt het de grondrechten van gebruikers, waaronder de vrijheid van meningsuiting. De DSA leidt ook tot een sterker overheids-toezicht op onlineplatforms. De DSA heeft betrekking op alle aanbieders van online digitale diensten en heeft als doel consumenten online beter te beschermen.
- b. Ook gemeenten bieden online diensten aan en vallen daarom onder de regels van de verordening. De Impactanalyse van de VNG is nog niet aanwezig. Op de gemeente Ridderkerk zal de impact naar verwachting klein zijn.
- c. De DSA die op 16-11-2022 in werking trad, heeft rechtstreekse werking. Onlineplatforms hadden tot 17-2-2023 de tijd om het aantal actieve eindgebruikers op hun websites te vermelden. Op 17-2-2024 zijn de regels van de DSA van toepassing geworden.
- d. Op dit moment verwachten wij geen of weinig extra kosten.
- e. We verwachten weinig impact op de capaciteit.

Vraag 3

De VNG-resolutie 'Digitale veiligheid kerntaak voor gemeenten' roept gemeenten op om verschillende punten op te pakken. Op eerdere vragen heeft u als college aangegeven hiervoor een 8 punten plan te hebben opgesteld, kan u het 8 punten plan delen met de raad?

Antwoord:

Dit 8 puntenplan was in 2019 een opsomming van de 8 aandachtspunten opgesteld door Nationaal Cyber Security Centrum (NCSC) om te komen tot meer (digitale) Informatieveiligheid binnen de 4 organisaties. Deze 8 punten zijn verwerkt in het huidige Informatieveiligheidsbeleid 2024-2026.

Vraag 4

In de resolutie zijn o.a. de volgende punten opgenomen waarbij gemeenten worden opgeroepen deze op te pakken:

- Incidenten te delen met de Informatie Beveiligingsdienst (IBD) wanneer een dergelijk incident ook zou kunnen optreden bij andere gemeenten en/ of andere sectoren.
- Jaarlijks een incidentoverzicht op categorieniveau te delen met de IBD, zodat een compleet inzicht bestaat van dreigingen, trends en ontwikkelingen.
- Een digitaal incidentbestrijdingsplan vast te stellen en jaarlijks te actualiseren • invulling te geven aan de noodzakelijke intergemeentelijke solidariteit bij (gemeentelijke) digitale incidenten mede op aangeven van de Informatiebeveiligingsdienst.
- Periodiek te oefenen met cyberincidenten om daarmee de gemeentelijke weerbaarheid te toetsen en te vergroten.
- Periodiek het onderwerp digitale veiligheid in het college van B&W te agenderen.
- In de Integrale Veiligheidsplannen ook de digitale aspecten expliciet te benoemen.

Wilt u per genoemd punt, specifiek aangeven/ toelichten welke acties de gemeente Ridderkerk/ DBP heeft verricht?

Antwoord:

- Punt 1: Deze incidenten worden aan de IBD gemeld.
- Punt 2: Dit staat op de planning. De CISO is als werkgroeplid van de IBD hierbij betrokken.
- Punt 3: Dit staat op de planning. De CISO is als werkgroeplid van de IBD hierbij betrokken.
- Punt 4: Deze oefening staat gepland voor najaar 2025 i.s.m. de IBD en de VNG.
- Punt 5: Momenteel is het team Informatieveiligheid & Privacy (IV&P) van DBP (ook namens de gemeente Ridderkerk) bezig met het opzetten van kwartaalrapportages aangaande de speerpunten uit het Informatieveiligheidsbeleid 2024-2026. Hierin zijn ook de digitale aspecten meegenomen.
- Punt 6: De digitale aspecten worden in de veiligheidsplannen / continuïteitsplannen meegenomen.

Vraag 5

Betreft het periodiek bespreken van digitale veiligheid binnen het college van B&W, is de aanname van de CDA-fractie juist dat dit de afgelopen jaren niet is gebeurd (in ieder geval niet genoteerd op de agenda):

- a. Zo nee tijdens welke B&W vergaderingen is dit geagendeerd?
- b. Zo ja, kan het college toezeggen dit onderwerp periodiek (minimaal 1 keer per kwartaal) op de agenda te zetten?

Antwoord:

- Punt a: Dit is correct. Zie onder vraag 4, punt 5.
- Punt b: Zie onder vraag 4, punt 5.

Vraag 6

Ziet het college het inzetten van ethische hackers als mogelijkheid voor de gemeente Ridderkerk/ DBP om 'zwakke plekken' binnen onze informatiesystemen op te sporen? Graag toelichten waarom wel/niet?

Antwoord:

Momenteel is dit niet opgenomen in het Bewustwordingsprogramma 2025. Wel staat er op de websites van de gemeente Ridderkerk en DBP een Responsible disclosure procedure. Responsible disclosure is een cyberveiligheidspraktijk waarbij beveiligingsonderzoekers of ethische hackers ontdekte kwetsbaarheden privé melden aan de betrokken organisatie in plaats van ze direct openbaar te maken. Dit geeft de organisatie de tijd om het probleem op te lossen voordat kwaadwillenden er misbruik van kunnen maken.

Vraag 7

Kan het college toelichten welk beleid de gemeente op dit moment heeft rondom het gebruik van apps afkomstig uit landen met een offensief cyberprogramma op werkdevices?

Antwoord:

DBP en de gemeente Ridderkerk hebben, aan de hand van een lijst volgens de richtlijnen van de VNG, applicaties geblokkeerd waarvan niet met zekerheid de informatieveiligheid en privacy van de medewerkers en burgers te garanderen is. Daarnaast werken de gemeente Ridderkerk en DBP conform de richtlijn dat de applicaties die gebruikt worden door de medewerkers van de gemeente Ridderkerk en DBP, wanneer niet afkomstig uit de applicatiebibliotheek, hier toestemming voor gevraagd moet worden bij het team IV&P / I&A.

Vraag 8

Kan het college aangegeven welke apps er op dit moment verboden zijn om op werk devices te gebruiken? En wanneer er geen apps verboden zijn, kan het college specifiek toelichten waarom hiervoor gekozen is?

Antwoord:

Zie het antwoord op vraag 7. Twee voorbeelden: Trello en CoPilot mogen niet gebruikt worden. Hiervoor worden dan alternatieven geboden vanuit de applicatiebibliotheek van DBP.

Vraag 9

In het advies van de VNG wordt ook gesproken over een risicoanalyse om te kijken welke functies de meeste risico lopen bij het gebruik van bepaalde apps. Is deze risicoanalyse ook uitgevoerd in Ridderkerk/ DBP en kan het college aangeven of er voor bepaalde functies strengere eisen zijn gesteld rondom het gebruik van bepaalde apps?

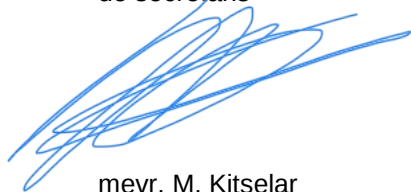
Antwoord:

DBP heeft een risicoanalyse gedaan op de meest kritische applicaties (applicaties waarin veel persoonsgegevens worden gedeeld). Hiermee weet DBP ook meteen om welke functies het gaat. Er zijn nog geen extra eisen gesteld, naast dat elke medewerker een VOG bij indiensttreding moet aanleveren.

Wij vertrouwen erop u voldoende te hebben geïnformeerd.

Hoogachtend,

het college van burgemeester en wethouders van Ridderkerk,
de secretaris



mevr. M. Kitselar

de burgemeester,



dhr. C.A. Oosterwijk