19434441

0000000001

19434441

KPMG Advisory N.V.
Postbus 74500
1070 DB Amsterdam

Laan van Langerhuize 1
1186 DS Amstelveen
Telefoon (020) 656 7890

Vertrouwelijk
Provincie Groningen
De heer 5.1.2e
Sintjansstraat 4
9712 JN GRONINGEN

Amstelveen, 17 oktober 2017

Geachte heer 5.1.2e

Namens KPMG Advisory N.V. (hierna: KPMG) danken wij u voor de mogelijkheid die de Provincie Groningen ons heeft gegeven om een privacynulmeting uit te mogen voeren. In dit rapport presenteren wij de resultaten van de door ons uitgevoerde werkzaamheden. Wij hebben de opdracht uitgevoerd conform onze offerte "Privacynulmeting", d.d. 18 november 2016 met referentie A1600009000 VO.

Het doel van de opdracht was inzicht te verschaffen in hoeverre de Provincie Groningen voldoet aan huidige en toekomstige privacywet- en regelgeving en wat de Provincie Groningen nog zou moeten doen om hier op termijn volledig aan te voldoen.

Wellicht ten overvloede merken wij op dat deze rapportage uitsluitend is bestemd voor de Provincie Groningen en zonder wederzijdse, voorafgaande toestemming niet verder mag worden verspreid.

Met de oplevering van deze rapportage beschouwen wij onze werkzaamheden, zoals overeengekomen in onze offerte en de daarop volgende afstemming over de opdracht, tijdig en conform afspraak afgerond.

Wij hebben de samenwerking met uw organisatie tijdens onze werkzaamheden zeer op prijs gesteld en hopen onze relatie met uw organisatie te mogen continueren.

Mochten er nog vragen zijn met betrekking tot dit rapport, schroom dan niet om contact met mij op te nemen.

Hoogachtend,
KPMG Advisory N.V.

5.1.2e

Partner

0000000002

Inhoudsopgave

Achtergrond, doelstellingen aanpak (1.3)

1. Achtergrond

Per 1 januari 2016 is de uitbreiding op de Nederlandse privacywetgeving 'Meldplicht datalekken en boetebevoegdheid CBP' van kracht. Daarnaast zal de stringentere privacywetgeving op Europees niveau, de 'Algemene Verordening Gegevensbescherming' (AVG) per 25 mei 2018 van toepassing zijn. De bestaande en aankomende wetgeving is complex en soms nog vaag. Voor de Provincie Groningen bestaat er onvoldoende duidelijkheid in hoeverre er op dit moment wordt voldaan aan bestaande en toekomstige privacyvereisten en welke risico's daarmee samenhangen.

Sinds de invoering van de Meldplicht datalekken begin 2016 kunnen er potentieel hoge boetes worden opgelegd. Met de inwerkingtreding van de AVG zijn de boetebedragen verhoogd. Daarnaast ondervinden organisaties steeds vaker reputatieschade door de toenemende media-aandacht voor privacy-incidenten. Effectief risicomanagement op het gebied van security en privacy is voor de Provincie Groningen van fundamenteel belang voor het behalen van de doelstellingen van de organisatie en het behouden van de reputatie naar burgers, leveranciers, haar eigen medewerkers en andere stakcholders.

2. Doelstelling onderzoek

De Provincie Groningen heeft ons gevraagd adviseswerkzaamheden uit te voeren met als doel:

- inzicht te geven in de mate waarin de Provincie op organisatorisch, technisch en procedureel niveau invulling geeft aan de principes en eisen die worden gesteld door de huidige privacywetgeving;
- inzicht te geven in de belangrijkste risico's die de Provincie Groningen op dit moment loopt inzake de huidige en toekomstige privacywetgeving;
- op basis van de AVG de Provincie Groningen te voorzien van aanbevelingen voor het verbeteren en implementeren van aanvullend benodigde privacymaatregelen en deze vorm te geven in een verbeterplan.

De nulmeting is gedaan bij de ambtelijke organisatie die onder Gedeputeerde Staten valt.

3. Aanpak

Wij hebben onze werkzaamheden uitgevoerd door het doorlopen van de volgende vijf fasen.

1. Kick-off

Tijdens een kick-offbijeenkomst en de daarop volgende afstemming is de aanpak bevestigd en de scope van de opdracht nader bepaald. Er is afgesproken het onderzoek nader te richten op al dan niet aanwezige privacybeschermende maatregelen in de processen:

- Subsidieverlening;
- Toezicht en handhaving;
- Cameratoezicht bij bruggen en sluizen.

Aanpak en beperkingen van het onderzoek (2/3)

Vervolgens is in samenwerking met de Concernfunctionaris Informatiebeveiliging en de Concern Jurist bepaald wie zijn uitgenodigd voor deelname aan de interviews. Tevens is in deze fase documentatie opgevraagd die ons inzicht geeft in de huidige inrichting van de privacy- en beveiligingsorganisatie. Daarnaast zijn praktische afspraken gemaakt over de opdrachtuitvoering, zoals de interviewplanning, communicatie en het uitwisselen van (vertrouwelijke) informatie.

2. Veldonderzoek

In deze fase hebben wij op basis van interviews en het bestuderen van documentatie met behulp van het KPMG Privacy Management Raamwerk en de tien daarbij behorende privacyprincipes (zie Bijlage A en B) de waarborgen ten aanzien van privacybescherming binnen de Provincie Groningen onderzocht. De geselecteerde processen zijn hiertoe vanaf de verzameling van persoonsgegevens, de opslag, het gebruik, de wijzigingen van de gegevens, de toegang tot en met archivering en eventuele vernietiging van persoonsgegevens onderzocht, waarbij tevens is nagegaan in hoeverre relevante beveiligingsmaatregelen zijn getroffen.

3. Analyse

In de analysefase hebben wij de verkregen informatie geconsolideerd en het volwassenheidsniveau van de organisatie op het gebied van privacybeheersing aan de hand van de relevante elementen uit het KPMG Privacy Management Raamwerk bepaald.

Op basis van het uitgevoerde onderzoek hebben wij deze adviesrapportage opgesteld met hierin onze observaties, de geïdentificeerde risico's en onze aanbevelingen. De aanbevelingen zijn hierbij tevens in de vorm van een roadmap weergegeven (zie Bijlage D).

Wij hebben onze werkzaamheden uitgevoerd in de periode maart tot en met juni 2017. Deze rapportage geeft de stand van zaken weer per medio juni. De inhoud is op 10 juli jl. afgestemd met [redacted] en [redacted]. De resultaten van deze afstemming en de feedback van [redacted] op het conceptrapport van d.d. 28 juli jl. zijn verwerkt in deze versie van de rapportage.

4. Beperkingen van het onderzoek

De uitgevoerde nulmeting kan niet worden gezien als een alomvattend onderzoek op het gebied van data privacy. De privacynulmeting verschaft inzicht in de tekortkomingen en aandachtspunten op de vooraf gedefinieerde tien privacyprincipes en op een selectie aan voor dit onderzoek relevant geachte wettelijke eisen (zie Bijlage C).

Daarbij moeten de beperking in acht worden genomen:

- veranderingen aan de IT-omgeving kunnen impact hebben op één of meerdere privacyprincipes.
- Onze bevindingen zijn gebaseerd op en beperkt tot de interviews met medewerkers van de Provincie (zie Bijlage D) en de aan ons beschikbaar gestelde documenten (zie Bijlage E).

Leeswijzer (33)

- Wij hebben voor ons onderzoek gebruikgemaakt van zowel voor ons beschikbare schriftelijke informatie als mondeling verkregen informatie. Dit impliceert dat de juistheid en volledigheid van de in dit rapport opgenomen informatie afhankelijk is van de aan ons ter beschikking gestelde schriftelijke en mondelinge informatie. Wij hebben niet zelfstandig de juistheid en volledigheid van de verstrekte informatie onderzocht.
- Aan onze rapportage kan geen zekerheid met betrekking tot de gebruikte informatie worden ontleend. Het is de bedoeling dat u op basis van onze rapportage inzake deze adviesopdracht uw eigen conclusies ten behoeve van uw besluitvorming trekt.
- De aard van de opdracht brengt met zich mee dat wij geen juridisch advies verstrekken. Voor zover wij gedurende de opdracht of in ons rapport verwijzen naar relevante wet- en regelgeving dient dit derhalve niet beschouwd te worden als het verstrekken van een juridisch advies.
- Ons rapport is uitsluitend voor u bestemd en het is niet toegestaan het rapport dan wel delen daaruit te gebruiken voor andere doeleinden dan overeengekomen, openbaar te maken of aan derden te verstrekken, eruit te citeren of eraan te refereren zonder onze uitdrukkelijke voorafgaande toestemming.

5. Leeswijzer

- Dit rapport is verder als volgt opgebouwd: in hoofdstuk 2 is in de managementsamenvatting een overzicht van de belangrijkste resultaten opgenomen en hoofdstuk 3 bevat de detailuitwerking naar aanleiding van ons onderzoek.
- In deze bijlagen bij dit rapport zijn de privacyprincipes, het KPMG Privacy Management raamwerk, de bijbehorende wettelijke grondslagen en overzichten van geïnterviewde medewerkers en de bestudeerde documentatie opgenomen.
- Enkele van onze observaties in Hoofdstuk 3 zijn voorzien van een icoon van de Europese vlag ( ). Hiermee geven we aan dat de observatie voortkomt uit een nieuwe vereiste uit de aankomende Algemene Privacy Verordening (AVG). De overige observaties zijn gerelateerd aan reeds bestaande eisen, voortkomend uit de huidige Nederlandse privacy-wetgeving.

2 Managementsamenvatting (13)

1. Inleiding

De Provincie Groningen heeft ons gevraagd een privacynulmeting uit te voeren om inzage te geven in hoeverre de organisatie voldoet aan huidige en toekomstige privacywet- en regelgeving en wat de Provincie Groningen nog zou moeten doen om hier op termijn volledig aan te voldoen. Wij hebben onze meting uitgevoerd bij de ambtelijke organisatie die onder Gedeputeerde Staten valt en onze werkzaamheden nader gericht op al dan niet aanwezige privacybeschermende maatregelen in de processen: Subsidieverlening, Toezicht en handhaving en Cameratoezicht bij bruggen en sluizen.

2. Mate van volwassenheid

Om de volwassenheid objectief te kunnen toetsen, hebben wij gebruikgemaakt van een volwassenheidsmodel. Dit model is gebaseerd op de KPMG Privacy Maturity Assessment Methodology en helpt inzicht te bieden in de mate waarin aan wettelijke eisen is voldaan evenals de mate waarin randvoorwaardelijke organisatorische, procedurele en technische maatregelen zijn getroffen die een organisatie in staat stellen om aan deze eisen te kunnen voldoen. De hiernaast weergegeven tabel en het spinnenwebdiagram tonen het door ons vastgestelde volwassenheidsniveau voor de Provincie Groningen. De tabel en het diagram geven voor elk van de tien gedefinieerde privacyprincipes weer wat de volwassenheidsscore is en welke risico-indicatie wij daaraan hebben gekoppeld:

- De niveaus van volwassenheid variëren van niveau 1 tot en met 5, waarbij 5 het meest volwassen niveau is.
- De risico's zijn Hoog (H), midden (M) en laag (L) geclassificeerd.

Wij adviseren om minimaal volwassenheidsniveau 3 na te streven om 'AVG-compliant' te zijn.

Privacyvolwassenheid Provincie Groningen		
Privacyprincipes	Volwassenheid	Risico
1. Management	1	H
2. Transparantie	2	M
3. Keuze en toestemming	2	M
4. Doelbinding	2	H
5. Rechtmatige Grondslag	2	H
6. Rechten van betrokkenen	2	M
7. Verwerking door derde partijen	2	H
8. Beveiliging	3	H
9. Kwaliteit	3	L
10. Toetsing en handhaving	2	M

Overzicht volwassenheidsniveau's

2 Management samenvatting (2/3)

Samenvattend komt uit onze nulmeting naar voren dat de Provincie Groningen over een privacy-organisatie beschikt die het beste kan worden gekarakteriseerd als onvoldoende. Organisatorische technische en procedurele maatregelen zijn veelal informeel en borgen op ad-hoc basis dat aan de principes en eisen die worden gesteld door de huidige privacywetgeving wordt voldaan.

3. Belangrijkste bevindingen

De belangrijkste risico's die uit ons onderzoek naar voren zijn gekomen zijn:

- Er is geen sprake van een privacygovernance- en accountability-structuur waardoor het risico bestaat dat door onduidelijkheden in de verantwoordelijkheidsverdeling niet in lijn met de privacyvereisten wordt gehandeld.
- De Provincie Groningen beschikt niet over een geformaliseerd privacybeleid en -strategie, waaronder richtlijnen voor het uitvoeren van Privacy Impact Assesments (PIA's). Hierdoor bestaat er geen referentiekader om op terug te vallen en bestaat het risico dat niet consistent in lijn met de privacywetgeving wordt gehandeld.
- De Provincie Groningen beschikt niet over een actueel en compleet register van verzamelde en verwerkte persoonsgegevens. Dit gebrek aan overzicht leidt ertoe dat niet aantoonbaar kan worden gemaakt dat voor alle data aan de privacy-voorschriften voor het bewaren en verwerken wordt voldaan.
- Met partijen waarvoor de Provincie Groningen taken uitvoert, of die namens de Provincie werkzaamheden verrichten, zijn niet in alle gevallen bewerkersovereenkomsten afgesloten. Tevens is er geen actueel register beschikbaar waarin partijen zijn opgenomen waarmee de Provincie Groningen (persoons)gegevens uitwisselt. Gebrek aan bewerkersovereenkomsten en een gegevensuitwisselingsregister kunnen ertoe leiden dat niet aan de wet wordt voldaan doordat relevante afspraken ontbreken.
- Het eigenaarschap van datakwaliteit is niet duidelijk belegd. Dit kan resulteren in inconsistente vastleggingen of verkeerde interpretaties van data. Het correct verwerken van persoonsgegevens is een vereiste uit de Wbp en de AVG.
- De Provincie Groningen beschikt niet over een beleid en methode voor de overdracht van vertrouwelijke gegevens waardoor het risico bestaat dat de beveiliging niet is geborgd.
- De Provincie beschikt niet over een complete set aan richtlijnen en procedures voor het aantoonbaar voldoen aan de wet ten aanzien van:
  - het op transparante wijze informeren en vastleggen van gegevens;
  - het vragen om toestemming;
  - het bewaren, schonen en archiveren van persoonsgegevens;
  - inzage-, correctie- en verwijderingsrecht;
  - het verstrekken van gegevens (verstrekkingenbeleid).

4. Overzicht aanbevelingen

In onderstaande tabel is een overzicht opgenomen van de belangrijkste aanbevelingen die bij onze werkzaamheden naar voren zijn gekomen.

Overzicht aanbevelingen	
1	Een privacygovernance en -accountabilitystructuur op te stellen en te implementeren met daarin centraal een Functionaris Gegevensbescherming met een coördinerende rol.
2	Een privacybeleid en -strategie op te stellen en te zorgen voor implementatie door privacytrainingen en bewustwordingscampagnes zodat het beleid gaat leven binnen de organisatie. Voorbeelden van bewustzijnsacties zijn communicatie via intranet, e-mailen posters, formulieren en verklaringen bij indiensttreding.
3	Richtlijnen en template op te stellen en te implementeren voor het uitvoeren van PIA's en risicoanalyses voorafgaand aan nieuwe projecten en gegevensverzamelingen.

2 Managementsamenvatting (33)

Overzicht aanbevelingen (vervolg)	
4	In lijn met de verplichtingen vanuit de AVG een actueel en compleet register op te stellen met daarin een overzicht van alle verzamelde persoonsgegevens, het doel waarvoor ze worden verwerkt en wat er met die gegevens gebeurt.
5	Bewerkersovereenkomsten afsluiten met partijen waarvoor de Provincie taken uitvoert en die namens de Provincie werkzaamheden verrichten. Het gaat hierbij onder andere om de Omgevingsdienst Groningen (ODG) welke namens de Provincie werkzaamheden verricht en Samenwerkingsverband Noord Nederland (SNN) en Regio Assen – Groningen waarvoor de Provincie werkzaamheden verricht. Tevens dienen bewerkersovereenkomsten te worden afgesloten met partijen waarbij door de Provincie, ICT-diensten worden ingekocht.
6	Een register op te stellen om inzichtelijk te maken met welke partijen de Provincie (persoons)gegevens uitwisselt.
7	Het reeds opgestelde conceptplan van aanpak voor het project DOO-Data-kwaliteit definitief te maken en te starten met de realisatie van de projectdoelen.
8	Een beleid en methode voor de beveiligde overdracht van vertrouwelijke gegevens op te stellen en te implementeren.
9	Richtlijnen en procedures op te stellen en te implementeren ten aanzien van het op transparante wijze informeren en vastleggen van gegevens; vragen om toestemming; het bewaren, schonen en archiveren van (persoons)gegevens; en het inzage-, correctie- en verwijderingsrecht.
10	Een verstrekkingenbeleid op te stellen en te implementeren waarin richtlijnen staan beschreven voor het uitwisselen van (persoons)gegevens met derde partijen.

Voor de gedetailleerde uitwerking van onze bevindingen en aanbevelingen verwijzen wij naar Hoofdstuk 3. In Bijlage D is in de Privacy roadmap een samenvatting van het verbeterplan opgenomen.

A.Provinciale organisatie en gegevensverwerking

1. Inleiding

In deze paragraaf zijn als inleiding op de detailbevindingen de provinciale organisatie en belangrijkste vormen van gegevensverwerking in scope kort beschreven.

2. De provinciale organisatie

De privacynulmeting is uitgevoerd bij de ambtelijke organisatie die valt onder Gedeputeerde Staten (GS). De ambtelijke organisatie is gericht op beleidsvoorbereiding en uitvoering van provinciale taken op het gebied van bijvoorbeeld ruimtelijke ordening en openbaar vervoer.

3. Gegevensverwerking

Momenteel zijn organisaties nog verplicht om gegevensverzamelingen te melden bij de Autoriteit Persoonsgegevens (AP). Deze eis vervalt met de ingang van de AVG. Er zijn twee meldingen gedaan bij de AP:

- Eén voor camerabeelden bij bruggen en sluizen (AP-melding 1578410)en
- Eén voor een werkgelegenheidsonderzoek Provincie Groningen (AP-melding 1624652).

Onze nulmeting hebben wij met name gericht op de gegevensverwerking ten behoeve van:

- Subsidieverlening;
- Toezicht en handhaving;
- Cameratoezicht bij bruggen en sluizen.

Voorbeelden van persoonsgegevens die worden verwerkt in deze processen zijn NAW-gegevens van aanvragers van subsidies en van degenen waarbij toezicht en handhaving plaatsvindt. In geval van handhaving in het kader van de Wet BIBOB (Bevordering Integriteits-beoordelingen door het Openbaar Bestuur) en bij camerabeelden is daarbij sprake van verwerking van persoonsgegevens die in hoge mate vertrouwelijk zijn.

BOzservaties, risico's en aanbevelingen (10)

OBSERVATIES	RISICO'S	AANBEVELINGEN
A. Privacy-visie en strategie Alhoewel op hoofdlijnen privacy-uitgangspunten zijn beschreven, beschikt de Provincie niet over een expliciet formeel gedocumenteerde en geïmplementeerde beleid en strategie met betrekking tot de beschermíng van persoonsgegevens en het borgen van de privacy van de betrokkenen. **B. Rollen en verantwoordelijkheden** Er is geen sprake van een formele privacy-organisatie in de vorm van een Data Privacy Officer (DPO) of Functionaris voor de Gegevensbescherming (FG). Vraagstukken over het verstrekken van gegevens worden als impliciet onderdeel van bestaande processen afgehandeld. **C. Bewustzijn privacy - en informatiebeveiliging en meldplicht datalekken** Uit onze onderzoekswerkzaamheden is naar voren gekomen dat er binnen de Provincie recent een aantal bewustwordingsinitiatieven heeft plaatsgevonden. Voorbeelden hiervan zijn een mystery guest onderzoek, pentesten, phishing mails en een workshop datalekken. Deze initiatieven zijn vooral gericht op informatiebeveiliging en in mindere mate op privacy. Zo is er geen sprake van expliciete trainingen/opleidingen of andere bewustzijnscampagnes welke er op gericht zijn om privacy te laten leven binnen de organisatie. De Provincie heeft een beknopte procedure meldplicht datalekken (incident-responsplan) opgesteld. (Mogelijke) Datalekken dienen conform de procedure meldplicht datalekken te worden gemeld bij Facilitaire Zaken (FZ) of ICT. Op basis van de interviews is naar voren gekomen dat nog niet alle medewerkers op de hoogte zijn waar (privacy) incidenten dienen te worden gemeld. In de praktijk komen deze meldingen hierdoor in veel gevallen bij de Concernfunctionaris Informatiebeveiliging of bij de Concernjurist terecht. Er zijn tot op heden nog geen meldingen gedaan bij de Autoriteit Persoonsgegevens. **D. PIA's en risicoanalyses** Er zijn binnen de Provincie Groningen geen richtlijnen opgesteld en geïmplementeerd voor het voorafgaand aan nieuwe projecten en nieuwe gegevens-verzamelingen uitvoeren van Privacy Impact Assessments (PIA's).	Beleid en strategie zijn fundamenten voor de privacy-organisatie en privacybeheersomgeving. Gebrek aan compleet en actief uitgedragen privacy-beleid en strategie leidt ertoe dat er voor de medewerkers geen normenkaders of richtlijnen zijn om op terug te vallen. Hierdoor bestaat het risico dat niet consistent wordt gehandeld. Omdat er geen actueel en breed gecommuniceerd beleid is dat concrete richtlijnen bevat, ontbreken belangrijke nuances van de aankomende wet- en regelgeving. Wanneer privacyrollen en verantwoordelijkheden niet duidelijk zijn toegewezen, gecommuniceerd of genomen worden, bestaat het risico dat beleid niet in de praktijk wordt gerealiseerd of nageleefd. Het leidt er mogelijk toe dat bij privacyvraagstukken of -incidenten niet de juiste functionarissen (tijdig) worden benaderd, met inefficiënte of onjuiste besluitvorming tot gevolg. De reeds geratificeerde Algemene Verordening Gegevensbescherming verplicht organisaties om periodiek en voor nieuwe verwerkingen van persoonsgegevens PIA's uit te voeren.	Wij adviseren de Provincie Groningen: • Een privacybeleid en -strategie op te stellen en te zorgen voor implementatie door privacy-trainingen en bewustwordingscampagnes zodat het beleid gaat leven in de organisatie. Voorbeelden van bewustzijnsacties zijn communicatie via intranet, e-mail en posters, formulieren en verklaringen bij indienstreding. • Een privacygovernance en -accountability structuur op te stellen en te implementeren met daarin centraal een Functionaris Gegevensbescherming (FG) met een coördinerende rol. Tevens is het van belang om per domein of organisatieonderdeel een privacycoördinator aan te stellen die een ondersteunende functie heeft ten aanzien van de naleving van privacywet- en regelgeving. Deze coördinator betreft veelal een parttime rol en rapporteert direct aan de FG. • Te waarborgen dat medewerkers weten waar ze zich moeten melden en hoe zij dienen om te gaan met een (mogelijk) datalek incident. Zij dienen daarbij op de hoogte zijn van de consequenties indien de procedure niet juist, tijdig en volledig wordt nageleefd. • Richtlijnen en een template op te stellen en te implementeren voor het uitvoeren van PIA's en risicoanalyses voorafgaand aan nieuwe projecten en gegevensverzamelingen. De risicoanalyses zouden eventueel als onderdeel van die voor informatiebeveiliging kunnen plaatsvinden.

B Observaties, risico's en aanbevelingen (2/2)

	OBSERVATIES	RISICO'S	AANBEVELINGEN
2. TRANSPARANTIE - De organisatie heeft de verplichting om betrokkenen te informeren over hoe gegevens verzameld en verwerkt worden.	**E. Informatieplicht en wijzen op rechten van betrokkenen** Uit ons onderzoek is naar voren gekomen dat het niet altijd even duidelijk is voor welke doelen informatie wordt verzameld en op welke wettelijke gronden. De privacy voorwaarden en prodaimer op de website van de Provincie Groningen zijn beperkt van omvang. Voor de processen subsidieverlening en toezicht en handhaving zijn geen expliciete procedures opgesteld om betrokkenen te informeren omtrent de gegevensverwerking. Zo wordt niet op formulieren vermeld dat gegevens van betrokkenen worden verzameld en verwerkt. In de praktijk worden burgers door medewerkers ingelicht over geldende procedures inclusief de verzameling en verwerking van (persoons-) gegevens. Medewerkers handelen met betrekking tot het transparant zijn over de vastlegging en verwerking van persoonsgegevens geregeld op eigen gevoel. Dit levert inconsistent handelen op. Medewerkers zijn niet in alle gevallen goed op de hoogte over wat er precies met de betreffende persoonsgegevens gebeurt. Opslag van beelden in het kader van cameratoezicht bij bruggen en sluizen is door middel van een folder onder de aandacht gebracht van vaarrecreanten en door middel van een persbericht aan de beroepsvaart. Automobilisten, fietsers of voetgangers die gebruik maken van bruggen en sluizen worden echter niet op de hoogte gebracht van de camera's en opslag van camerabeelden door middel van bijvoorbeeld bordjes die hier melding van maken.	Het niet of op beperkte wijze communiceren over de verwerking van persoonsgegevens aan de betrokkenen leidt ertoe dat niet wordt voldaan aan de wettelijke vereisten. Dit kan een rol spelen bij de beoordeling door de Autoriteit Persoons-gegevens van een datalek en een wegingsfactor zijn bij de bepaling van de hoogte van een eventueel toe te kennen boete.	Wij adviseren de Provincie Groningen: • Het privacystatement op de website van de Provincie Groningen nader uit te werken zodat wordt voldaan aan de vereisten vanuit het transparantiebeginsel. • Procedures op te stellen en te implementeren om burgers te informeren over de gegevenszameling en -verwerking en hun rechten. • Bordjes te plaatsen bij camera's langs bruggen en sluizen waardoor burgers worden geïnformeerd omtrent de aanwezigheid van camera's en het opslaan van camerabeelden.

Observaties, risico's en aanbevelingen (3/10)

3. KEUZE EN TOESTEM MING - individuen moeten de mogelijkheid hebben om te kiezen of en welke gegevens worden verzameld en verwerkt.

OBSERVATIES	RISICO'S	AANBEVELINGEN
F. Keuze en Toestemming Bij de processen subsidieverlening en toezicht en handhaving handelen medewerkers vaak op eigen initiatief met betrekking tot de vastlegging van persoonsgegevens. Burgers zullen naar redelijkheid er vanuit gaan dat de door hen of hun aangeleverde persoonsgegevens worden opgeslagen. Uit de interviews blijkt echter dat er in sommige gevallen wordt uitgegaan van 'meer is beter' waardoor meer persoonsgegevens worden opgeslagen dan noodzakelijk. Deze situaties zijn vaak het gevolg van het ontbreken van richtlijnen om de medewerkers hierin te sturen. Betrokkenen kunnen geen invloed uitoefenen op opslag van beelden in het kader van cameratoezicht bij bruggen en sluizen.	Als er geen richtlijnen zijn die sturing geven aan de keuzemogelijkheden die medewerkers aan burgers mee kunnen geven, ontstaat het risico dat er inconsistent wordt gehandeld. Hierdoor worden mogelijk teveel persoonsgegevens verzameld zonder dat de burger daartegen bezwaar heeft kunnen maken. Wanneer het verzamelen van persoonsgegeven niet proportioneel is aan het vooraf gestelde doel, levert dit een onrechtmatige verwerking op.	Wij adviseren de Provincie Groningen: • Richtlijnen op te stellen en te implementeren om de medewerker richting te geven hoe te handelen bij het verzamelen van persoonsgegevens. Dit hoeven geen strikte werkinstructies te zijn, maar meer generieke richtlijnen, bijvoorbeeld geïllustreerd aan de hand van voorbeeldcases, die nog wel ruimte voor professional judgement overlaten voor de medewerkers. • Extra kaders te communiceren bij het verzamelen van bijzondere persoonsgegevens. Deze kaders zouden minder vrijblijvend moeten zijn dan de generieke richtlijnen.

Observaties, risico's en aanbevelingen (4/10)

4. DOELBINDING - Gegevens kunnen niet onbeperkt worden verzameld en verwerkt. Gegevens mogen niet worden verzameld en verwerkt zonder een precieze doelomschrijving

OBSERVATIES	RISICO'S	AANBEVELINGEN
G. Inventarisatie en classificatie GV De AVG schrijft voor dat organisaties waar verwerking van persoonsgegevens plaatsvindt over een actueel en compleet register dienen te beschikken met daarin een overzicht van alle door de organisatie verzamelde persoonsgegevens, het doel waarvoor ze worden verwerkt en wat er met die gegevens gebeurt. Bij de Provincie Groningen is geen recente inventarisatie beschikbaar waarin is opgenomen welke data, met welke classificatie, in welk systeem worden opgeslagen. Er ligt veel verantwoordelijkheid bij de individuele medewerkers met betrekking tot de keuze welke persoonsgegevens worden verzameld. Dataminimalisatie principes worden niet toegepast, waardoor in sommige gevallen het beginsel 'meer is beter' wordt gehanteerd. Er vinden geen gestructureerde (privacy) trainingen plaats waarbij medewerkers worden getraind om dataminimalisatie toe te passen en geen gegevens te verzamelen die buiten de oorspronkelijke doelbinding vallen. Wij hebben vernomen dat CVs tijdens sollicitatieprocedures langer worden bewaard dan toegestaan conform de AVG. Dit is in strijd met de doelbinding. Camerabeelden worden veelvuldig overschreven. Alleen als er iets gebeurd is en de gegevens zijn opgevraagd, bijvoorbeeld door de politie, dan worden de beelden langer bewaard. Bij de implementatie van KIWI is slechts in beperkte mate rekening gehouden met privacyaspecten. Zo is er niet in alle gevallen sprake van verplichte invoervelden, die waarborgen dat alleen gegevens worden verzameld die in lijn zijn met de doelbinding.	Gebrek aan een actueel en compleet register van verzamelde en verwerkte persoonsgegevens leidt ertoe dat door een gebrek een aan overzicht niet aan privacy-voorschriften voor wat betreft bijvoorbeeld transparantie, doelbinding en rechtmatige grondslag kan worden voldaan. Door de individuele medewerker veel ruimte te bieden om zelf te bepalen welke data hij/zij vastlegt ten behoeve van zijn casus brengt het risico met zich mee dat persoonsgegevens worden verzameld die buiten de doelbinding vallen of niet proportioneel zijn aan het te beantwoorden doel. Dit brengt compliance risico's met zich mee. Het risico wordt vergroot, doordat er weinig beleid, richtlijnen of kaders zijn die hier enige sturing op geven.	Wij adviseren de Provincie Groningen: • Om een register in lijn met de verplichtingen vanuit de AVG op te stellen met daarin een overzicht van alle door de organisatie verzamelde persoons-gegevens, het doel waarvoor ze worden verwerkt en wat er met die gegevens gebeurt en weg te gooien wat niet binnen de doelbinding valt. • Richtlijnen op te stellen en te implementeren om medewerkers richting te geven bij het verzamelen van persoonsgegevens, waarbij zogenaamde 'Privacy by design'-principes in acht dienen te worden genomen, zoals het principe van data-minimalisatie. • Medewerkers er op aan te sturen om hun belangen-afwegingen vast te leggen wanneer het gaat om het verzamelen van bijzondere persoonsgegevens of persoonsgegevens waar de burger geen toestem-ming voor heeft gegeven, maar die wel van belang zijn bij de verdere behandeling van de casus. • Een PIA uit te voeren met betrekking tot KIWI.

Observaties, risico's en aanbevelingen (5/10)

5. RECHTMATIGE GRONDSLAG - Een organisatie moet weten hoe het gegevens verzamelt, hoe veel, en op basis van welke grondslag.

OBSERVATIES	RISICO'S	AANBEVELINGEN
H. Rechtmatig gebruik De provinciale bestuursorganen verwerken allerlei persoonsgegevens. Denk aan de gegevens van personeel, indieners van bezwaarschriften, klachten, Wob-verzoeken en subsidieaanvragen. Er is een protocol Wbp en meldplicht datalekken waarin op hoofdlijnen waarborgen zijn ingericht om onrechtmatige verwerkingen tegen te gaan. Echter is hier geen (interne) controle op waardoor gegevens mogelijk onrechtmatig worden verwerkt. Medewerkers handelen in deze gevallen vaak op eigen initiatief, maar stemmen in de praktijk wel af met (privacy) juristen inzake het delen danwel verder verwerken van gegevens.	Wanneer medewerkers op eigen initiatief persoonsgegevens delen met andere partijen of afdelingen, ontstaat het risico dat gegevens worden gebruikt buiten de oorspronkelijke doelbinding of worden verwerkt zonder rechtmatige grondslag. Het breed interpreteren van de doelbinding en de rechtmatige grondslag, door bijvoorbeeld de reikwijdte van relevante wet- en regelgeving breed te interpreteren kan een onrechtmatige verwerking van persoonsgegevens opleveren wanneer niet wordt voldaan aan het proportionaliteits- of subsidiariteitsvereiste.	Wij adviseren de Provincie Groningen: • Richtlijnen op te stellen en te implementeren om beter gewogen beslissingen te maken omtrent het verder verwerken van data.
I. Dataretentie Binnen de processen in scope zijn verschillende wetten die invloed hebben op de bewaartermijnen. Dat er verschillende wetten en regels zijn maakt het complex voor de medewerker om te bepalen welke regeling van toepassing is en welke wet prevaleert boven de andere. Op dit moment hebben medewerkers onvoldoende handvatten om hier juiste beslissingen over te maken.	Gebrek aan retentiebeleid leidt tot het risico dat door onduidelijkheden persoonsgegevens te lang worden bewaard en er niet wordt voldaan aan de vereisten op het gebied van doelbinding.	Wij adviseren de Provincie Groningen: • Retentiebeleid te definiëren en te implementeren voor verschillende processen en systemen. Daarbij is het belangrijk om vast te leggen op basis van welke (wettelijke) grondslag de gegevens bewaard blijven en voor hoe lang.
J. Datavernietiging Er is geen beleid voor het schonen van data. In Promis is gegevensvernietiging niet mogelijk geweest. Hierin zitten gegevens die allang vernietigd hadden moeten worden. In KIWI worden momenteel functionaliteiten ingebouwd om bewaartermijnen te monitoren en te handhaven. Inzake het schonen van data dient een routine te worden ontwikkeld en is een jaarlijkse inhaalslag vereist om gegevens te vernietigen. Voor de vernietiging van fysieke informatie zijn speciale afgesloten papierbakken beschikbaar gesteld binnen de gehele Provincie. De inhoud van deze bakken wordt vernietigd door een gespecialiseerd bedrijf (Visser Assen). Een bewerkersovereenkomst met deze afvalverwerker ontbreekt.	Gebrek aan het schonen van data en een bewerkersovereenkomst voor het vernietigen van fysieke informatie leiden tot het risico dat door onduidelijkheden persoonsgegevens niet in lijn met de daartoe opgestelde vereisten worden vernietigd.	Wij adviseren de Provincie Groningen: • Een routine te ontwikkelen voor het schonen van data • Een bewerkersovereenkomst voor het vernietigen van fysieke data op te stellen en te implementeren

Observaties, risico's en aanbevelingen (6/10)

	OBSERVATIES	RISICO'S	AANBEVELINGEN
5. RECHTMATIGE GRONDSLAG	**J. Datavernietiging (vervolg)** Voor de vernietiging van digitale gegevens is een proces ingericht. Gegevensdragers die niet meer worden gebruikt worden vernietigd door een extern bedrijf dat daarin is gespecialiseerd. Een bewerkersovereenkomst ontbreekt. Camerabeelden worden wekelijks overschreven. Alleen als er iets gebeurd is en de gegevens zijn opgevraagd, bijvoorbeeld door de politie, dan worden de beelden langer bewaard.	Gebrek aan een bewerkersovereenkomst voor het vernietigen van digitale gegevens leidt tot het risico dat door onduidelijkheden persoonsgegevens niet in lijn met de daartoe opgestelde vereisten worden vernietigd.	Wij adviseren de Provincie Groningen: • Een bewerkersovereenkomst voor het vernietigen van digitale data op te stellen en te implementeren.
6. RECHTEN VAN BETROKKENEN - Betrokkenen hebben o.a. het recht van inzage en het recht om vergeten te worden.	**K. Rechten van betrokkenen** Conform het protocol Wbp en meldplicht datalekken is een hoofdregel dat de betrokkene vooraf in begrijpelijke taal geïnformeerd wordt over wat er precies aan informatie wordt verwerkt en wat het doel daarvan is. Dit is in lijn met de informatieplicht als vermeld in de AVG. Uit de interviews blijkt dat hier in de praktijk niet volledig naar wordt gehandeld. Zo zijn er geen geformaliseerde procedures over hoe om te gaan met het inzage- correctie-, overdraagbaarheids- en verwijderingsrecht van burgers. Formele verzoeken worden formeel afgerond. In de praktijk komen dergelijke verzoeken nog niet in grote aantallen voor. Camerabeelden worden alleen langer dan één week bewaard indien beelden worden opgevraagd. Bovenstaande observatie ten aanzien van de rechten van geregistreerden, is hier ook van toepassing.	Gebrek aan begrijpelijke procedures met betrekking tot inzage-, correctie- en verwijderingsrecht leidt tot het risico dat door onduidelijkheden niet aan deze rechten wordt voldaan.	Wij adviseren de Provincie Groningen: • Begrijpelijk procedures op te stellen en te implementeren om te voldoen aan rechten van betrokkenen voor wat betreft inzage-, correctie-, verwijderings- en overdraagbaarheidsrecht.

Observaties, risico's en aanbevelingen (7/9)

	OBSERVATIES	RISICO'S	AANBEVELINGEN
7. VERWERKING DOOR DERDEN - Persoonsgegevens kunnen alleen worden verstrekt aan derden wanneer specifieke overeenkomsten zijn aangegaan en hierop wordt toegezien.	**L. Delen van data** Binnen de organisatie worden persoonsgegevens verwerkt waarop de Wet bescherming persoonsgegevens van toepassing is. Dit feit moet conform de huidige wetgeving worden gemeld bij de AP. Wij hebben vastgesteld dat er twee meldingen bij de AP zijn gedaan door de Provincie Groningen. Dit betreft melding 1578410 logging audio video en data ten aanzien van bediening bruggen en sluizen in Groningen en melding 1624652 ten aanzien van een werkgeliegenheids-onderzoek door de Provincie. Deze melding(en) zijn enigszins verouderd. Een periodieke controle op bestaande en nieuwe gegevensverwerkingen ontbreekt. Binnen de Provincie is geen verstrekkingenbeleid geformaliseerd ten aanzien van het delen van persoonsgegevens met derde partijen. In de praktijk worden niet zo maar gegevens verstrekt. Bij twijfel wordt er een beroep gedaan op een juridische medewerker. Een overzicht van interne gegevensverwerking is aanwezig, echter is deze niet meer in lijn met de huidige situatie. Er is geen beleid en/of register waarin beschreven staat welke data met welke externe partij (bewerkers) wordt gedeeld. Dit is een vereiste in de Algemene Verordening Gegevensbescherming. Het is derhalve niet duidelijk met welke partijen persoonsgegevens worden gedeeld en of deze partij(en) voldoen aan de wettelijke vereisten bij de gegevensverwerking.	Zonder beleid of richtlijn met betrekking tot het verstrekken van data aan derde partijen, bestaat de kans dat medewerker zelf gaan beoordelen of data gedeeld kan worden. Dit brengt het risico met zich mee dat er onrechtmatig persoonsgegevens worden gedeeld met derde partijen en er mogelijk een datalek plaatsvindt. Wanneer belangenafwegingen van medewerkers niet worden vastgelegd omtrent het delen van persoonsgegevens met derde partijen is het lastig om verantwoording af te leggen tegenover een toezichthouder.	Wij adviseren de Provincie Groningen: • Een verstrekkingenbeleid op te stellen en te implementeren inzake het delen van persoonsgegevens met derde partijen. • Periodiek te inventariseren of er (nieuwe) verwerkingen binnen de organisatie worden uitgevoerd die aan de Autoriteit Persoonsgegevens dienen te worden gemeld of dat bestaande meldingen kunnen worden ingetrokken. Deze eis vervalt bij de inwerkingtreding van de AVG wetgeving. Conform de AVG dient de organisatie een compleet en actueel register bij te houden van verwerkte persoonsgegevens.

BOzservaties, risico's en aanbevelingen (8/10)

	OBSERVATIES	RISICO'S	AANBEVELINGEN
7. VERWERKEN DOOR DERDEN	**M. Relaties met bewerkers** M et partijen waarvoor de Provincie taken uitvoert en die namens de Provincie werkzaamheden verrichten zijn op Prolander na, geen bewerkersovereenkomsten afgesloten. Het gaat hierbij onder andere om de Omgevingsdienst Groningen (ODG) welke namens de Provincie werkzaamheden verricht en Samenwerkingsverband Noord Nederland (SNN) en Regio Assen – Groningen waarvoor de Provincie werkzaamheden verricht. Tevens dienen bewerkersovereenkomsten te worden afgesloten met partijen waarbij door de Provincie, ICT-diensten worden ingekocht. Voorafgaand aan de gegevensverwerking bij nieuwe samenwerkingsverbanden dient er bij de selectie van een dergelijke partij te worden gekeken naar de volwassenheid van de interne beheersomgeving en certificeringen. In de praktijk hangt het delen van gegevens met deze partijen af van de individuele keuzes en afwegingen van de medewerker. Individuele medewerkers hebben de mogelijkheid om advies te vragen aan (privacy) juristen.	Als er data worden gedeeld met externe partijen, zonder dat daar juridische afspraken aan ten grondslag liggen kan de Provincie geen acties afdwingen bij deze externe partij met betrekking tot de mate van bescherming van persoonsgegevens of transparantie ten opzichte van een datalek. Zonder deze basis kan de Provincie mogelijk niet voldoen aan wettelijke vereisten zoals bijvoorbeeld de meldplicht datalekken, nu de Provincie verantwoordelijk blijft voor de persoonsgegevens. Wanneer de Provincie geen assessment uitvoert op nieuw te contracteren partijen die in aanraking komen met persoonsgegevens waarvoor de Provincie verantwoordelijk is, kan de Provincie niet garanderen dat er een adequaat niveau van bescherming wordt geboden voor de persoonsgegevens. Zonder bewerkersovereenkomsten en een register met daarin vastgelegd welke bewerkingen er worden gedaan door externe partijen, voldoet de Provincie niet aan toekomstige wettelijke vereisten.	Wij adviseren de Provincie Groningen: • Te inventariseren en vast te leggen met welke partijen er persoonsgegevens worden gedeeld en of er een adequate juridische basis is voor de Provincie om als verantwoordelijke voor deze gegevens aan wettelijke vereisten (bijv. de meldplicht datalekken) kunnen voldoen. Eventuele tekortkomingen dienen te worden aangevuld door aanvullende afspraken te maken met deze partijen in de vorm van bewerkersovereenkomsten. • Een proces in te richten dat waarborgt dat nieuw te contracteren partijen die als bewerker kunnen worden aangemerkt eerst door middel van een assessment worden getoetst. Met deze toetsing wordt beoogd om vast te stellen of een adequaat niveau van gegevensbescherming kan worden gewaarborgd. Certificeringen en standaarden kunnen daarbij een belangrijke rol spelen.
8. BEVEILIGING	**N. Logische toegangsbeveiliging** Het wachtwoordbeleid is in 2017 aangescherpt. Randvoorwaarden voor logische toegangsbeveiliging zijn vastgelegd in het informatiebeveiligingsbeleid. Systeemeigenaren zijn verantwoordelijk voor de toegangsbeveiliging van hun systeem. In de praktijk blijkt dat autorisatiebeheer (het toekennen, wijzigen en intrekken van rechten) tot systemen met persoonsgegevens, een aandachtspunt vormen. Het is hierbij niet inzichtelijk in welke applicaties, welke persoonsgegevens zijn opgeslagen en wie hier toe toegang heeft. Er worden slechts in beperkte mate periodieke controles uitgevoerd op toegekende rechten. Zie hier ook de bevinding ten aanzien van classificatie van gegevens en het beschikken over een compleet en actueel overzicht van data.	Ongeautoriseerd toegang tot persoonsgegevens levert mogelijk een onrechtmatige verwerking van persoonsgegevens op. Onvoldoende inzicht de opzet, bestaan of effectieve werking van autorisaties en logging brengt een verhoogt risico op ongeautoriseerde toegang. Daarnaast kan de Provincie niet aantonen aan een toezichthouder dat autorisaties goed ingeregeld zijn.	Wij adviseren de Provincie Groningen: • Binnen de organisatie meer aandacht te besteden in de opzet, bestaan en effectieve werking van logische toegangsbeveiliging. Het periodiek auditen van deze autorisaties is daarbij een harde vereiste.

BOosservaties, risico's en aanbevelingen (9/10)

8. BEVEILIGING - Technische beveiliging, waaronder netwerkbeveiliging en toegangscontrole, is niet geïmplementeerd en gehandhaafd worden.

OBSERVATIES	RISICO'S	AANBEVELINGEN
O. Gegevensdoorgifte Binnen de Provincie is geen formeel beleid opgesteld ten aanzien van het overdragen van persoonsgegevens. Gegevensdoorgifte gebeurt nog niet consistent middels beveiligde methoden. Data wordt in veel gevallen gedeeld met andere partijen via e-mail (onbeveiligd) gegevens worden alleen verstrekt, indien er een WOB-verzoek aan ten grondslag ligt. Bij twijfel wordt een leidinggevende geraadpleegd.	Het niet veilig of versleuteld versturen van persoonsgegevens verhoogt het risico op datalekken. Tevens voldoet het onversleuteld versturen van (gevoelige) persoonsgegevens niet aan de adequate mate van bescherming, zoals gesteld wordt in wettelijke Wbp- en AVG-vereisten.	Wij adviseren de Provincie Groningen: • Een proces in te richten om veilige danwel versleutelde data-overdracht te waarborgen. Het inrichten van een technisch platform om dit te faciliteren is daarbij een belangrijk vereiste. Het is belangrijk dat deze manier van data verzenden in het systeem van de medewerkers komt.
P. Werkplekken en gebruikersbeleid Medewerkers krijgen bij indiensttreding te maken met het informatiebeveiligingsbeleid. Tevens zijn er spelregels vastgesteld over het gebruik van social media, e-mail en internet. Uit de gesprekken is naar voren gekomen dat privacy nog niet echt leeft binnen de organisatie.	Het creëren van privacybewustzijnen het opstellen en implementeren van regels blijft ineffectief als er onvoldoende middelen beschikbaar worden gesteld om te kunnen voldoen aan verwachtingen van het management. Het naleven van bijvoorbeeld het clear-desk-beleid of het dossierbeleid is lastig wanneer er onvoldoende faciliteiten aanwezig zijn.	Wij adviseren de Provincie Groningen: • Voldoende faciliteiten te bieden aan medewerkers om compliant te zijn met zorgvuldigheidsregels omtrent gegevensbescherming.
Q. Fysieke beveiliging Fysieke toegangsbeveiliging is beperkt aanwezig. In sommige gebouwen wordt gewerkt met toegangspassen, maar de toegangscontrole is zeer beperkt. Recent is een zogenaamd 'mystery guest'-onderzoek uitgevoerd. Dit onderzoek bestond uit drie onderdelen, een bezoek aan provinciale locaties; een phising-mail; en een interne en externe hacktest. De bevindingen uit dit onderzoek zijn onder andere als input gebruikt om verbeteringen door te voeren op het gebied van fysieke toegangs-beveiliging (gebouw, netwerk, systemen, software) en om de bewustwording onder personeel te vergroten.	Een ineffectieve fysieke en logische toegangsbeveiliging verhoogt het risico op ongeautoriseerde toegang tot persoonsgegevens en eventuele datalekken. Bij een eventuele controle van een toezichthouder zal de Provincie moeilijk aan kunnen tonen dat zij voldoende maatregelen hebben genomen om persoonsgegevens een adequaat niveau van bescherming te kunnen bieden.	Wij adviseren de Provincie Groningen: • De resultaten van het 'mistery guest'-onderzoek ten aanzien van fysieke beveiliging op te volgen. Wij adviseren daarbij om de afwegingen en keuzes ten aanzien van de opvolging van de adviezen expliciet vast te leggen.

Observaties, risico's en aanbevelingen (1/1)

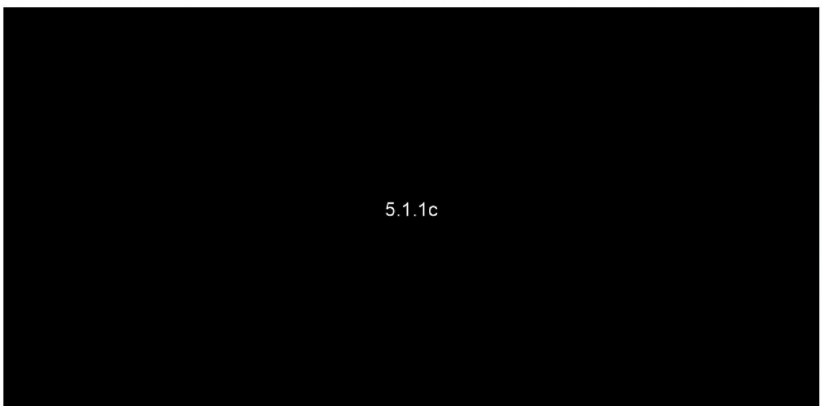
	OBSERVATIES	RISICO'S	AANBEVELINGEN
9. KWALITEIT - De kwaliteit van gegevens benaderd de noodzaak van het accuraat, compleet en up-to-date houden van persoonsgegevens.	**R. Datakwaliteit** EU Het correct verwerken van persoonsgegevens is een vereiste uit de Wbp en de AVG. Uit ons onderzoek is naar voren gekomen dat er binnen de Provincie Groningen op dit moment nog geen expliciet beleid is inzake de kwaliteit van gegevens en de kwaliteit van verwerkingsprocessen waarmee data wordt ingewonnen, verwerkt en beschikbaar wordt gesteld. Zo zijn rollen en verantwoordelijkheden ten aanzien van data kwaliteit zijn nog niet expliciet belegd binnen de organisatie, zijn in beperkte mate standaard invoerprotocollen ingericht om consistente invoer te garanderen en ontbreken er periodieke audits om de data kwaliteit te waarborgen. De Provincie heeft bovenstaande onderkend en heeft reeds een plan van aanpak in concept opgesteld voor het project DOO-Datakwaliteit. Dit project heeft als doelen: het onderwerp data kwaliteit onder de aandacht te brengen; de kwaliteit van brongegevens inzichtelijk te maken; het verbeteren van data kwaliteit in bronsystemen; en inzicht te geven in het verbeterproces. Het project valt onder het programma "Data huishouding op orde".	Onduidelijk eigenaarschap voor datakwaliteit kan resulteren in inconsistente vastleggingen of verkeerde interpretaties van data. Het correct verwerken van persoonsgegevens is een vereiste uit de Wbp en de AVG.	Wij adviseren de Provincie Groningen: • Het reeds opgesteide conceptplan van aanpak voor het project DOO-Datakwaliteit definitief te maken en te starten met de realisatie van de projectdoelen.
10. TOEZICHT EN HANDHAVING - Naleving van beleid en procedures dient te worden gemonitord.	**S. Toetsing en handhaving** Binnen de Provincie worden er verscheidene audits, self-assessments en kwaliteitscontroles uitgevoerd op verschillende onderwerpen die grenzen aan data privacy, zoals informatie-beveiliging, penetratietesten en een mystery guest-onderzoek. Er vindt echter geen expliciete toetsing en handhaving plaats ten aanzien van privacy. Zo hebben wij vastgesteld dat er nog geen PDCA-cyclus is ingericht ten aanzien van privacy.	Wanneer een datalek plaatsvindt als gevolg van tekort-komingen in systemen of processen, weegt dit extra zwaar wanneer dit al eerder is blootgelegd door een audit. Het niet adequaat opvolgen van (kritische) bevindingen die een impact hebben op de mate van bescherming van persoons-gegevens zal zwaar worden aangerekend door de Autoriteit Persoonsgegevens. Het niet opvolgen van auditbevindingen ondermijnt de (onafhankelijke) positie van de auditors. Wanneer niet voldoende duidelijk is wie er verantwoordelijk is voor het opvolgen van acties uit auditbevindingen, zullen deze langer blijven liggen.	Wij adviseren de Provincie Groningen: • Een jaarlijkse PDCA-cyclus in te richten in het kader van privacy.

KPMG

Bijlagen

Bijlage A – KPMG privacymanagementraamwerk
Bijlage B – Privacy principes
Bijlage C – Wettelijke grondslag
Bijlage D – Privacy roadmap
Bijlage E – Budgetindicatie privacy-implementatie
Bijlage F – Geïnterviewde personen
Bijlage G – Bestudeerde documenten

Bijlage A - KPMG PRIVACY MANAGEMENT FRAMEWERK



Bijlage B - Privacyprincipes

Door middel van de privacynulmeting zijn de eerste stappen gezet voor uw weg naar een beter beheerste privacyomgeving. Samen met u en uw collega's is een initiële privacynulmeting uitgevoerd die gebaseerd is op de tien privacy grondbeginselen zoals door KPMG gedefinieerd. Deze tien grondbeginselen zijn op hun beurt gebaseerd op bestaande good practices en bestaande en aankomende wet- en regelgeving.

1. MANAGEMENT – Management moet betrokken zijn bij privacyprocessen, en privacy moet opgenomen zijn in het beleid van de organisatie.
2. TRANSPARANTIE – De organisatie heeft de verplichting om betrokkenen te informeren over hoe gegevens verzameld en verwerkt worden.
3. KEUZE EN TOESTEMMING – Individuen moeten de mogelijkheid hebben om te kiezen of en welke gegevens worden verzameld en verwerkt.
4. DOELBINDING – Gegevens kunnen niet onbeperkt worden verzameld en verwerkt. Gegevens mogen niet worden verzameld en verwerkt zonder een precieze doelomschrijving.
5. RECHTMATIGE GRONDSLAG – Een organisatie moet weten hoe het gegevens verzamelt, hoe veel, en op basis van welke grondslag.
6. RECHT VAN BETROKKENEN – Personen over wie gegevens worden verzameld hebben o.a. het recht om hun gegevens in te zien en het recht om vergeten te worden.
7. VERWERKING DOOR EEN BEWERKER – Persoonsgegevens kunnen alleen worden verstrekt aan derden wanneer specifieke overeenkomsten zijn aangegaan en hierop wordt toegezien.
8. BEVEILIGING – Technische beveiliging, waaronder netwerkbeveiliging en toegangscontrole, moet geïmplementeerd en geformaliseerd worden.
9. KWALITEIT – De kwaliteit van gegevens benadrukt de noodzaak van het accuraat, compleet en up-to-date houden van persoonsgegevens.
10. TOEZICHT EN HANDHAVING – Naleving van privacybeleid en -procedures dient te worden gemonitord. Werknemers die persoonsgegevens verwerken moeten opgeleid worden en in staat zijn om klachten of issues met betrekking tot privacy op een juiste wijze af te handelen.

Bijlage C – Wettelijke grondslag (12)

Privacyprincipes	Wetsartikelen AVG	Wettelijke vereisten op hoofdlijnen
1. Management	Art. 35, 36	Wanneer er nieuw soortige verwerkingen of technieken om persoonsgegevens te verwerken plaatsvinden, dient de verantwoordelijke een privacy impact assessment uit te voeren (PIA).
	Art. 37, 38, 39	Aanwijzen en positionering van een functionaris gegevensbescherming
2. Transparantie	Art. 12	Rechten van betrokkenen dienen op transparante en beknopte wijze, in een toegankelijke vorm, in duidelijke en eenvoudige taal gecommuniceerd te worden naar betrokkene.
	Art. 13, 14	De verantwoordelijke informeert de betrokkene over waarvoor en hoe zijn persoonsgegevens worden gebruikt.
3. Keuze en toestemming	Art. 7	Wanneer verwerking op toestemming van betrokkene berust, moet dit aantoonbaar zijn.
	Art. 18	Recht op beperking van de verwerking.
	Art. 4	Toestemming moet ondubbelzinnig zijn en voldoen aan de vereisten die worden geschetst in art. 4 en in overweging 32 van de verordening.
4. Doelbinding	Art. 6	Er dient een rechtmatige grondslag te zijn voor de verzameling van persoonsgegevens.
	Art. 9	Het verwerken van bijzondere persoonsgegevens is aan zwaardere eisen onderhevig. Er dient te worden getoetst of aan deze voorwaarden wordt voldaan wanneer er bijzondere persoonsgegevens worden verzameld.
	Art. 8	Extra zware vereisten voor de verwerking van persoonsgegevens van kinderen
5. Rechtmatige grondslag	Art. 6	Er dient een rechtmatige grondslag te zijn voor de verwerking van persoonsgegevens. De gegevens mogen alleen worden gebruikt voor het daarvoor bestemde doel.
	Art. 9	Het verwerken van bijzondere persoonsgegevens is aan zwaardere eisen onderhevig. Er dient te worden getoetst of aan deze voorwaarden wordt voldaan wanneer er bijzondere persoonsgegevens worden verwerkt.

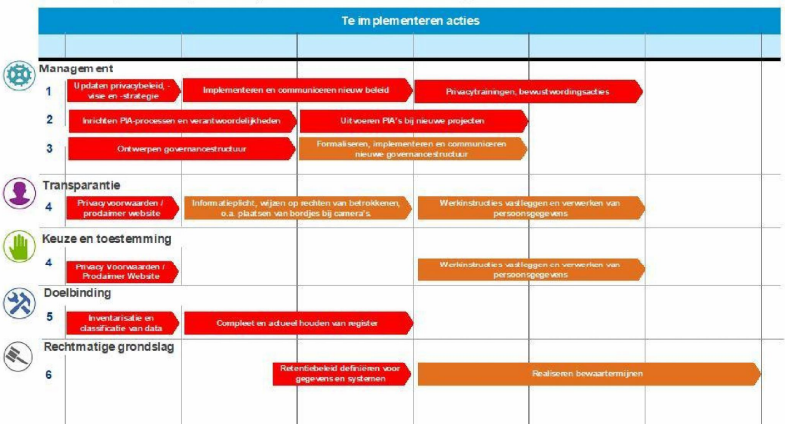
Bijlage G – Wettelijke grondslag (2/2)

Privacyprincipes	Wetsartikelen AVG	Wettelijke vereisten op hoofdlijnen
6. Rechten betrokkenen	Art. 15, 19	Recht op inzage van de betrokkene over zijn of haar persoonsgegevens.
	Art. 16, 19	Recht op correctie/ rectificatie van persoonsgegevens.
	Art. 17, 19	Recht op gegevensuitwissing (vergetelheid).
	Art. 18, 19	Recht op beperking van de verwerking.
	Art. 20	Recht op overdraagbaarheid van gegevens (dataportabiliteit)
	Art. 21	Recht van bezwaar tegen de verwerking van persoonsgegevens.
7. Verwerking door derde partijen	Art. 28 lid 1	Verwerkers dienen een adequaat niveau van gegevensbescherming te kunnen garanderen.
	Art. 28 lid 3	Er dient een overeenkomst of andere rechtshandeling geregeld te zijn tussen verwerker en verantwoordelijke.
	Art. 30	Verantwoordelijke legt een register van verwerkersactiviteiten vast.
8. Beveiliging	Art. 25, 32	Verantwoordelijke treft passende technische en organisatorische maatregelen om ervoor te zorgen dat alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel.
	Art. 33	De verantwoordelijk is verplicht te melden aan de toezichthoudende autoriteit indien een inbreuk in verband met persoonsgegevens heeft plaatsgevonden.
	Art. 34	Deze mededeling dienen onder bepaalde voorwaarden ook te worden gedaan aan alle betrokkenen.
9. Kwaliteit	Art. 5 lid 1 sub c	De verwerking van gegevens moet juist en geactualiseerd zijn.
10. Toezicht en handhaving	Art. 5 lid 2	Verantwoordelijke moet aantoonbaar kunnen maken dat ze de algemene beginselen van de verwerking van persoonsgegevens zoals bepaald in art. 5 lid 1 naleven.

Data privacy volwassenheidsmeting

Bijlage D - Privacyroadmap (1/2)

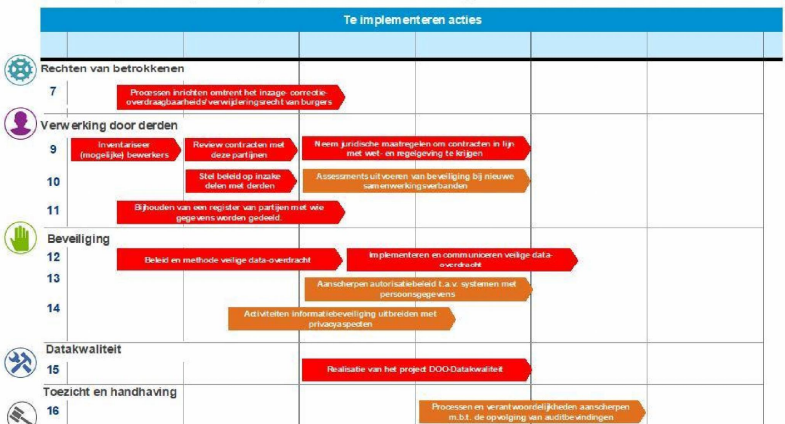
Onderstaande acties, uitgezet in de volgorde van implementatie, stellen de Provincie Groningen in staat te voldoen aan de AVG.



Data privacy volwassenheidsmeting

Bijlage D - Privacyroadmap (2/2)

Onderstaande acties, uitgezet in de volgorde van implementatie, stellen de Provincie Groningen in staat te voldoen aan de AVG.



Bijlage E – Budgetindicatie privacy-implementatie (13)

ID	Aanbeveling	Op te leveren product	Budget-indicatie[1]	Juridische grond
1	Een privacygovernance en -accountabilitystructuur op te stellen en te implementeren met daarin centraal een Functionaris Gegevensbescherming met een coördinerende rol (N.B. niet noodzakelijkerwijs een full-time rol).	• Formaliseren governancestructuur • Aanstellen Functionaris Gegevens-bescherming • Formaliseren centrale privacy-organisatie • Implementeren en communiceren van de privacy-organisatiestructuur	€€€	Art. 37, 38, 39 AVG
2	Een compleet privacybeleid en -strategie op te stellen en te zorgen voor implementatie door privacytrainingen en bewustwordingscampagnes zodat het beleid gaat leven in de organisatie. Voorbeelden van bewustzijnsacties zijn communicatie via intranet, e-mail en posters, formulieren en verklaringen bij indiensttreding.	• Privacystrategie • Privacybeleid • Bewustwordingscampagne	€€ - €€€	Art. 39
3	Richtlijnen en template op te stellen en te implementeren voor het uitvoeren van PIA's en risico-analyses voorafgaand aan nieuwe projecten en gegevensverzamelingen.	• Vastleggen proces voor het uitvoeren van PIA's • Vastleggen rollen en verantwoordelijk-heden bij het uitvoeren van PIA's • PIA-template, checklijsten	€	Art. 35, 36 AVG
4	In lijn met de verplichtingen vanuit de AVG een actueel en compleet register op te stellen met daarin een overzicht van alle verzamelde persoonsgegevens, het doel waarvoor ze worden verwerkt en wat er met die gegevens gebeurt.	• Een compleet register met daarin een overzicht van alle verzamelde persoonsgegevens, het doel waarvoor ze worden verwerkt en wat er met die gegevens gebeurt.	€€€	
5	Bewerkersovereenkomsten afsluiten met partijen die namens de Provincie werkzaamheden verrichten of waarvoor de Provincie taken uitvoert. Het gaat hierbij onder andere om de Omgevingsdienst Groningen (ODG) welke namens de Provincie werkzaamheden verricht en Samenwerkingsverband Noord Nederland (SNN) en Regio Assen – Groningen waarvoor de Provincie werkzaamheden verricht. Tevens dienen bewerkersovereenkomsten te worden afgesloten met partijen waarbij door de Provincie, ICT-diensten worden ingekocht.	• Aanpassingen/verrijking contracten met derde partijen.	€	Art. 28, 30 AVG

[1] Een toelichting op de afgegeven budgetindicatie is opgenomen op pagina 30.

Bijlage E – Budgetindicatie privacy-implementatie (2/3)

ID	Aanbeveling	Op te leveren product	Budget-indicatie[1]	Juridische grond
6	Een register op te stellen om inzichtelijk te maken met welke partijen de Provincie (persoons)gegevens uitwisselt.	• Register van verwerkingsactiviteiten cf. AVG • Aanpassingen/verrijking contracten met derde partijen.	€€	Art. 28, 30 AVG
7	Het reeds opgestelde conceptplan van aanpak voor het project DOO-Datakwaliteit definitief te maken en te starten met de realisatie van de projectdoelen.	• Projectplan DOO-Datakwaliteit	€€	Art. 47 AVG
8	Een beleid en methode voor de beveiligde overdracht van vertrouwelijke gegevens op te stellen en te implementeren.	• Richtlijn inzake datatransfer • Opzetten beveiligde dataportaal	€€	Art. 32 AVG
9	Richtlijnen en procedures op te stellen en te implementeren ten aanzien van het op transparante wijze informeren en vastleggen van gegevens; vragen om toestemming; het bewaren, schonen en archiveren van (persoons)gegevens; en het inzage-, correctie-, overdraagbaarheids- en verwijderingsrecht.	• Richtlijnen verzameling persoons-gegevens • Richtlijnen dataretentie • Implementeren oplossing voor het schonen en archiveren van (persoons)gegevens	€€	Art. 6, 8, 9 AVG
10	Een verstrekkingenbeleid op te stellen en te implementeren waarin richtlijnen staan beschreven voor het uitwisselen van (persoons)gegevens met derde partijen.	• Verstrekkingenbeleid	€	Art. 28 AVG

Bijlage E – Budgetindicatie privacy-implementatie (3/3)

Budgetindicatie	Schatting benodigd aantal dagen	Toelichting
€	1 – 5	Tijd nodig om activiteit te realiseren of deliverable te maken is beperkt. Betreft voornamelijk het opstellen van een beleids- of procedure document, werkinstructies of richtlijnen, het definiëren en toewijzen van taken en verantwoordelijkheden, of bijvoorbeeld het testen van het privacy incident respons plan. De verwachte tijd die nodig is om de activiteit af te ronden is maximaal 40 uur. Activiteiten kunnen veelal door medewerkers van de gemeente zelf worden uitgevoerd. Geen aanvullende, externe expertise noodzakelijk.
€€	5 – 15	Er is een gemiddelde inspanning nodig om de activiteit te realiseren. Betreft bijvoorbeeld het uitwerken van een overkoepelend privacybeleidsdocument en de communicatie daarvan binnen de organisatie. Maar omvat bijvoorbeeld ook het inventariseren van alle verwerkingen van persoonsgegevens, inclusief de contractuele afspraken met eventuele bewerkers (derde partijen). De verwachte tijd die nodig is om de activiteit af te ronden is maximaal 15 dagen per gemeentelijk domein. Activiteiten kunnen veelal door medewerkers van de gemeente zelf worden uitgevoerd. Mogelijk moet aanvullende (juridische) expertise worden ingehuurd.
€€€	15+	Benodigde inspanning om activiteit te realiseren of deliverable op te stellen (en te laten accorderen) is aanzienlijk. Het optuigen van een (klein) project om de activiteit te realiseren is wenselijk. Gaat gepaard met aanvullende investeringen, zoals het creëren van één of meerdere nieuwe functies binnen de organisatie (o.a. DPO) of bijvoorbeeld het aanschaffen en de inrichting van tooling om logische toegangsbeveiliging op een hoger plan te brengen. Activiteiten kunnen grotendeels door medewerkers van de gemeente worden uitgevoerd, maar naar verwachting dient ook externe expertise of aanvullende capaciteit te worden ingehuurd om het project te realiseren.

Bijlage F – Geïnterviewde personen (12)

Interviewoverzicht

We hebben gesproken met de volgende medewerkers van de volgende organisatieonderdelen:

Organisatieonderdeel	Functie
5.1.2e	Concernjurist
5.1.2e 5.1.2e	Data-analist
5.1.2e 5.1.2e	Functioneel Beheerder
I/ 5.1.2e	Architect
5.1.2e 5.1.2e	Security Officer
5.1.2e 5.1.2e	Beleidsmedewerker DIV
I/ 5.1.2e	Beleidsmedewerker DIV
5.1.2e 5.1.2e	Landschapsbeheer
I/ 5.1.2e	Projectmanager ECP
5.1.2e 5.1.2e	Concernfunctionaris informatiebeveiliging
I/ 5.1.2e	HRM Adviseur
5.1.2e 5.1.2e	Medewerker P&O

Bijlage F – Geïnterviewde personen (22)

Interviewoverview

We hebben gesproken met de volgende medewerkers van de volgende organisatieonderdelen:

Organisatieonderdeel	Functie
5.1.2G 5.1.2G	Applicatiebeheerder Unit 4 Financials
5.1.2G 5.1.2G	Afdeling BJC
5.1.2G 5.1.2G	Projectleider KWI
5.1.2G 5.1.2G	Ondersteunend beleidsmedewerker

Bijlage G - Bestudeerde documenten (12)

We hebben de volgende documenten ontvangen en beoordeeld.

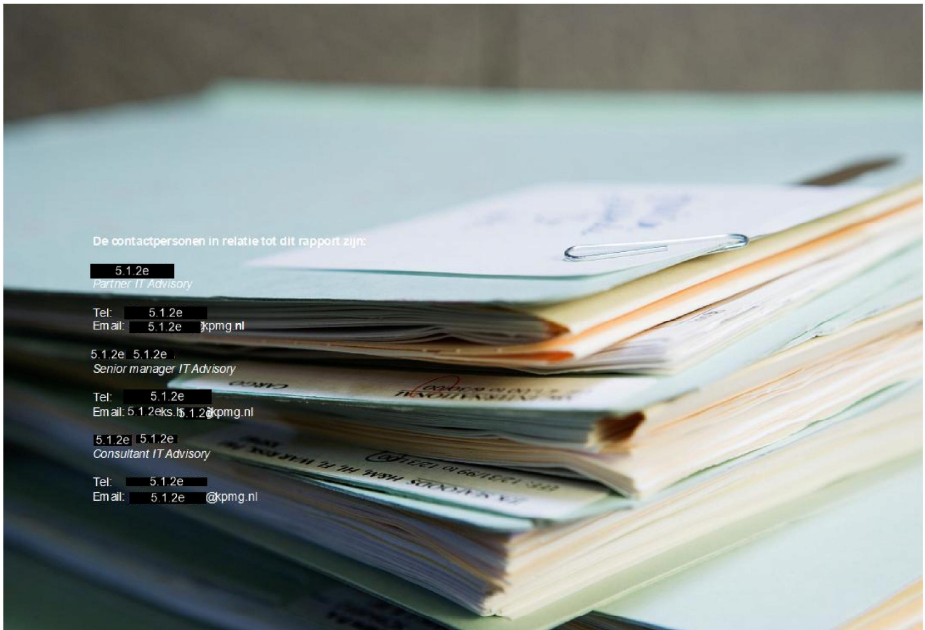
Documentnaam
Protocol Wbp en meldplicht datalekken
Privacy kader Provincie Groningen
Memo Privacy regelgeving
Memo WOB-verzoeken en WhatsApp- en sms-berichten
Gedragscode internet en e-mailgebruik
Richtlijnen gebruik sociale media binnen de Provincie Groningen
Meldplicht datalekken
Beleid niet persoonsgebonden accounts.doc
Besluit informatieclassificatie.pdf
Bijlage 1 – Implementatieadvies mvbi v1.4.doc
Bijlage 1 – Informatiebeveiliging Provincie Groningen, het kader v1.1.docx
Bijlage 1 – LogischeToegangsbeveiliging_v1.1.docx
Bijlage 2 – Proces stamgegevens_v1.0.docx
Concept protocol personeelsdossiers_versie 5 febr 2016.docx
IB-classificatie_1.2.xltx
Intake_Logische_Toegangsbeveiliging_v0.1.docx
lege voorbeeld relatiematrix.xls
Organisatie roept medewerkers op lekken in beveiliging te melden 1.0.docx
Procedure toegang tot informatie.pdf
Proclaimer website.pdf
Protocol onderzoek integriteitschendingen instem U-09-024.pdf
Rapportage_RODIN_Groningen_20150511.pdf
Wachtwoordenbeleid Provincie Groningen v2017.doc
Werkinstructie informatieclassificatie applicaties.docx

Bijlage G Bestudeerde documenten (22)

We hebben de volgende documenten ontvangen en beoordeeld:

Documentnaam
161031 Memo GS Wob Whatsapp.pdf
Bewerkersovereenkomsten Prolander.msg
def. handvest 9 12 2014.docx
Digitale_wegwijzer_dienstverlening .pdf
Intake_Logische_Toegangsbeveiliging_v0.3.docx
Introductiefolder_FZ.pdf
Normenboekje integriteit 2014.pdf
Richtlijnen gebruik sociale media binnen de Provincie.pdf
2015-04-16 Persbericht Provincie gaat beelden brugbediening bewaren.doc
bevestiging melding bij CBP tevens goedkeuring logging 06-11-2014.pdf
brief aan operators melding start logging.pdf
Communicatieplan logging camerabeelden brugbediening.doc
ingevulde en getekende melding bij cbp logging data brug en sluisbediening.pdf
melding start logging camerabeelden en marifoonverkeer.msg
modelbewerkersovereenkomstarvodi2014 RWS-PG.docx
notitie logging data audio en video vastgestelde versie.pdf
Privacyreglement verkeersregistratiesystemen Rijkswaterstaat_tcm174-280516 juli 2003.pdf
Provincie Groningen Provincie gaat camerabeelden brugbediening bewaren.htm
schuttevaer 9mei2015 stukje logging.pdf
Privacykader Provincie Groningen.pdf

19434441



0000000035

KPMG

KPMG op sociale media

Download on the App Store

KPMG app