



Jaarverslag *toezicht*
Functionaris Gegevens-
bescherming (FG)
Provincie Limburg
2021

Jaarverslag *toezicht* Functionaris Gegevens- bescherming (FG) Provincie Limburg 2021

Inhoud

Managementsamenvatting en aanbevelingen FG	4
1. Inleiding	7
1.1. Privacybeleid	
1.2. Functionaris Gegevensbescherming (FG)	
1.3. Verantwoording	
1.4. Rapportage FG	
2. Overview: wat is er gedaan?	10
2.1. Bewustwording en organisatie	
2.2. Beleid en governance	
2.3. Toetsing en auditing	
2.4. Concernbreed beheer persoonsgegevens	
2.5. Verwerkingsregister	
2.6. Privacy-by-design	
2.7. Privacy in data innovatie	
3. Status thema's FG Toezichtplan	14
3.1. Bewaren van persoonsgegevens	
3.2. Intern toezicht	
3.3. Beveiligen van de verwerking van persoonsgegevens	
3.4. Bewustwording	
3.5. Implementeren privacy-by-design	
4. Trends & ontwikkelingen	16
4.1. Samenwerking in informatieketens	
4.2. Gebruik social media	

Managementsamenvatting en aanbevelingen FG

Privacy onderdeel	Conclusies en aanbevelingen	Score
Bewustwording en organisatie	<p>Bewustwording in de organisatie van privacyrisico's in de verwerking van persoonsgegevens van burgers is in redelijk tot voldoende mate aanwezig.</p> <p>Bewustwording van privacyrisico's in de verwerking van persoonsgegevens van medewerkers vormt een aandachtspunt.</p> <p>Bewustwording van privacy aspecten binnen PS (griffie) dient te worden versterkt.</p> <p>Aanbeveling is om de verschillen in bewustzijn tussen clusters en provinciale organen te adresseren door, daar waar nodig, de rol van de privacy ambassadeurs sterker te positioneren.</p>	
Beleid en governance	<p>Het Privacybeleid Provincie Limburg dateert uit 2018. Met de komst van de Wet Open Overheid in 2022 wordt de druk op transparantie opgevoerd. De privacy van medewerkers kan hierbij ook in het geding komen.</p> <p>Aanbevelenswaardig is een evaluatie van het huidige privacybeleid binnen de interne organisatie. Ook te bezien in de context van de aanbevelingen gedaan door de enquêtecommissie om informatie langer te bewaren.</p>	
Toetsing en auditing	<p>Toetsing en auditing binnen het privacydomein vinden voornamelijk plaats met het instrument DPIA. In 2021 zijn meerdere DPIA's uitgevoerd waarmee de voornaamste privacyrisico's zijn geduid.</p> <p>Aanbevelenswaardig is om te verankeren dat, na een DPIA, in een later stadium wordt getoetst of voorgestelde mitigerende maatregelen ook daadwerkelijk zijn geïmplementeerd (toepassen PDCA cyclus).</p> <p>Bij de Provincie Limburg zijn zogenoemde buitengewone opsporingsambtenaren (boa's) werkzaam die persoonsgegevens verwerken onder het regime van de Wet politiegegevens (WPG). Hiervoor dient nog een FG te worden aangewezen in het kader van het toezicht op de WPG.</p>	

Concernbreed beheer persoonsgegevens	De informatiehuishouding binnen de Provincie Limburg is complex, omvangrijk en volledig digitaal. Geconstateerd is dat er teveel persoonsgegevens worden bewaard die geen onderdeel zijn van het formele informatie- en archiefbeheer. Het goed beheersen van privacyrisico's is onlosmakelijk verbonden met een integraal informatie- en archiefbeheer, waarmee de gehele informatiehuishouding in control wordt gebracht en de geldige vernietigings- en bewaartermijnen worden gehanteerd.	
Verwerkingen persoonsgegevens	Het verwerkingsregister is volledig en actueel. Aanbevelenswaardig om de vernietigings- en bewaartermijnen met de Provisa IPO selectielijst te synchroniseren.	
Privacy-by-design	In de huidige digitale informatiehuishouding van de Provincie Limburg is het belangrijk om in de ontwerpfase van projecten, programma's, samenwerkingsverbanden en werkprocessen, de privacy- en informatiebeveiligingsrisico's in beeld te brengen en te mitigeren reeds voor de implementatiefase. Een belangrijke stap hiervoor is gezet met de inrichting van het CIO overleg. De projectbrieven die worden geagendeerd in het CIO overleg, krijgen een pre-check in het Privacy en Informatiebeveiligingsteam (PIT), waarbij in een vroegtijdig stadium privacy risico's worden herkend en gerapporteerd aan het CIO overleg.	
Privacy in data innovatie	In het nieuwe Strategisch Informatiebeleid Limburg (SIBL 2021-2024) wordt prioriteit gegeven aan innovatieve ontwikkelingen die helpen maatschappelijke	

	opgaven beter en sneller te realiseren. Vanuit een wettelijk en ethisch perspectief is het belangrijk om te monitoren dat in de keuze- en ontwerpfase van dit soort innovaties (bijv. toepassing algoritmen) de privacyrisico's in kaart worden gebracht. Deze monitor- en toetsingsfunctie dient in 2022 verder te worden geborgd in de governancestructuur.	
--	---	--

1. Inleiding

1.1. Privacybeleid

Binnen het collegeprogramma Vernieuwend verbinden 2019-2023 is privacy expliciet opgenomen in de uitgangspunten die betrekking hebben op verbindende bestuurlijke vernieuwing als ambitie:

Privacy is een groot goed. Wij respecteren de persoonlijke levenssfeer van de inwoners van Limburg. De Provincie Limburg voert een privacy-beleid dat voldoet aan de relevante, actuele wetgeving, jurisprudentie en ontwikkelingen.

En (impliciet):

Wij werken open en transparant. Wij maken een eigen, autonome, Limburgse afweging en laten ons primair leiden door hetgeen waarop wij als Limburgs provinciebestuur invloed kunnen uitoefenen in het belang van Limburg. Gedeputeerde Staten leggen hierover verantwoording af aan Provinciale Staten. Uitgangspunt is dat alle informatie openbaar is voor iedereen die hiernaar vraagt, tenzij er relevante redenen zijn om de (bijvoorbeeld bedrijfsgevoelige) informatie vertrouwelijk te houden.

In 2018 is het Privacybeleid Provincie Limburg vastgesteld op welke wijze de Provincie Limburg zou moeten voldoen aan de Algemene verordening gegevensbescherming (AVG). In de Programmabegroting 2022 is opgenomen dat de Provincie Limburg een privacybeleid voert waarin wordt uitgesproken dat een adequaat niveau van privacy- en informatiebeveiliging wordt nagestreefd waarbij, voor het reduceren van risico's, voortdurend afwegingen worden gemaakt om de juiste balans te vinden tussen relevante wetgeving, de taakstelling van de organisatie, een praktische manier van werken en de persoonlijke levenssfeer van betrokkenen.

Het Privacybeleid kenmerkt zich door een cyclisch proces dat - in theorie - voldoet aan een gestandaardiseerd patroon met daarin de elementen: voorbereiden, ontwikkelen, goedkeuren, communiceren, uitvoeren, implementeren en evalueren. Dit houdt in dat er sprake is van een terugkoppelmechanisme waarbij - door inzicht in de uitvoering - het beleid kan worden bijgesteld en gecorrigeerd.

1.2. Functionaris Gegevensbescherming (FG)

De Functionaris voor de Gegevensbescherming (FG) fungeert in het cyclisch proces als interne privacy toezichthouder en rapporteert rechtstreeks aan de Algemeen directeur/secretaris over zijn werkzaamheden. De huidige FG is aangewezen en voor de werkzaamheden is 0,2 fte gereserveerd. De FG rol is belegd in de functie van provinciearchivaris (1fte).

De volgende rollen inclusief verantwoordelijkheden zijn vastgelegd in het Privacybeleid:

Functie/rol	Taken/verantwoordelijkheid
Gedeputeerde Staten	Eindverantwoordelijk voor het privacybeleid en het waarborgen van de privacy van betrokkenen.
Secretaris/algemeen directeur	Verantwoordelijk voor kaderstelling en sturing met betrekking tot het privacybeleid.
Cluster-/project/-programmamanagers	Uitvoering en controle op naleving privacybeleid
Functionaris Gegevensbescherming	Controle op naleving en advies op het gebied van privacy.
Het privacy- en informatiebeveiligingsteam (PIT)	Ondersteuning en advisering bestuur, de clusterambassadeurs privacy en het management bij de op het terrein van bescherming van persoonsgegevens en uitvoering van het Provinciale privacybeleid.
Privacy coördinator	Advisering over en implementatie privacybeleid en -wetgeving. Actueel houden register van verwerkingsactiviteiten.
Clusterambassadeurs privacy	Informatieverstrekking, bewustwording en cluster specifieke privacy taken

1.3. Verantwoording

Het gebruikte toetsingskader wordt gevormd door de AVG en alle relevante wet- en regelgeving, betrekking hebbende op het privacydomein. Op basis van verzamelde documentatie als beleidsnotities, rapportages, verbeterplannen, visiedocumenten zijn gesprekken binnen de ambtelijke organisatie gevoerd. Uit de gesprekken kwam een beeld van de huidige stand van zaken naar voren. De voorliggende rapportage is compact, dashboardachtig van opzet. Hiermee ontstaat een logisch en overzichtelijk geheel dat enerzijds monitoring op hoofdlijnen en anderzijds de vergelijkbaarheid van opeenvolgende rapportages dient te vergemakkelijken.

1.4. Rapportage FG

Deze rapportage heeft als doel inzicht te bieden in de voortgang van het FG toezichtplan en de opbouw van het privacy risk control framework van de Provincie. Hiervoor wordt tevens het Privacy Volwassenheidsmodel gehanteerd dat vijf volwassenheidsniveaus kent. Deze halfjaarlijkse rapportages dragen bij om naar het gewenste volwassenheidsniveau 3 op het gebied van privacy te groeien. Op niveau 3 verwerkt de Provincie persoonsgegevens, waarbij keuzes zijn en worden gemaakt op basis van operationeel beleid, richtlijnen en werkinstructies op organisatieniveau. Het beleid is formeel vastgesteld op organisatieniveau en daarmee bekrachtigd als beleid voor de gehele organisatie. De vereisten vanuit de organisatie zijn ook vertaald naar de inrichting van de context, de systemen en de beheerprocessen. De organisatie leert concernbreed, omdat er een systematische samenhang bestaat tussen de uitvoerende onderdelen, beleidsonderdelen en controleonderdelen op zowel clusterniveau als bedrijfsniveau. Er is structurele evaluatie van en rapportage over de rechtmatige gegevensverwerking (en beveiliging van persoonsgegevens) naar de algemeen directeur, wat tot aanpassing van het organisatiebrede beleid kan leiden. Er bestaat sturing op de naleving van het beleid, richtlijnen en (werk)instructies. In tegenstelling tot niveau 2 wordt de sturing afgestemd met de bestuurder. De bestuurder is betrokken bij de handhaving van het beleid en de uitvoering, waarbij gerapporteerd wordt ondersteund door controlemiddelen en informatie. Dit leidt tot een lerend proces op zowel clusterniveau als op organisatieniveau.

Deze rapportage kent de volgende opbouw:

- globaal overzicht van de werkzaamheden op het gebied van privacy;
- status thema's FG toezichtplan;

- trends & ontwikkelingen;

2. Overview: wat is er gedaan?

Werken aan privacy is een doorlopend en structureel proces. De monitoring en sturing, op basis van het vastgestelde privacy beleidskader, is binnen de Provincie Limburg belegd bij een aantal functionarissen. Samen vormen deze het Privacy Impact Team (PIT). Binnen dit gremium wordt op tweewekelijkse basis de voortgang gemonitord op basis van een actielijst en jaarplanning. De actielijst fungeert als verbeterplan voor de aandachtspunten uit de rapportages van de FG. Hieronder wordt per privacy onderdeel een overzicht gegeven in hoeverre de gestelde doelstellingen in 2021 zijn bereikt.

2.1. Bewustwording en organisatie

In de organisatie wordt op dagelijkse basis gewerkt met persoonsgegevens. Dat betekent dat privacy structureel onderdeel uitmaakt van de werkprocessen. Vóór de komst van de AVG in 2018, was de bewustwordingsgraad van privacyrisico's in overheidsorganisaties laag. Sinds de vaststelling van het provinciaal Privacybeleid in 2018 wordt proactief gewerkt aan voorlichting en bewustwording op het gebied van privacy.

Bewustwording en organisatie	Planning	Status maart 2022
Ronde 'Are you secure'	Q1 2021	Afgerond en nieuwe ronde is momenteel bezig
Bewustwording Sharepoint dossiers vertrouwelijk/bedrijfsvertrouwelijk	Q2 2021	Afgerond
Bijeenkomst organiseren clusterambassadeurs	Q2 2021	Afgerond (digitaal ivm Corona)
Voorlichting AVG	Doorlopend	Doorlopend
Privacy onderdeel in verplicht introductieprogramma	4x per jaar in 2021	Afgerond (digitaal ivm Corona)
Privacy onderdeel in module digitale ontwikkelingen Limburg Academie	Q3 2020	Niet gerealiseerd
Communicatie over Privacybeleid	Doorlopend	Doorlopend
Intern privacybeleid actualiseren en aanvullen (instemming OR)	Q4 2021	Vertraagd naar Q2 2022

2.2. Beleid en governance

In 2018 is het Privacybeleid door GS vastgesteld, waarmee de kaders van uitvoering helder zijn. Het Privacybeleid dient echter uitgewerkt te worden in de praktijk van alledag, zodat de werkprocessen zodanig ingericht worden dat alle privacyrisico's in beeld zijn en op een adequate wijze worden beheerst. Hiervoor zijn diverse protocollen op werkprocesniveau opgesteld, afgestemd met de OR en geïmplementeerd. Nu de kaders zijn uitgewerkt, is het zaak om de komende periode te focussen op de governancestructuur. Het is belangrijk dat structureel wordt gemonitord in welke mate de informatieprocessen ook daadwerkelijk 'in control' zijn op het gebied van privacy. De volgende logische stap in het verhogen van het volwassenheidsniveau is de implementatie van de PDCA cyclus en het risicomanagementproces. Vanaf 2021 fungeert het PIT team als toetsteam van de SIBL projectbrieven op het gebied van privacy en archivering. Vanuit het PIT wordt het CIO overleg geadviseerd.

Beleid en governance	Planning	Status Maart 2022
PDCA cyclus inclusief risicomanagementproces privacy: implementatie [REDACTED]	Q4 2021	Vertraagd naar 2022
Intern privacyreglement actualiseren en aanvullen (instemming OR)	Q3 2021	Vertraagd naar 2022
Verwerkingsovereenkomsten Provincie Limburg en RUD Zuid-Limburg (bijlage dienstverleningsovereenkomst 2021 ev)	Q1 2021	Gereed
Dienstauto protocol	Q1 2020	Gereed (ingebracht OR 2021)
Projectbrieven toetsing door PIT team	Q4 2021	Gereed
Tools O&I; monitoring en logging acties personeel in kaart brengen	Q1 2021	Gereed

2.3. Toetsing en auditing

Een DPIA audit wordt uitgevoerd als er aanwijzingen zijn dat een gegevensverwerking waarschijnlijk een hoog privacyrisico oplevert voor de mensen van wie de Provincie Limburggegevens verwerkt. De resultaten van een DPIA worden teruggelegd bij de proceseigenaar. Nadien dient getoetst te worden of er mitigerende maatregelen zijn genomen om de eventueel geconstateerde risico's weg te nemen.

Data Protection Impact Assessment	Planning	Status maart 2022
DPIA burgemeestersbenoemingen (bewaartermijn CV's (afgewezen) burgemeesterskandidaten)	Q1 2021	Gereed
Herhalingscheck DPIA e-HRM aanbestedingsfase	Q1 2021	Gereed (toetsing maatregelen 2022)
DPIA vergunningen/toezicht/handhaving in applicatie [REDACTED]	Q1 2021	DPIA voorzien in Q2 2022
DPIA nieuwe bezoekersregistratie	Q1 2021	Gereed
DPIA [REDACTED]	Q3 2021	Gereed

2.4. Concernbreed beheer persoonsgegevens

Binnen de informatiehuishouding van de Provincie Limburg wordt veel informatie bewaard die persoonsgegevens bevat. Uit een analyse blijkt dat op de K-L-M-schijven 21.000.000 informatieobjecten (circa 31 TB) worden beheerd. Van die 31 TB bestaat 6,5 TB uit Outlook mailbestanden. Deze

informatieobjecten bevatten vrijwel zeker persoonsgegevens die een groot risico vormen (bijvoorbeeld bij onrechtmatig gebruik of bij een hack). De uitfasering van dit soort 'schaduwarchieven' hangt nauw samen met de invoering van het centrale dossier- en archiefsysteem SharePoint (DDI).

Beheer persoonsgegevens	Planning	Status maart 2022
Bewaartermijn mailboxen	Q4 2021	In ontwikkeling Besluit Informatiebeheer 2022
Plan uitfasen K-L-M-schijven	Q2 2021	Analyse heeft plaatsgevonden door O&I Instructie opruimen netwerkschijven is gereed
Opruimprotocol uitdiensttreding	Q4 2021	In ontwikkeling Besluit Informatiebeheer 2022
Tools O&I monitoring technisch- en functioneel beheer	Q4 2021	Gereed
toegang tot sollicitatiebrieven en CV's.	Q2 2021	Gereed
Intern verhuisde medewerkers oude rechten verwijderen	Doorlopend	Wordt wisselend opgepakt

2.5. Verwerkingsregister

Het register van verwerkingsactiviteiten (verwerkingsregister) bevat informatie over de persoonsgegevens die een organisatie verwerkt. De AVG schrijft voor welke informatie als verwerkingsverantwoordelijke of verwerker in het verwerkingsregister moet worden opgenomen. In 2021 is het verwerkingsregister concernbreed actueel.

Actueel verwerkingsregister	Planning	Status maart 2022
Continuïteit bijhouden register/ophalen verwerkingen	Doorlopend	Doorlopend
Dataminimalisatie controleren	Q3 2021	Niet uitgevoerd
Datalekkenregister opnemen in	Q1 2021	Niet uitgevoerd
Verwerkingsregister opnemen in	Q1 2021	Gereed
Verwerkingen RIEC/LIEC	Q1 2021	Gereed
Boa-registratie ()	Q3 2021	Vertraagd naar 2022

2.6. Privacy-by-design

Privacy-by-design houdt in dat er al bij het ontwerpen van werkprocessen en dienstverlening rekening wordt gehouden met de bescherming van persoonsgegevens en dat die de gegevens niet langer worden bewaard dan nodig is voor het doel van de verwerking. De eerste stappen op dit gebied zijn gezet, maar dient tot het gewenste volwassenheidsniveau 3 te groeien zodat dit ontwerpprincipe integraal organisatiebreed wordt toegepast.

Privacy-by-design	Planning	Status maart 2022
Implementeren als structurele processtap in het inkoopproces Verplichte check op verwerkersovereenkomst	Q1 2021	Gereed
Continuïteit bijhouden register/ophalen verwerkingen	Doorlopend	Doorlopend
Anonimiseringsprotocol opstellen	Q1 2021	Niet uitgevoerd
Verwerkingen [REDACTED]	Q1 2021	Niet uitgevoerd
Inzet [REDACTED] tool bij know-your-customer procedure	Q4 2021	In uitvoering
Dataminimalisatie controleren	Q2 2021	Niet uitgevoerd

2.7. Privacy in data innovatie

Nieuwe technologieën, zoals algoritmes, worden ingezet om menselijke taken te ondersteunen of zelfs over te nemen, ook binnen de dienstverlening van de overheid. Naast de kansen die dit biedt, zijn er volop keerzijdes aan te merken, zoals het gebrek aan transparantie en uitlegbaarheid. Mochten we in de toekomst gebruik maken van nieuwe technologieën in ons dagelijks werk, dan brengt dit bestuurlijke, juridische en financiële risico's met zich mee. Momenteel is de privacy officer en de FG betrokken in een landelijk consortium waarin een algoritmekader wordt ontwikkeld. De prognose is dat dit kader medio 2022 wordt opgeleverd en kan worden gebruikt in de governance structuur van de Provincie.

Privacy in data innovatie	Planning	Status maart 2022
Toetsingskader Grip op Algoritmes (landelijk consortium)	Q4 2021	Vertraagd naar 2022
Inzet drone	Q1 2021	Niet meer inzetbaar ivm security

3. Status thema's FG toezichtplan

3.1. Bewaren van persoonsgegevens

Vanuit de dubbele rol provinciearchivaris-FG vindt een proactief, integraal toezicht plaats op de informatiehuishouding. Deze integraliteit is wenselijk omdat vele vereisten vanuit privacy wetgeving overeenkomen met de vereisten uit archief- en informatiewetgeving.

In het vorige FG verslag is uitgebreid aandacht besteed aan het intern beheer van persoonsgegevens en dat op dit vlak risico's zijn gesignaleerd. In 2021 is verder onderzoek gedaan naar de omvang van deze risico's. Met name de hoeveelheid informatieobjecten (13.000.000), die ook mogelijk persoonsgegevens bevatten, op de K-L-M-schijven vormt een significant risico. Het afbouwplan van de K-L-M-schijven was voor oplevering gepland in 2021, maar is – mede - door de ontwikkeling naar de SharePoint cloud omgeving *on hold* gezet.¹ Wel is een externe analyse gedaan naar de inhoud van de K en M schijven, Docman en Sharepoint. De provinciearchivaris-FG zal het afbouwplan toetsen als het gereed is in 2022.

Behalve de gesignaleerde risico's op de K-L-M-schijven, is monitoring wenselijk bij de uitfasering van verouderde vakapplicaties en de implementatie van nieuwe vakapplicaties. Het risico is dat er digitale schaduwarchieven ontstaan in dit soort systemen, buiten de scope van het formele informatie- en archiefbeheer (gekoppeld aan de formele SharePoint omgeving).

Bij een correcte toepassing van de Provisa selectielijst, worden persoonsgegevens tijdig vernietigd volgens de geldende bewaartermijnen. De Provincie Limburg heeft stappen gezet door de dossiervorming in SharePoint conform de correcte bewaartermijnen te borgen. Echter, er bevinden zich nog te veel persoonsgegevens in mailboxen en vakapplicaties, buiten de formele SharePoint omgeving.

3.2. Intern toezicht

Het intern toezicht op het gebied van privacy kan worden opgedeeld in drie 'verdedigingslijnen': 1^{ste}, 2^{de} en 3^{de} lijns toezicht. Het toezicht in de 1^{ste} lijn, binnen het primair proces, bestaat uit zelfevaluatie en het bewust zijn van privacyrisico's als een onderdeel van de organisatiecultuur. Ieder cluster heeft een privacyambassadeur als eerste aanspreekpunt voor de medewerkers, die de brug vormt tussen de 1^{ste} en 2^{de} lijn. Deze interne rol dient in 2022 verder te worden geoptimaliseerd. Hierbij kan gedacht worden aan een betere positionering in de gewenste rol (rolvastheid) en training op inhoudelijke vraagstukken.

De wettelijk vastgelegde toezichthoudende taak vanuit de 3^{de} lijn bestaat uit het structureel toetsen door de FG of in de 1^{ste} en 2^{de} lijn een uniforme handelwijze wordt gehanteerd om zodoende risico's beheersbaar te houden in de uitvoering. Het 3^{de} lijns toezicht geeft tevens inzicht in de mate waarin de informatieprocessen 'in control' zijn: zijn de werkprocessen zodanig ingericht dat alle privacyrisico's in beeld zijn en op een adequate wijze worden beheerst? Gezien de (steeds groeiende) omvang van de informatiehuishouding van de Provincie, waarop het Privacybeleid van toepassing is, dient de beschikbare 0,2 fte voor dit toezichtonderdeel uiterst efficiënt te worden ingericht. Daarnaast is, gelet op de breedte en omvang van de scope, slagkracht benodigd en is een duidelijke positionering en herkenbare status richting de organisatie noodzakelijk om de toezichttaken efficiënt te kunnen uitvoeren.

¹ Dit houdt verband met de doorontwikkeling van de team- en mysites, resp. one drive in een cloud omgeving.

3.3. Beveiligen van de verwerking van persoonsgegevens

We hebben als organisatie het doel om informatie als een betrouwbare productiefactor te blijven gebruiken, dat voldoet aan de privacywetgeving. Dit is een verantwoordelijkheid van de hele organisatie (1^e lijn), waarbij het cluster Organisatie en Informatie de kaders schept en ondersteunt (2^e lijn) via o.a. de rol van Concern Information Security Officer (CISO). Hiervoor dient het basisbeveiligingsniveau op het gewenste niveau te blijven. Voor dit gewenste niveau hanteren we een internationale normering (ISO 27001) en de Baseline Informatieveiligheid Overheid (BIO) als uitgangspunt. Op basis hiervan komen we tot een set van maatregelen waarmee informatiebeveiligingsrisico's tot een acceptabel niveau worden beperkt. De verdere professionalisering van het (informatieveiligheids-)risicomanagement proces is erop gericht om eind 2022 te beslissen of een ISO27001 certificering wenselijk is. In 2022 zijn er 5 datalekken geconstateerd.

3.4. Bewustwording

Groeien naar structurele bewustwording van privacyrisico's als onderdeel van de organisatiecultuur is essentieel. Hiervoor zijn stappen gezet door het onderwerp privacy op te nemen in training- en cursusaanbod. In het introductieprogramma is vanaf Q4 2020 als vast onderdeel de module 'informatiebeveiliging, privacy en archiveren' geïntegreerd. Deze module wordt gegeven door de CISO, de privacy officer en de provinciearchivaris-FG. Met deze nieuwe module worden nieuwe medewerkers bewust gemaakt van de risico's op het gebied van informatiebeveiliging, privacy en archiveren. De privacyambassadeurs binnen de clusters dienen in 2022 versterkt te worden in hun rol zodat deze op clusterniveau ook structureel werken aan bewustwording op het gebied van privacy.

3.5. Implementeren privacy by design

Een blijvend aandachtspunt vormt de aandacht voor de privacyrisico's bij het opzetten van nieuwe samenwerkingen met externen en bij het herzien van werkprocessen binnen de organisatie. Vanaf de initiatief-fase dient de privacy officer en de FG betrokken te worden, zodat in het beginstadium de juiste maatregelen kunnen worden genomen waarmee risico's zoveel als mogelijk vooraf kunnen worden uitgesloten. Vanaf Q4 2021 zijn hiervoor de eerste stappen gezet door de behandeling van de projectbrieven CIO team in het PIT team. Voorgenomen initiatieven dienen met deze nieuwe methode in een vroegtijdig stadium te worden geanalyseerd op mogelijke privacyrisico's om daarmee tijdig de juiste mitigerende maatregelen in beeld te krijgen. Het beeld is dat er momenteel een informatie achterstand bestaat op dit gebied, waardoor in de praktijk vaak, op ad hoc basis, alsnog privacyrisico's dienen te worden gemitigeerd binnen korte doorlooptijden. Hiermee komt de effectiviteit van de voorgestelde maatregelen onder druk te staan.

4. Trends & ontwikkelingen

4.1. Samenwerking in informatieketens

Het delen van gegevens is een ontwikkeling die potentieel grote maatschappelijke kansen biedt, maar ook vraagt om nieuw beleid en juridische kaders om die ontwikkeling optimaal te benutten en in goede banen te leiden. Met de komst van nieuwe wetgeving (o.a. de Omgevingswet) wordt steeds meer samengewerkt met andere overheden in samenwerkingsverbanden. Binnen een zogenaamde informatieketen dienen goede afspraken te worden gemaakt over het delen en verwerken van persoonsgegevens. In 2021 is de gezamenlijke dossieropbouw in de nieuwe VTH-applicatie () begonnen, waarin ook persoonsgegevens met elkaar gedeeld gaan worden. Het is noodzakelijk om dit proces beter te toetsen, monitoren en adviseren op welke wijze de verwerking van persoonsgegevens wordt ingericht in dit soort ketendossiers.

4.2. Gebruik social media

Het gebruik van berichtenapps, ook binnen de Provincie, is snel toegenomen door de laagdrempeligheid en gebruiksvriendelijkheid van het medium om snel informatie uit te wisselen in chatberichten. Zowel het gebruik van berichtenapps als het beheer van informatie in berichtenapps zijn actuele vraagstukken geworden sinds de uitspraak van de Raad van State van 20 maart 2019: *WhatsApp en SMS-berichten op zowel zakelijke als privételefoons van bestuurders en ambtenaren vallen onder de Wet openbaarheid van bestuur (Wob), als deze in het kader van het werk zijn verstuurd*.

Veel zaken maken het informatiebeheer van chatberichten ingewikkeld. Zo zijn berichtenapps niet in beheer van de overheid en zijn de technische functionaliteit voor informatiebeheer binnen de berichtenapps zeer beperkt. De data is ongestructureerd; chatgesprekken zijn niet geordend naar onderwerp en beslaan juist vaak meerdere onderwerpen. Formele, informele en soms zelfs privécommunicatie loopt door elkaar, waardoor de privacy van medewerkers onder druk kan komen te staan. Het is noodzakelijk om met een concernbreed protocol deze ontwikkeling te toetsen en te monitoren in 2022.