Intern onderzoek naar de verwerking van persoonsgegevens bij het publiceren van stukken

Aan: het college van burgemeester en wethouders van de gemeente Raalte
Van: de Functionaris voor gegevensbescherming
Datum: 10 februari 2022

Vooraf

De gemeentesecretaris van de gemeente Raalte heeft op 27 januari 2022 de Functionaris gegevensbescherming (FG) gevraagd een oordeel te geven over eventuele overtredingen op het gebied van privacy bij het anonimiseren en publiceren van stukken in de gemeente Raalte.

De aanleiding voor dit verzoek was een incident waarbij de namen van 12 medewerkers van de gemeente op verkeerde wijze waren weggelakt (geanonimiseerd). Na de publicatie van de bestuursverslagen op de gemeentewebsite wees een journalist de gemeente erop dat de met balkjes afgeschermde gegevens na het kopiëren daarvan in Word gewoon te lezen waren. Bij het onderzoeken van dit incident bleek dat er ook andere stukken met weggelakte persoonsgegevens online stonden waarbij deze knip- en plak- methode kon worden toegepast. Het ging om publicaties op de raadspagina. Deze stukken bleken in deze vorm door het college bij de griffie te zijn aangeleverd.

De gemeente Raalte werd eerder met vergelijkbare incidenten geconfronteerd. Het ging in deze gevallen om het onterecht *niet* weglakken van persoonsgegevens. In 2021 werden er bijvoorbeeld bij het anonimiseren van een reactie op een Wob-verzoek namen en contactgegevens van ambtenaren en relaties over het hoofd gezien.

De gemeentesecretaris gaf in haar verzoek om onderzoek aan dat zij graag van de FG wilde weten of het anonimiseren en publiceren van stukken in de gemeente Raalte met waarborgen is omkleed, of eventuele werkafspraken, werkbeschrijvingen en/of protocollen vastgesteld en toegankelijk zijn voor medewerkers en of er bij het meest recente incident rondom de publicatie van bestuursverslagen conform deze zorgvuldigheidseisen is gewerkt. Ook wilde zij graag weten of de FG concrete aanbevelingen voor de organisatie had.

1. Inleiding

In deze rapportage zijn de bevindingen vastgelegd van het door de FG uitgevoerde onderzoek. Deze rapportage is geschreven door de FG in diens rol als onafhankelijk toezichthouder binnen de gemeente op de naleving van de AVG. De rapportage richt zich tot het college van burgemeester en wethouders van de gemeente Raalte als ‘verwerkingsverantwoordelijke’ in de zin van de AVG.

In diens hoedanigheid van intern toezichthouder heeft de FG een eigen bevoegdheid om te bepalen of een intern onderzoek naar verwerkingen van persoonsgegevens wordt ingesteld. Aan het wel of niet starten van en/of rapporteren over een intern onderzoek ligt een risico inschatting van de FG ten grondslag. In dit geval zijn de omvang en aard van de risico’s voor betrokkenen (de personen over wie de persoonsgegevens gaan) en het vermoeden van het ontbreken van technische en organisatorische maatregelen doorslaggevend geweest.

Om iets te kunnen zeggen over de verwerkingen van persoonsgegevens bij het anonimiseren en publiceren van stukken en het college een gedegen inhoudelijk advies te kunnen geven, is door de FG in beeld gebracht of deze verwerkingen rechtmatig plaatsvinden. Hierna volgt daarom eerst een rechtmatigheidsbeoordeling van de FG. Vervolgens zal worden ingegaan op de daarbij geconstateerde gebreken en de aanbevelingen aan het college.

2. Het anonimiseren en publiceren van stukken

Bij het anonimiseren en publiceren van stukken worden persoonsgegevens van inwoners, maar ook van medewerkers en relaties verwerkt. Deze handelingen vinden bijvoorbeeld plaats in het kader van Wob-procedures en het verwerken van bestuurlijke stukken. De daarbij verwerkte persoonsgegevens komen uit de domeinen waar de stukken van afkomstig zijn. Het betreft verwerkingen van persoonsgegevens die incidenteel tot wekelijks plaatsvinden. Bij bepaalde stukken betreft het namen

van personen die weggelakt moeten worden, maar er zijn ook stukken bij waar bijzondere persoonsgegevens in staan, zoals medische gegevens.

Technische en organisatorische maatregelen

Uitgangspunt bij de AVG is dat persoonsgegevens niet zomaar gepubliceerd mogen worden. De wet bepaalt wanneer de gemeente verplicht is stukken openbaar te maken. Waar deze verplichting door de privacy van betrokkenen wordt begrensd, moeten stukken vóór publicatie worden geanonimiseerd. Het anonimiseren van stukken is een methode waarbij identificerende gegevens handmatig of met een programma (Adobe Pro of Bluebeam) definitief worden verwijderd.

Het college heeft in 2014 twee checklists vastgesteld die de medewerkers van het toenmalige team Communicatie & Informatie geacht werden te gebruiken bij het anonimiseren van stukken (zie bijlage 1). Dat deze verantwoordelijkheid inmiddels bij zaakeigenaren is komen te liggen kan worden afgeleid uit het Handboek E-suite/Medewerkersportaal aangezien zaakeigenaren daarin verantwoordelijk worden gehouden voor de inhoud van een zaak. De gemeenteraad heeft in 2018 een Protocol geheimhouding en beslotenheid vastgesteld waarin wordt ingegaan op de informatie-uitwisseling tussen college en raad. De afspraken uit dit protocol zijn uitgewerkt in werkinstructies voor medewerkers van de gemeente (zie bijlage 2). Daarin staat wat het betekent voor stukken in een zaak als deze op enig moment gepubliceerd gaan worden. Zowel de checklists als de werkinstructies staan op Sharepoint en zijn beschikbaar voor de medewerkers van de gemeente Raalte.

Over het gebruik van Adobe Pro en Bluebeam bij het anonimiseren van stukken zijn in 2021 twee DOWR-i handleidingen verschenen (zie bijlage 3 en 4). Daarin wordt het anonimiseren van stukken en het definitief verwijderen van persoonsgegevens met behulp van deze tools stap voor stap beschreven. Volgens de door de FG bevraagde functioneel beheerders wordt er naar deze handleidingen verwezen bij vragen van medewerkers. Deze handleidingen staan op een daarvoor ingerichte Sharepoint site waar de medewerkers van de gemeente Raalte bij kunnen. Onduidelijk is echter of deze instructies naar de medewerkers zijn gecommuniceerd. De met medewerkers van de gemeente Raalte gevoerde gesprekken bevestigen dat niet alle personen die stukken moeten anonimiseren ook voldoende op de hoogte zijn van het juiste gebruik van Adobe Pro en Bluebeam voor het verwijderen van persoonsgegevens. Hoe stukken feitelijk geanonimiseerd worden verschilt volgens hen daarnaast per medewerker en per domein. Er zijn geen instructies gevonden die ingaan op het handmatig, doormiddel van een zwarte stift, anonimiseren en vervolgens weer inscannen van stukken.

Het meest recente incident rondom de publicatie van bestuursverslagen bij de gemeente Raalte laat zien dat Bluebeam niet altijd op juiste wijze wordt toegepast. De betreffende medewerker had naar eigen zeggen geen weet van de daarbij verschenen handleiding en heeft naar eer en geweten geprobeerd de gegevens in de bestuursverslagen weg te lakken door over de tekst zwarte balken te plaatsen en er vervolgens in Bluebeam een Pdf-bestand van te maken. Het op deze manier digitaal afschermen van persoonsgegevens maakt echter dat weggelakte gegevens na het toepassen van de knip- en plak- methode in Word te raadplegen zijn.

Op basis van intern gevoerde gesprekken en de door de FG opgevraagde documentatie kan worden geconcludeerd dat de gemeente de eisen die zij aan het feitelijke gedrag van haar medewerkers stelt om ervoor te zorgen dat het anonimiseren en publiceren van stukken op zorgvuldige wijze plaatsvindt onvoldoende duidelijk heeft gecommuniceerd. Hierdoor missen deze eisen de beoogde werking.

3. Verbetering van de interne privacyorganisatie

Voor het voorkomen van incidenten in de toekomst doet de FG de volgende aanbevelingen:

Versterken bewustzijn handelingsperspectief

Het bewustzijn van de organisatie over wanneer stukken geanonimiseerd moeten worden en wat de juiste toepassing is van de daarvoor beschikbare programma's is onvoldoende gebleken. Adobe Pro en Bluebeam zullen tot de introductie van nieuwe anonimiseringstooling binnen het DOWR-project 'de 5 wetten' in gebruik blijven. Om het management en de medewerkers (opnieuw) bekend te maken met de eisen rondom het anonimiseren en publiceren van stukken verdient het aanbeveling om de

daarbij te gebruiken checklists, werkinstructies en handleidingen doormiddel van NanoLearning bij medewerkers te (her)introduceren. Het is raadzaam om de Privacy Officer te vragen daartoe een minicursus te ontwikkelen die onder de medewerkers van de gemeente Raalte kan worden verspreid.

Naleving procedure meldplicht datalekken

Een belangrijk vereiste voor het feitelijk zorgvuldig omgaan met persoonsgegevens binnen een organisatie is het tijdig kunnen handelen bij incidenten. Van medewerkers wordt niet verwacht dat zij privacy expert zijn, maar er wordt wel van hen verwacht dat zij weten wat zij moeten doen in het geval van een (vermoedelijk) incident. Het per ongeluk onterecht publiceren van persoonsgegevens levert in alle gevallen een datalek op wat door de Privacy Officer beoordeeld en geregistreerd moet worden.

In 2019 is de procedure meldplicht datalekken geactualiseerd en in alle drie de DOWR-gemeentes door de directie vastgesteld (zie bijlage 5). Van de vijf incidenten die zich de afgelopen jaren hebben voorgedaan rondom het publiceren van stukken is er niet één incident waarbij deze procedure op juiste wijze is doorlopen. De FG heeft bijvoorbeeld slechts bij één van deze incidenten een beoordeling van de Privacy Officer terug kunnen vinden. Voor de andere vier incidenten geldt dat zij helemaal niet terug te vinden zijn in de registratie van datalekken van de gemeente Raalte. Het blijft daardoor onduidelijk op welke manier de gemeente bij die gevallen zorg heeft gedragen voor de privacy van de daarbij betrokken personen. Het publiceren van persoonsgegevens kan immers vervelende gevolgen voor de betrokkenen hebben. Zeker daar waar het om gevoelige informatie of kwetsbare personen gaat. Door het niet registreren van incidenten kan tevens niet worden nagegaan of de gemeente accuraat heeft gehandeld vanaf het moment dat zij zich bewust was van deze onrechtmatige verwerkingen van persoonsgegevens. Het is dan ook raadzaam om het management en de medewerkers (opnieuw) te instrueren over hun verantwoordelijkheden bij het constateren en onderzoeken van incidenten en datalekken. Het advies is om ook hier gebruik te maken van de mogelijkheden van Nanolearning. De Privacy Officer kan de opdracht worden gegeven de minicursus over dit onderwerp die reeds in deze tool klaar staat onder de medewerkers van de gemeente Raalte te verspreiden.

Aangezien het gebruik van Nanolearning slechts een basisniveau van bewustzijn stimuleert is het aan te raden naast het gebruik van dit programma ook op andere manieren het bewustzijn rondom het handelingsperspectief bij anonimiseren en het doorlopen van de procedure meldplicht datalekken te vergroten dan wel te verstevigen. De uitkomsten van het onderzoek van de FG kunnen bijvoorbeeld via intranet met medewerkers worden gedeeld of managers kan gevraagd worden bij een eerstvolgend teamoverleg hier aandacht aan te besteden.

Gezien de relatie tussen de door de FG onderzochte incidenten en de verwerkingen die plaatsvinden onder de verantwoordelijkheid van de gemeenteraad wordt geadviseerd de aanbevelingen van de FG met de gemeenteraad te delen.

Conclusie

De interne privacyorganisatie ten aanzien van het anonimiseren en publiceren van stukken functioneert op een aantal onderdelen niet naar behoren. Werkinstructies leven nog onvoldoende onder medewerkers en de in opzet aanwezige waarborgen die moeten leiden tot bijsturing, zoals het doorlopen van de procedure meldplicht datalekken, missen hun werking. De FG acht herhaling van dit type incidenten aannemelijk en benadrukt de noodzaak tot verbetering.

Bijlage 1. Spelregels voor publiceren

Gemeente Raalte

PROCEDUREBLAD COLLEGEVOORSTEL

GEGEVENS VOORSTEL

Zaaknummer	: 5874	Gerelateerde zaak	: geen
Notanummer	:	Onderwerp: Spelregels voor publiceren van persoonsgegevens op de website	
Openbaar	: Ja		
Auteur	: J.K. van Olst 27/05	Eenheid: Dienstverlening	
Portefeuillehouder	: dhr. P.A. Zoon	Team: Advies	
Collegevergadering	d.d.:		

PROCEDURE TOT BESLUITVORMING COLLEGE (INTEGRALE ADVISERING)

Financieel	:
Juridisch	:
Personeel	:
Communicatie	:
ICT	:
Inkoop	:
Minima-effecten	:
Anders	:

	DATUM:	HANDTEKENING:
Portefeuillehouder		
MB		
Advies OR		
Teammanager	22 mei 2014	
Eenheidmanager		
Gemeentesecretaris		

PROCEDURE NA BESLUITVORMING COLLEGE

Gemeenteraad	: ✓	ter informatie	ter besluitvorming	
Ondernemingsraad	:	ter kennisname	adviesrecht	instemmingsrecht

BEKENDMAKING

Belanghebbenden	Gemeentepagina	✓	Intranet	Wkpb
Internet	Persbericht		Staatscourant	Geen

ROUTERING	AKKOORD	BESPREKEN
Burgemeester Zoon		
Wethouder van Loevezijn		
Wethouder Hiemstra		
Wethouder Wagenmans		
Secretaris		

DOCUMENTEN

Bijlage 1	informatienotitie
Bijlage 2	checklist 'persoonsgegevens' voor het opstellen van bestuurlijke documenten
Bijlage 3	overzicht welke gegevens anonimiseren
Bijlage 4	artikel uit Binnenlands Bestuur en de Kamervragen daarover van D66

Kopie na besluitvorming:

Gemeente Raalte

COLLEGEVOORSTEL

ZAAKNUMMER	: 5874	**GERELATEERDE ZAAK**	: geen
ADVIESNOTANUMMER	:		
VOOR INFORMATIE	: Jeanet van Olst		

ONDERWERP EN BESTUURSSAMENVATTING

Spelregels voor publiceren van persoonsgegevens op de website
Bij het publiceren van informatie op de website kunnen belangen van openbaarheid en bescherming van privacy conflicteren. Dit maakte het noodzakelijk duidelijkheid te scheppen en spelregels op te stellen. Uitgangspunt is dat Bescherming van privacy prevaleert boven digitale publicatie van gegevens.

BESLISPUNTEN

1. Te besluiten dat documenten uit het bestuurlijke besluitvormingsproces van het college op de gemeentelijke website geanonimiseerd gepubliceerd worden.
2. De raad te informeren door bijgevoegde informatienotitie.

BESLUIT

Conform

INLEIDING

Toegankelijkheid van informatie draagt bij aan een transparant openbaar bestuur. Het is steeds makkelijker informatie algemeen toegankelijk te maken via internet en documenten integraal (gescand) te plaatsen. Internet is laagdrempelig en wereldwijd 24 uur per dag toegankelijk voor een omvangrijk en divers publiek. Echter, informatie op internet kan ook grote gevolgen hebben voor betrokkenen. Is het niet de informatie zelf, dan kunnen die gevolgen ook een resultaat zijn van het combineren van op internet te vinden gegevens. Toegankelijkheid van gegevens kan bijvoorbeeld identiteitsfraude vergemakkelijken. In de afgelopen tijd is in ieder geval twee keer door personen verzocht persoonsgegevens van de gemeentelijke website te verwijderen.

Het onderwerp persoonsgegevens op internet staat op dit moment in de belangstelling. Zowel binnen ons eigen bestuur komt het onderwerp met enige regelmaat ter sprake, maar het speelt ook in andere gemeenten. Zie bijvoorbeeld het artikel in Binnenlands Bestuur over de gemeente Groningen en de Kamervragen die D66 daarover gesteld heeft aan de Minister van BZK (bijgevoegd).

Daar waar informatie persoonsgegevens bevat of de persoonlijke levenssfeer raakt is het dan ook nodig zorgvuldig te zijn. Dit maakt dat niet alle informatie, ook al is deze openbaar, geschikt is voor digitale publicatie. Het spanningsveld tussen openbaarheid en bescherming van de persoonsgegevens brengt met zich mee dat steeds een afweging plaats moet vinden welk belang in een bepaald geval zwaarder weegt.

Als het gaat om publicatie van persoonsgegevens op internet, komen zowel de Wet openbaarheid van bestuur als de Wet bescherming persoonsgegevens in beeld. Beide regelingen geven uitzonderingen

en beperkingen op het openbaar maken van persoonsgegevens. Daarnaast kennen beide regelingen een belangenafweging. Dit betekent kort gezegd dat niet alle openbare informatie, ook geschikt is voor digitale publicatie. Het is echter ook niet zo dat informatie die niet geschikt is voor digitale publicatie, per definitie ook niet openbaar is.

Het college kiest uit oogpunt van transparantie voor het digitaal publiceren van zijn (openbare) besluitenlijsten en de daarop vermelde collegevoorstellen en –besluiten, maar zonder alle achterliggende documenten en bijlagen.

Dit alles maakt het noodzakelijk duidelijkheid te scheppen en spelregels op te stellen over het publiceren van gegevens in documenten uit het bestuurlijke besluitvormingsproces van het college op de gemeentelijke website (www.raalte.nl).

BEOOGD EFFECT

Privacywetgeving correct uitvoeren waardoor misbruik van persoonsgegevens niet wordt bevorderd en het introduceren van een uniforme werkwijze hoe om te gaan met het publiceren van persoonsgegevens op internet.

ARGUMENTEN

1.1 Volgens het CBP is het op grond van de Wet bescherming persoonsgegevens noodzakelijk persoonsgegevens altijd te anonimiseren.
Het College Bescherming Persoonsgegevens houdt toezicht op de naleving en toepassing van wetten die het gebruik van persoonsgegevens regelen. Het CBP heeft ook taken op het gebied van advisering, voorlichting en informatieverstrekking. Het CBP verschaft helderheid over de uitleg van wettelijke normen in de vorm van richtsnoeren of zienswijzen. In dit geval is een tweetal richtsnoeren van belang, te weten "Publicatie van persoonsgegevens op internet" en "Actieve openbaarmaking en eerbiediging van de persoonlijke levenssfeer". Uit deze documenten is te destilleren dat het CBP van mening is dat het belang van openbaarheid niet opweegt tegen het belang van bescherming van persoonsgegevens. Het publiceren van persoonsgegeven is soms mogelijk, maar volgens het CBP, dan alleen met uitdrukkelijke toestemming van de betrokkene.

1.2 Met het sturen van een document naar een bestuursorgaan doet iemand niet automatisch afstand van bescherming van zijn persoonlijke levenssfeer.
Personen kunnen zich op verschillende wijzen richten tot het gemeentebestuur. Bijvoorbeeld door het sturen van een brief of e-mail bericht, het doen van een aanvraag, het indienen van een bezwaarschrift of klacht of het indienen van zienswijzen. Deze documenten bevatten over het algemeen in ieder geval naam en adresgegevens van de afzender en vaak een handtekening.

Dat een ieder kennis kan nemen van deze documenten draagt bij aan democratisch bestuur. Het belang van openbaarheid vereist niet dat bijvoorbeeld bekend wordt wie de brief heeft geschreven, waar de persoon woont en hoe de handtekening er uit ziet. Met het sturen van een document naar een bestuursorgaan doet iemand ook niet automatisch afstand van bescherming van zijn persoonsgegevens/ persoonlijke levenssfeer. Ter illustratie, de Raad van State heeft in een uitspraak (ECLI:NL:RVS:2012:BY5071) over een bestemmingplanprocedure geconcludeerd dat indieners van zienswijzen mogelijk kunnen worden geacht te hebben ingestemd met integraal ter inzage leggen van die zienswijze gedurende de bestemmingplanprocedure, maar dat dit niet betekent dat zij hebben ingestemd met het openbaar maken van hun persoonsgegevens. Het indienen van zienswijzen kan niet worden aangemerkt als het instemmen van betrokkene met openbaarmaking van persoonsgegevens. Er is dan ook geen grond voor het oordeel dat de betrokkenen personen volledig afstand hebben gedaan van bescherming van hun persoonlijke levenssfeer.

1.3 Bescherming van privacy prevaleert boven digitale publicatie.
Informatie op het wereld wijde web is op veel eenvoudiger manier voor iedereen beschikbaar. Informatie die op het web staat is heel makkelijk te hergebruiken en veel moeilijker te verwijderen en daardoor lang beschikbaar. Zoekmachines worden steeds geavanceerder en het koppelen van informatie is steeds makkelijker. Om die reden passen bij het digitaal publiceren van gegevens zwaardere voorwaarden. In de eerder genoemde uitspraak van de Raad van State (ECLI:NL:RVS:2012:BY5071) is benadrukt dat het college van B&W van de betreffende gemeente in redelijkheid aan de bescherming van de persoonlijke levenssfeer van de indieners van zienswijzen meer gewicht heeft kunnen toekennen dan aan het belang van openbaarheid. Het belang van openbaarheid was voldoende gediend met het geanonimiseerd publiceren van de zienswijze en de reactie van het college daarop.

De belangenafweging tussen digitale openbaarheid en bescherming van persoonsgegevens zou daarom moeten doorslaan naar bescherming van persoonsgegevens. Ook willen we voorkomen dat mensen terughoudend worden zich te richten tot het gemeentebestuur vanwege de mogelijkheid dat hun gegevens digitaal openbaar worden. Een dergelijke situatie draagt niet bij aan democratisch bestuur.

1.4 Anonimiseren heeft geen inhoudelijk effect op procedures
Het anonimiseren, noch het nalaten van anonimiseren van persoonsgegevens heeft, indien het publiceren van gegevens niet daadwerkelijk noodzakelijk is voor de procedure, inhoudelijk geef effect op procedures. Ter verduidelijking, de Raad van State heeft in een uitspraak (ECLI:NL:RVS:2010:BO1177) geconcludeerd dat het plaatsen van een niet-geanonimiseerde versie van een zienswijzenota op internet geen gebrek is dat kan leiden tot vernietiging van het bestreden bestemmingsplan, maar dat betrokkenen daarover wel kunnen klagen bij het CBP.

1.5 Ook Wet openbaarheid van bestuur maakt uitzondering voor persoonsgegevens
Er lijkt een schijnbare tegenstelling te zitten tussen de Wet openbaarheid van bestuur (Wob) en de Wet bescherming persoonsgegevens (Wbp). Echter, artikel 1, lid 1 onder e van de Wob stelt dat het verstrekken van informatie in alle gevallen achterwege blijft voor zover het persoonsgegevens betreft als bedoeld in paragraaf 2 van hoofdstuk 2 van de Wbp, tenzij de verstrekking kennelijk geen inbreuk op de persoonlijke levenssfeer maakt.
Paragraaf 2 van hoofdstuk 2 van de Wbp bevat bijzondere persoonsgegevens. Bijzondere persoonsgegevens zijn gegevens over: godsdienst, levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging, strafrechtelijke persoonsgegevens, persoonsgegevens over onrechtmatig of hinderlijk gedrag vanwege een opgelegd verbod voor dat gedrag.

2.1 Collegebevoegdheid, raad informeren
Het publiceren van gegevens via de gemeentelijke website is een bevoegdheid van het college op grond van artikel 160 lid 1 onder a van de Gemeentewet.
Gelet op de aandacht voor dit onderwerp in de raad(spleinsessie) en de inlichtingenplicht van het college aan de raad op grond van artikel 169 Gemeentewet, stellen wij voor de raad over dit onderwerp te informeren middels bijgevoegde informatienotitie.

KANTTEKENINGEN

1.1 Anonimiseren betekent extra werkzaamheden voor medewerkers van team C&I.
Het anonimiseren gebeurt door gegevens te vervangen door neutrale termen, het weergeven van de rol van betrokkene of een algemene omschrijving. Het anonimiseren van documenten betekent extra werkzaamheden voor medewerkers van team C&I. Zij bekijken de documenten en vervangen waar nodig gegevens. In het document is zichtbaar op welke plek gegevens zijn geanonimiseerd. In de bijlage is een checklist van uitgangspunten en een overzicht van al dan niet te anonimiseren gegevens opgenomen. Deze bijlage is opgesteld aan de hand van de richtsnoeren van het CBP en de anonimiseringsrichtlijn uit de rechtspraak.
De extra handelingen voor medewerkers van team C&I zijn zoveel mogelijk te beperken als medewerkers bij het opstellen van documenten rekening houden met de uitgangspunten en de richtlijn. De extra handelingen wegen bovendien niet op tegen het belang van bescherming van privacy van personen.

FINANCIËN

Dit voorstel heeft geen financiële gevolgen.

VERVOLG

Het gaat om interne werkafspraken. Dit voorstel vraagt dan ook geen verdere besluitvorming.

COMMUNICATIE

Na een besluit van uw college:
1. de raad informeren middels bijgevoegde informatienotitie;
2. medewerkers informeren over de uitgangspunten en de anonimiseringsrichtlijn.

In het Directieoverleg is al besloten dat medewerkers van team C&I documenten uit het besluitvormingsproces van het college anonimiseren.

BIJLAGEN

Bijlage 1	informatienotitie
Bijlage 2	checklist 'persoonsgegevens' voor het opstellen van bestuurlijke documenten
Bijlage 3	overzicht welke gegevens anonimiseren
Bijlage 4	artikel uit Binnenlands Bestuur en de Kamervragen daarover van D66

Gemeente Raalte

INFORMATIENOTITIE RAAD

ZAAKNUMMER	: 5874	**GERELATEERDE ZAAK**	:
B&W VERGADERING	: 3 juni 2014		
ONDERWERP	: Spelregels publiceren persoonsgegevens op internet		
BEHANDELEND AMBTENAAR	: Jeanet van Olst telefoon: (0572) 347 622, e-mail: Jeanet.van.Olst@raalte.nl		

KENNIS TE NEMEN VAN

Kennis nemen van de uitgangspunten van het college voor het publiceren van persoonsgegevens op internet.

INLEIDING

Toegankelijkheid van informatie draagt ook bij aan een transparant openbaar bestuur. Het is steeds makkelijker informatie algemeen toegankelijk te maken via internet en documenten integraal (gescand) te plaatsen. Internet is laagdrempelig en wereldwijd 24 uur per dag toegankelijk voor een omvangrijk en divers publiek. Informatie op het wereld wijde web is heel makkelijk te hergebruiken en veel moeilijker te verwijderen en daardoor lang beschikbaar. Zoekmachines worden steeds geavanceerder en het koppelen van informatie is steeds makkelijker.
Informatie op internet kan ook grote gevolgen hebben voor betrokkenen. Is het niet de informatie zelf, dan kunnen die gevolgen ook een resultaat zijn van het combineren van op internet te vinden gegevens. Toegankelijkheid van gegevens kan bijvoorbeeld identiteitsfraude vergemakkelijken.

Daar waar informatie persoonsgegevens bevat of de persoonlijke levenssfeer raakt is het dan ook nodig zorgvuldig te zijn. Dit maakt dat niet alle informatie, ook als is deze openbaar, geschikt is voor online publicatie. Het spanningsveld tussen openbaarheid bescherming van de persoonsgegevens brengt met zich mee dat steeds een afweging plaats moet vinden welk belang in een bepaald geval zwaarder weegt.

Als het gaat om publicatie van persoonsgegevens op internet, komen zowel de Wet openbaarheid van bestuur als de Wet bescherming persoonsgegevens in beeld. Beide regelingen geven uitzonderingen en beperkingen op het openbaar maken van persoonsgegevens. Daarnaast kennen beide regelingen een belangenafweging. Dit betekent kort gezegd dat niet alle openbare informatie, ook geschikt is voor digitale publicatie. Het is echter ook niet zo dat informatie die niet geschikt is voor digitale publicatie, per definitie ook niet openbaar is.

Wij kiezen uit oogpunt van transparantie voor het digitaal publiceren van onze (openbare) besluitenlijsten en de daarop vermelde collegevoorstellen en –besluiten, maar zonder alle achterliggende documenten en bijlagen.

Bovenstaande maakte het noodzakelijk duidelijkheid te scheppen. Ons college heeft daarom uitgangspunten en spelregels geformuleerd over de wijze waarop wij documenten uit het ons bestuurlijke besluitvormingsproces op de gemeentelijke website (www.raalte.nl) plaatsen.

Wij zijn van mening dat in de afweging tussen het belang van openbaarheid via de website en het belang van bescherming van persoonsgegevens de balans doorslaat naar bescherming van persoonsgegevens.

Wat zijn persoonsgegevens?
Het begrip persoonsgegevens is heel ruim. Het gaat over iedere informatie betreffende de geïdentificeerde of identificeerbare natuurlijke persoon. Het kan gaan over kenmerken die iemand direct kan identificeren, maar ook over gegevens die indirect naar iemand leiden. Denk bijvoorbeeld aan fysieke kenmerken, naam, adres en woonplaatsgegevens, geboortedatum, telefoonnummer, e-mailadres, handtekening en handschrift, voertuigkenteken, maar ook iemands eigenschappen, opvattingen en gedragingen. Ook subjectieve informatie valt onder dit begrip.

Naast de hiervoor genoemde persoonsgegevens, zijn er ook bijzondere persoonsgegevens. Voor deze persoonsgegevens geldt een strenger regime voor publicatie. Deze informatie mag alleen worden gepubliceerd met uitdrukkelijke toestemming van de betrokkene. Het gaat dan om gegevens over godsdienst, levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging, strafrechtelijke gegevens en gegevens over onrechtmatig/ hinderlijk gedrag. Opmerking: het verbod om informatie over iemands politieke gezindheid te vermelden geldt niet als die vermelding te maken heeft met het vervullen van functies in bestuursorganen en adviescolleges.

Een aparte categorie bijzondere persoonsgegevens zijn identificatienummers, bijvoorbeeld het burgerservicenummer. Identificatienummers maken het koppelen van bestanden makkelijker en vormen daarmee een extra bedreiging voor de persoonlijke levenssfeer. Het is daarom niet toegestaan iemands identificatienummer op internet te publiceren, ook niet met toestemming van de betrokkene.

Geen persoonsgegevens zijn gegevens over bedrijven en instellingen en objecten, tenzij deze gegevens herleidbaar zijn naar een persoon, bijvoorbeeld individuele bestuurders.

Uitgangspunten
Wij hanteren de volgende uitgangspunten voor publicatie van documenten uit het ons bestuurlijke besluitvormingsproces op de gemeentelijke website:
1. Alles is openbaar, tenzij een uitzondering van toepassing is.
2. We voorkomen onnodige publicatie van persoonsgegevens.
3. We plaatsen alleen persoonsgegevens op internet als sprake is van noodzaak en als betrokkene daartoe toestemming geeft;
4. Bij het actief publiceren van persoonsgegevens op internet houden we rekening met de aard van de gegevens, de mogelijke gevolgen van het publiceren voor betrokkenen en de mate waarin voor de betrokkene wordt voorzien in passende waarborgen;
5. Als de betrokkene zijn toestemming intrekt, verwijderen we gegevens zo snel mogelijk.

Bij deze uitgangspunten hebben we rekening gehouden met een tweetal richtsnoeren van het College Bescherming Persoonsgegevens, te weten “Publicatie van persoonsgegevens op internet” en “Actieve openbaarmaking en eerbiediging van de persoonlijke levenssfeer”.
Het College Bescherming Persoonsgegevens houdt toezicht op de naleving en toepassing van wetten die het gebruik van persoonsgegevens regelen. Het CBP heeft ook taken op het gebied van advisering, voorlichting en informatieverstrekking. Het CBP verschaft helderheid over de uitleg van wettelijke normen in de vorm van richtsnoeren of zienswijzen.

Ook houden we rekening met het feit dat iemand zich richt tot het gemeentebestuur, dit niet betekent dat iemand daarmee automatisch afstand doet van bescherming van zijn persoonsgegevens. Personen kunnen zich op verschillende wijzen richten tot het gemeentebestuur. Bijvoorbeeld door het sturen van een brief of e-mail bericht, het doen van een aanvraag, het indienen van een bezwaarschrift of klacht of het indienen van zienswijzen. Deze documenten bevatten over het algemeen in ieder geval naam en adresgegevens van de afzender en vaak een handtekening.

Dat een ieder kennis kan nemen van deze documenten draagt bij aan democratisch bestuur. Het belang van openbaarheid vereist echter niet dat via de website bijvoorbeeld bekend wordt wie de brief heeft geschreven, waar de persoon woont en hoe de handtekening er uit ziet.
Ter illustratie, de Raad van State heeft in een uitspraak (ECLI:NL:RVS:2012:BY5071) over een bestemmingplanprocedure geconcludeerd dat indieners van zienswijzen mogelijk kunnen worden geacht te hebben ingestemd met integraal ter inzage leggen van die zienswijze gedurende de bestemmingplanprocedure, maar dat dit niet betekend dat zij hebben ingestemd met het openbaar maken van hun persoonsgegevens. Het indienen van zienswijzen kan niet worden aangemerkt als het instemmen van betrokkene met openbaarmaking van persoonsgegevens. Er is dan ook geen grond voor het oordeel dat de betrokkenen personen volledig afstand hebben gedaan van bescherming van hun persoonlijke levenssfeer.

Als derde hebben we rekening gehouden met het feit dat het anonimiseren, noch het nalaten van anonimiseren van persoonsgegevens inhoudelijk effect heeft op procedures. Voorwaarde is dat het hierbij gaat op gegevens die niet daadwerkelijk noodzakelijk zijn voor de procedure. De Raad van State heeft in een uitspraak (ECLI:NL:RVS:2010:BO1177) geconcludeerd dat het plaatsen van een niet-geanonimiseerde versie van een zienswijzenota op internet geen gebrek is dat kan leiden tot vernietiging van het bestreden bestemmingsplan, maar dat betrokkenen daarover wel kunnen klagen bij het CBP.

Wijze van anonimiseren
Het anonimiseren gebeurt door gegevens te vervangen door neutrale termen, het weergeven van de rol van betrokkene of een algemene omschrijving. In het document is zichtbaar op welke plek gegevens zijn geanonimiseerd.

KERNBOODSCHAP

Bij het publiceren van informatie op de website kunnen belangen van openbaarheid en bescherming van privacy conflicteren. Dit maakte het wenselijk duidelijkheid te scheppen en spelregels op te stellen. Uitgangspunt is dat Bescherming van privacy prevaleert boven digitale publicatie van gegevens.

VERVOLG

Niet van toepassing

COMMUNICATIE

Niet van toepassing

Burgemeester en wethouders van Raalte,

de secretaris, de burgemeester,

P.A. Zoon

Gemeente Raalte

Checklist 'persoonsgegevens' bij het opstellen van bestuurlijke documenten

Uitgangspunten:

1. Alles is openbaar, tenzij een uitzondering van toepassing is.
2. We voorkomen onnodige publicatie van persoonsgegevens, dus we vermelden geen persoonsgegevens in bestuurlijke documenten, tenzij dit absoluut noodzakelijk is voor de besluitvorming.
3. We plaatsen alleen persoonsgegevens op internet als sprake is van noodzaak en als betrokkene daartoe toestemming geeft;
4. Bij het actief publiceren van persoonsgegevens op internet houden we rekening met de aard van de gegevens, de mogelijke gevolgen van het publiceren voor betrokkenen en de mate waarin voor de betrokkene wordt voorzien in passende waarborgen;
5. Als de betrokkene zijn toestemming intrekt, verwijderen we gegevens zo snel mogelijk.

Vragen die kunnen helpen bij het opstellen van bestuurlijke documenten en het toevoegen van bijlagen zijn:

- Komt het document waar ik aan werk of de achterliggende informatie en documenten op internet?
- Bevatten die documenten persoonsgegevens? Bevat het document gegevens die het mogelijk maken een persoon direct of indirect te identificeren?
- Is het publiceren van persoonsgegevens op internet noodzakelijk, kan het bestuursorgaan zijn taak niet vervullen als vermelding van de gegevens op internet achterwege blijft?
- Zijn er andere manieren of middelen om het document te publiceren?
- Is het mogelijk de informatie te anonimiseren door het gebruik van neutrale termen?
- Als het noodzakelijk is de persoonsgegevens op internet te publiceren en anonimiseren niet mogelijk is, heeft betrokkene dan expliciet toestemming gegeven voor publicatie?

I. Wanneer is sprake van persoonsgegevens?

Persoonsgegevens zijn: elk gegeven waardoor een natuurlijk persoon direct of indirect te identificeren is.

Voorbeelden van persoonsgegevens zijn: naam, (e-mail)adres, woonplaats, telefoonnummer, handtekening, handschrift, bankrekeningnummer, burgerservicenummer, kenmerken van fysieke, fysiologische, psychische, economische, culturele of sociale identiteit, godsdienst, levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging, strafrechtelijke persoonsgegevens, voertuigkenteken, foto's, etc.

II. Houd rekening met het volgende:

- Vermeld geen persoonsgegevens in bestuurlijke voorstellen, tenzij de burgemeester, het college of de raad zijn bestuurlijke taak niet kan vervullen als vermelding van de gegevens achterwege blijft.

- Probeer persoonsgegevens zoveel mogelijk te anonimiseren door het gebruik neutrale termen of vermeld alleen het hoogst noodzakelijke. Voorkom combinaties van persoonsgegevens, waardoor een persoon te identificeren is. Stel bij zienswijzen, inspraakreacties, meerder aanvragers/ belanghebbenden e.d. een geanonimiseerde nota/ notitie op, of volsta, indien nodig, met alleen de naam, of de locatie, of een ander gegeven specifiek van belang voor de nota of notities. Vervang persoonsgegevens door neutrale termen.

- Vermeld geen persoonsgegevens in het onderwerp, de beslispunten of de bestuurssamenvatting.

- Vermeld geen persoonlijke identificatienummers, zoals het burgerservice nummer (BSN). Het is in geen enkel geval toegestaan dergelijke identificatienummers te publiceren, er gelden geen uitzonderingen.

- Vermeld geen persoonsgegevens in bestandsnamen van documenten.

III. Beoordeling 'Openbaar?' bij het invullen van een procedureblad/ bijzondere persoonsgegevens:

Beoordeel of een voorstel, inclusief de achterliggende documenten, openbaar is volgens de Wet openbaarheid van bestuur (Wob). Op deze plaats besteden we alleen aandacht aan de openbaarheid van persoonsgegevens. Kijk voor openbaarheid van andere informatie naar de "Handleiding verzoeken om informatie Wob" op intranet.

Niet openbaar

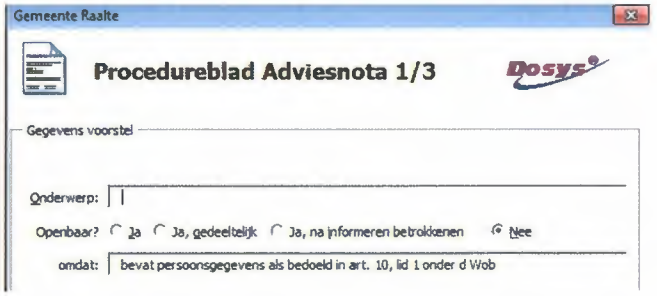
Als vermelding van *bijzondere* persoonsgegevens noodzakelijk is, is het voorstel of een achterliggend document volgens artikel 10, lid 1 onder d van de Wet openbaarheid van bestuur in ieder geval niet openbaar. Bijzondere persoonsgegevens zijn gegevens over: godsdienst, levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging, strafrechtelijke persoonsgegevens, persoonsgegevens over onrechtmatig of hinderlijk gedrag vanwege een opgelegd verbod voor dat gedrag. Publicatie op de website van een niet-openbaar document blijft achterwege.

Uitzonderingen

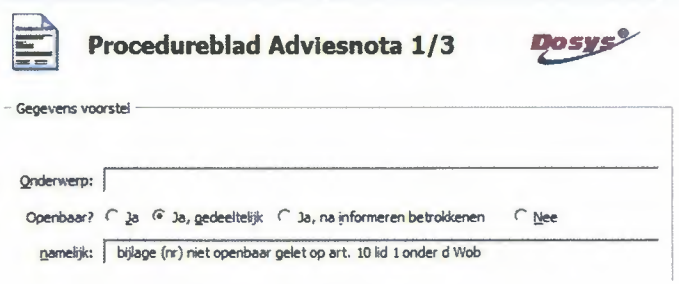
Voor bijzondere persoonsgegevens geldt een uitzondering:
POLITIEKE GEZINDHEID: persoonsgegevens over politieke gezindheid zijn wel openbaar als deze gegevens te maken hebben met de vervulling van functies in bestuursorganen en adviescolleges.

Werkwijze:

Is het noodzakelijk *in het voorstel* bijzondere persoonsgegevens te vermelden, en
is de uitzondering niet van toepassing,
vermeld dan:



Is het noodzakelijk *bijlagen toe te voegen* die bijzondere gegevens bevatten, en
is de uitzondering niet van toepassing,
vermeld dan:



IV. Beoordeling 'overige' persoonsgegevens:
Voorbeelden van 'overige' persoonsgegevens zijn: naam, (e-mail)adres, woonplaats, telefoonnummer, handtekening, handschrift, kenmerken van fysieke, fysiologische, psychische, economische, culturele of sociale identiteit, voertuigkenteken, foto's, etc.

Werkwijze:

Vermeld geen persoonsgegevens in bestuurlijke documenten of vervang persoonsgegevens door neutrale termen.

Vermeld je toch persoonsgegevens in bestuurlijke documenten of staan ze in de daarbij behorende achterliggende documenten, toon dan aan of motiveer dat:

- Betrokkene ondubbelzinnig en zonder twijfel toestemming heeft verleend voor publicatie van gegevens op internet;
- Publicatie van persoonsgegevens noodzakelijk is voor de uitvoering van een overeenkomst waarbij betrokkene partij is, of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene en die noodzakelijk zijn voor het sluiten van een overeenkomst;
- Publicatie van persoonsgegevens noodzakelijk is om een wettelijke verplichting na te komen;
- Publicatie van persoonsgegevens noodzakelijk is voor de goede vervulling en een publiekrechtelijke taak door het bestuursorgaan;
- Publicatie van persoonsgegevens noodzakelijk is voor de behartiging van het gerechtvaardigd belang van het bestuursorgaan, en dit belang prevaleert boven het belang of de fundamentele rechten en vrijheden van betrokkenen (waaronder het recht op bescherming van de persoonlijke levenssfeer) en het belang niet kan worden gediend met minder ingrijpende middelen.

Persoonsgegevens die reden- of richtinggevend zijn voor een document hoeven niet te worden verwijderd.

➥ Vermeld de toelichting in je voorstel onder het kopje 'communicatie'.

Bevat je voorstel geen toelichting en is het voorstel openbaar, dan zal het voorstel met bijlagen op enig moment geanonimiseerd op de website terechtkomen. Het op deze wijze anonimiseren van documenten komt over het algemeen de leesbaarheid niet ten goede.

Welke gegevens anonimiseren?

NIET anonimiseren:

- ☐ Gegevens over (overheids)instanties of ondernemingen die behoren tot rechtspersonen, zoals bv, nv, vereniging, stichting en publiekrechtelijke rechtspersoon,

tenzij deze direct herleidbaar zijn tot een natuurlijke persoon.

- ☐ Gegevens van natuurlijke personen in dienst van een rechtspersoon of bestuursorgaan en *handelend in de uitoefening van een specifieke functie*, bijvoorbeeld namen van deskundigen, adviseurs, advocaten, gemachtigden, accountant.

- ☐ Namen/ gegevens van gemeentebestuurders (collegeleden en raadsleden), handelend in de uitoefening van hun functie/ ambt in bestuursorganen.

WEL anonimiseren:

- ☐ Gegevens van natuurlijke personen (of de combinatie daarvan) → vervangen door neutrale termen, rol of omschrijving:
  - naam, adres, woonplaats
  - e-mail adres;
  - geboortedatum;
  - bankrekeningnummer;
  - telefoonnummer;
  - kentekennummers;
  - handtekening;
  - handschrift;
  - persoonlijke identificatienummers als burgerservicenummer of nummers van paspoort/ identiteitsbewijs;
  - godsdienst/ levensovertuiging;
  - ras;
  - politieke gezindheid;
  - gezondheid;
  - seksuele leven;
  - lidmaatschap van een vakvereniging;
  - strafrechtelijke persoonsgegevens;
  - persoonsgegevens over onrechtmatig of hinderlijk gedrag vanwege een opgelegd verbod voor dat gedrag.

- ☐ Gegevens van natuurlijke personen *in dienst van* een rechtspersoon of bestuursorgaan, bijvoorbeeld namen van medewerkers van die rechtspersoon of dat bestuursorgaan → vervangen door neutrale termen, omschrijving, of naam van de organisatie.

- ☐ E-mailadressen en telefoonnummers van *medewerkers* van de gemeente Raalte → vervangen door het algemeen telefoonnummer en het algemeen e-mailadres.
  Een van de werkafspraken in de organisatie is dat op documenten, berichten en dergelijke die 'naar buiten' gaan geen rechtstreekse telefoonnummers en eigen e-mailadressen genoemd worden, maar het algemeen telefoonnummer (0572-347799) en het algemeen e-mailadres (info@raalte.nl).

- ☐ Namen van rechtspersonen als deze naam herleidbaar is tot een natuurlijke persoon → vervangen door neutrale termen, bijvoorbeeld 'bv', 'nv', 'vereniging', 'stichting' of 'adviesbureau'.

Bijlage 2. Werkinstructie openbare gegevens en geheimhouding

Werkinstructie openbare gegevens en geheimhouding

Gemeente Raalte

De gemeenteraad heeft een protocol openbaarheid en geheimhouding vastgesteld. In dit protocol staan de afspraken tussen het college en de raad over de openbaarheid en geheimhouding van stukken en informatiebijeenkomsten. De afspraken in dit protocol zijn verder uitgewerkt in deze werkinstructie zodat stellers van bestuurlijke stukken op de juiste wijze vormgeven aan de afspraken uit het protocol.

Vooraf: alle informatie is openbaar, tenzij

Openbaarheid is een groot goed en regel in het openbaar bestuur. Beslotenheid en geheimhouding moeten een uitzondering blijven, maar kunnen noodzakelijk zijn ter bescherming van bepaalde belangen. Die afweging maakt een steller van een stuk niet zelf, maar in samenspraak met een juridisch adviseur op basis van wet- en regelgeving. Bij (tijdelijk) niet-openbare of geheime stukken worden daarom altijd verwezen naar de Wet openbaarheid van bestuur (Wob).

De werkinstructie maakt onderscheid in schriftelijke informatie en mondelinge informatie.

Schriftelijke informatie

Voor schriftelijke informatie (denk aan collegevoorstellen, raadsvoorstellen, memo's, informatienotities) zijn er vier varianten mogelijk:

1. Openbaar
2. Tijdelijk niet – openbaar
3. Niet – openbaar
4. Geheim

Openbaar

1. Collegevoorstellen waarop het college een besluit heeft genomen, worden genoteerd op de openbare besluitenlijst.
2. De openbare besluitenlijst wordt de week erop vastgesteld (dinsdag) en gepubliceerd op de woensdag.
3. De afzonderlijke collegevoorstellen en – besluiten worden ook op de woensdag actief openbaar gemaakt doordat het bestuurssecretariaat de stukken publiceert op de website.
4. De achterliggende stukken (bijlagen) van een collegevoorstel worden – indien er een Wob-verzoek is ingediend – op aanvraag openbaar gemaakt.

Tijdelijk niet – openbaar

1. Tijdelijk niet openbare stukken betreffen stukken waarover eerst een belanghebbende (inwoner, initiatiefnemer, organisatie, maar ook gemeenteraad etc.) moet worden ingelicht of er eerst andere acties moeten worden ondernomen (denk aan een gezamenlijk persbericht van meerdere gemeenten) voordat het collegevoorstel actief openbaar wordt gemaakt. Bedenk zorgvuldig wie als eerste en op welk tijdstip moet worden geïnformeerd (eerst inwoner, dan de gemeenteraad of andersom).
2. Geef op het procedureblad/zaaksysteem aan dat het een tijdelijk niet – openbaar stuk betreft, aangezien eerst de belanghebbende moet worden geïnformeerd en geef aan hoe lang het stuk niet openbaar is (standaard een week). Verwijs daarbij naar artikel 10 Wob, lid 2 onder f.
3. **Standaard worden deze stukken alsnog door het college één week later mondeling toegelicht in het persgesprek**, tenzij anders is aangegeven (een langere termijn noodzakelijk is). Zorg er dus voor dat je die week benut om de belanghebbende mondeling of schriftelijk te informeren over het besluit. Bedenk ook hoe je de gemeenteraad informeert en op welk moment.
4. Het collegevoorstel en – besluit wordt vervolgens alsnog op de woensdag van die week erop actief openbaar gemaakt doordat het bestuurssecretariaat de stukken publiceert op de website.
5. De samenvatting van het onderwerp en het collegebesluit worden toegevoegd aan de openbare besluitenlijst van dezelfde week onder verwijzing naar het collegebesluit van die week ervoor.
6. De achterliggende stukken (bijlagen) worden – indien er een Wob-verzoek komt – op aanvraag openbaar gemaakt.

Niet – openbaar

1. Niet openbare stukken betreffen stukken die niet actief openbaar gemaakt mogen worden ter bescherming van bepaalde belangen. Of daar sprake van is, bepaal je samen met juridisch advies. Niet-openbaar betekent overigens niet dat niemand kennis kan nemen van de documenten (zie daarvoor punt 6 als voorbeeld).
2. Geef op het procedureblad/zaaksysteem aan dat het om een niet openbaar stuk gaat met een verwijzing naar het juiste artikel van de Wob.
3. De Wob artikel 10 kent absolute en relatieve weigeringsgronden.
   Bij absolute weigeringsgronden gaat het om informatie die (a) de eenheid van de Kroon in gevaar zou kunnen brengen, (b) de veiligheid van de Staat zou kunnen schaden, het (c) bedrijfs- en fabricagegegevens betreft die vertrouwelijk aan de overheid zijn meegedeeld (denk aan offertes) of (d) het persoonsgegevens betreft.

   Daarnaast kent de Wob een aantal relatieve weigeringsgronden. Hier wordt telkens een afweging gemaakt tussen het belang van openbaarmaking en de (b) de economische of financiële belangen van de gemeente (bijvoorbeeld de exploitatieopzet bij een bestemmingsplan, beroepsprocedures, gerechtelijke procedures), (d) inspectie, controle en toezicht door bestuursorganen of (e) eerbiediging van de persoonlijke levenssfeer.

4. Zet in het voorstel bij het kopje "Communicatie" uiteen waarom het stuk een niet openbaar karakter kent met een verwijzing naar de Wob, waarom dat artikel van toepassing is, alsmede de duur van het niet openbare karakter van de stukken. Geef aan of en op welk moment de gemeenteraad wordt geïnformeerd.
5. De samenvatting van het onderwerp en het collegebesluit worden genoteerd op de niet openbare besluitenlijst. Deze besluiten worden niet toegelicht in het persgesprek en komen ook niet op de website.
6. De niet openbare besluitenlijst wordt op de griffie ter inzage gelegd voor raadsleden. In het protocol is afgesproken dat raadsleden de niet-openbaarheid respecteren en geen mededelingen zullen doen betreffende deze besluiten. Raadsleden kunnen op verzoek de achterliggende stukken (collegevoorstel en – besluiten, maar ook bijlagen) inzien.

Niet-openbaar is een uitzondering op het uitgangspunt van (actieve) openbaarmaking van overheidsdocumenten. Niet-openbaar betekent niet dat niemand kennis kan nemen van de documenten. Daarom is het soms wenselijk te kiezen voor het instrument van het opleggen van geheimhouding. Geheimhouding betekent dat iemand die kennis heeft van de geheime informatie, deze niet met derden mag bespreken of aan derden ter beschikking mag stellen. Schending van geheimhouding is strafbaar. Geheimhouding is echter ook een beperking van de vrijheid van meningsuiting. Het opleggen van geheimhouding is een zwaar instrument dat we alleen bij uitzondering toepassen. Voor het opleggen van geheimhouding geldt de volgende, strikte procedure.

Geheim[1]

1. Het college en de raad hebben de formele bevoegdheid om in bepaalde gevallen geheimhoudingsplicht op te leggen dan wel te bekrachtigen.
2. Of er sprake is van geheimhouding, bepaal je samen met juridisch advies.
3. Geef op het procedureblad/zaaksysteem aan dat het om een geheim stuk gaat met een verwijzing naar artikel 25 (raad) of 55 (college) van de gemeentewet inclusief de motivering naar de Wob en de termijn van geheimhouding.
4. De Wob artikel 10 kent absolute en relatieve weigeringsgronden.
   Bij absolute weigeringsgronden gaat het om informatie die (a) de eenheid van de Kroon in gevaar zou kunnen brengen, (b) de veiligheid van de Staat zou kunnen schaden, het (c) bedrijfs- en fabricagegegevens betreft die vertrouwelijk aan de overheid zijn meegedeeld (denk aan offertes) of (d) het persoonsgegevens betreft.

   Daarnaast kent de Wob een aantal relatieve weigeringsgronden. Hier wordt telkens een afweging gemaakt tussen het belang van openbaarmaking en de (b) de economische of financiële belangen van

[1] Let op: we hanteren dus de term geheim en niet de term vertrouwelijk.

de gemeente (bijvoorbeeld de exploitatieopzet bij een bestemmingsplan, beroepsprocedures, gerechtelijke procedures), (d) inspectie, controle en toezicht door bestuursorganen of (e) eerbiediging van de persoonlijke levenssfeer.
5. Formuleer een apart beslispunt en besluit waarbij de geheimhouding door het college wordt opgelegd en bekrachtigd. De precieze formulering stem je af met juridisch advies.
6. Bij een raadsvoorstel formuleer je ook een apart beslispunt en besluit waarbij je de raad de geheimhouding laat bekrachtigen. Let op: deze bekrachtiging dient in de eerstvolgende vergadering plaats te vinden! De precieze formulering stem je af met juridisch advies, zij bezitten standaard sjablonen.
7. Geef **alle** pagina's een watermerk "Geheim" door in Word achtereenvolgens te klikken op Pagina-indeling, Watermerk, Aangepast Watermerk, Tekst als Watermerk en verander het woordje CONCEPT in GEHEIM en klik op "ok".
8. Zet in het voorstel bij het kopje "Communicatie" uiteen waarom het stuk geheim is met verwijzing naar de gemeentewet en de Wob, waarom deze artikelen van toepassing zijn, alsmede de duur van de geheimhouding op de stukken. Geef aan of en op welk moment de gemeenteraad wordt geïnformeerd.
9. De samenvatting van het onderwerp en het collegebesluit worden genoteerd op de niet openbare besluitenlijst. Deze besluiten worden niet toegelicht in het persgesprek en komen ook niet op de website.
10. De niet openbare besluitenlijst wordt op de griffie ter inzage gelegd voor raadsleden. Het schenden van geheimhouding is strafbaar. Raadsleden kunnen op verzoek de achterliggende stukken (collegevoorstel en – besluiten, maar ook bijlagen) inzien onder oplegging van geheimhouding.

Mondelinge informatie

Soms wil het college, de raad mondeling informeren over onderwerpen die op zich openbaar of niet geheim zijn, maar op het moment van bespreking nog niet in openbaarheid kunnen worden besproken. Voorbeelden hiervan zijn bijvoorbeeld de stand van zaken bij gerechtelijke procedures (zie bv. de zaak Haarman), bijeenkomsten over personen en grote maatschappelijke impact (zie bv. de Wet sociale werkvoorziening) of financiële belangen voor de gemeente (zie bv. de aanbesteding Nieuw Tijenraan).

Voor het organiseren van deze (besloten) bijeenkomsten en het delen van mondelinge informatie geldt de volgende werkinstructie:
1. Stel een memo op voor de agendacommissie met het verzoek tot het houden van een besloten bijeenkomst voor de gemeenteraad. Let op: dit memo wordt openbaar gepubliceerd (stukken van de agendacommissie zijn openbaar).
2. In het memo wordt met een verwijzing naar het juiste artikel van de Wob of op andere gronden (zoals de vooraankondiging van collegebesluiten met grote maatschappelijke impact) gemotiveerd aangegeven wat het doel en de status van de bijeenkomst zijn. Daarnaast wordt aangegeven hoe raadsleden met de besproken informatie om dienen te gaan inclusief de termijn van de niet openbare informatie. In het protocol is afgesproken dat, indien een raadslid zich niet wil houden aan deze afspraken, de betrokkene niet zal deelnemen aan de bijeenkomst.
3. Stem met de griffier af hoe je wilt omgaan met hetgeen tijdens die bijeenkomst mondeling wordt besproken met name wie namens het college of de raad notuleert. Maak ik je memo duidelijk dat er een audio opname wordt gemaakt. Voeg het verslag en de opname vertrouwelijk toe aan het zaaksysteem en leg deze ter inzage bij de griffie. Ook op mondelinge informatie kan geheimhouding worden opgelegd.

Stem voor juridisch advies af met Jeanet van Olst, voor collegevoorstellen af met de bestuurssecretaris (Coen Knipping) en voor raadsvoorstellen af met de griffier (Jan Bouke Zijlstra)

Bijlage 3. Anonimiseren met Acrobat Pro

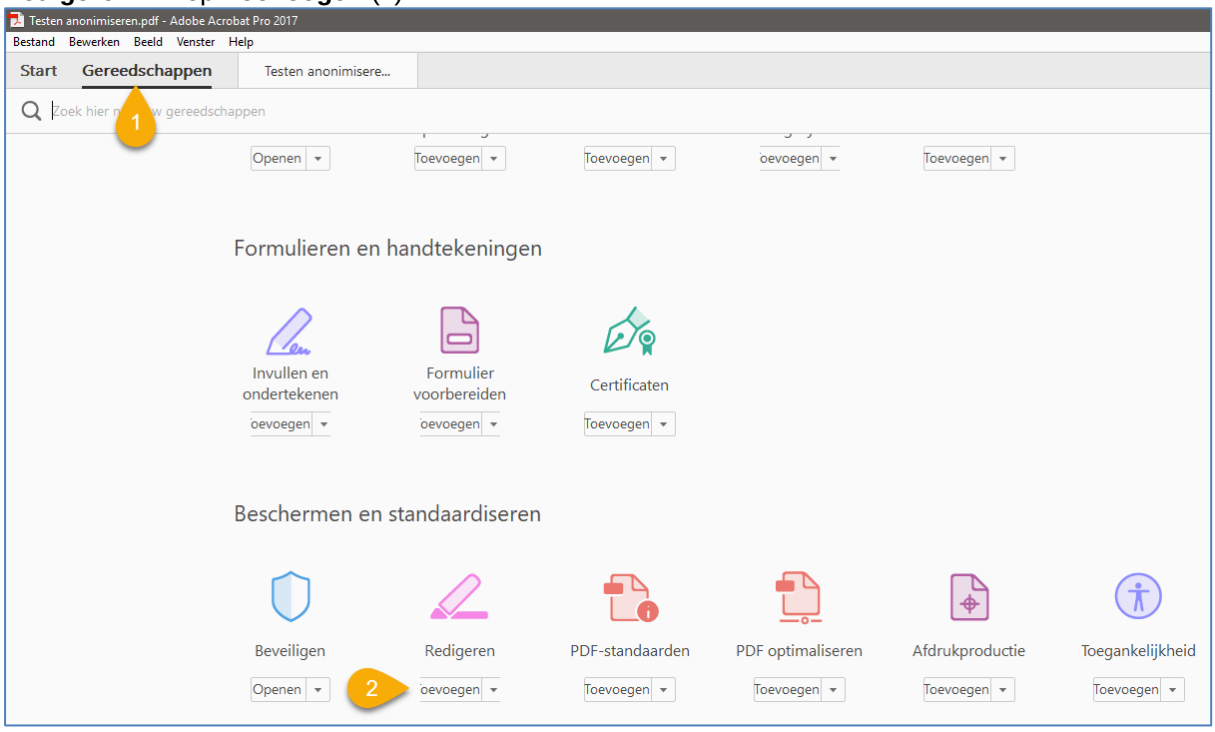
Anonimiseren met Acrobat PRO

Open het document in Acrobat PRO

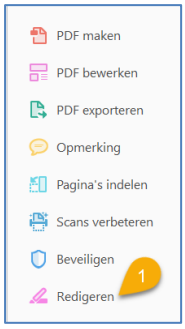
<u>Voorbereiding:</u>
Aan de rechterkant staan de gereedschappen, controleer of daar de optie **Redigeren (1)** bij staat



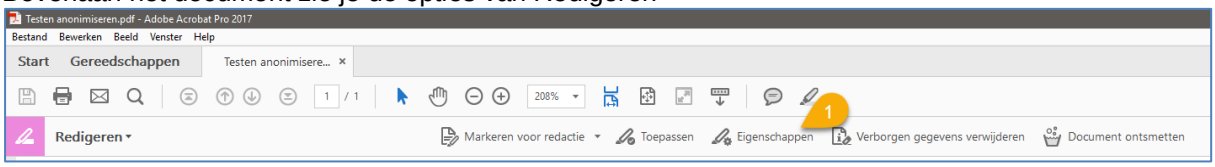
Als dat **<u>niet</u>** zo is, ga naar het tabblad **Gereedschappen**(1), scroll naar beneden en bij de optie **Redigeren** klik op **Toevoegen** (2)



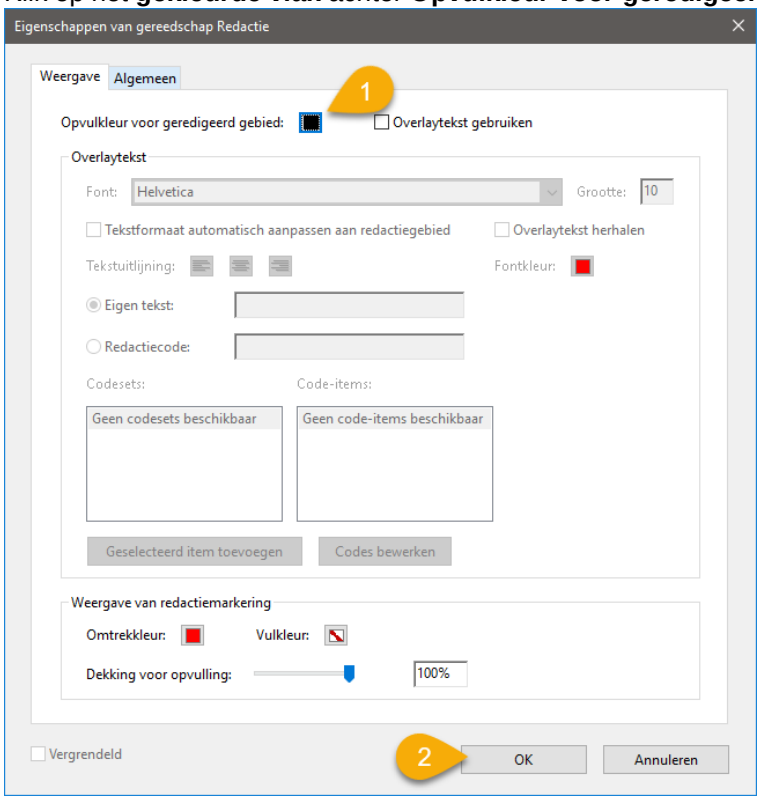
Ga naar het tabblad van het document, en klik rechts van het document op de optie **Redigeren (1)**



Bovenaan het document zie je de opties van Redigeren

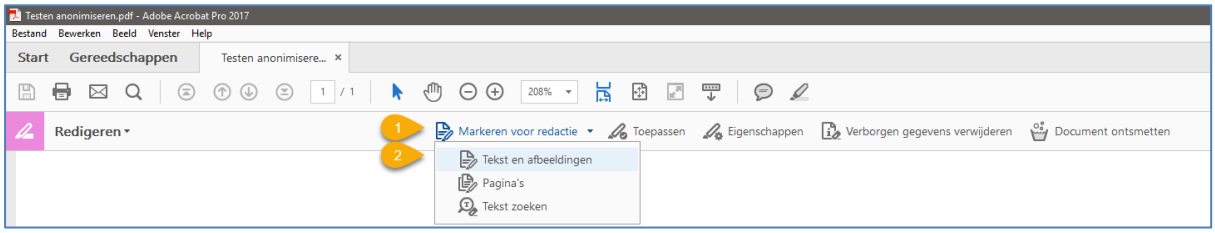


<u>Anonimiseren:</u>
Klik op de knop **Eigenschappen** (1)
Hier kun je instellen hoe je de gewiste gegevens wilt tonen, als zwart vlak of als wit vlak bv, maar kan ook een andere kleur. Standaard is de kleur zwart.
Klik op het **gekleurde vlak** achter **Opvulkleur voor geredigeerd gebied** (1), je ziet onderstaand pop-up met alle kleuren.
Selecteer de kleur dit je wilt, in deze handleiding kies ik voor wit.



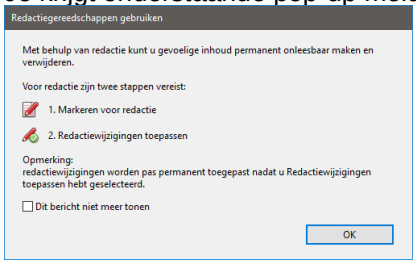


Klik daarna onderaan het scherm op de knop **OK** (2) om dit op te slaan.

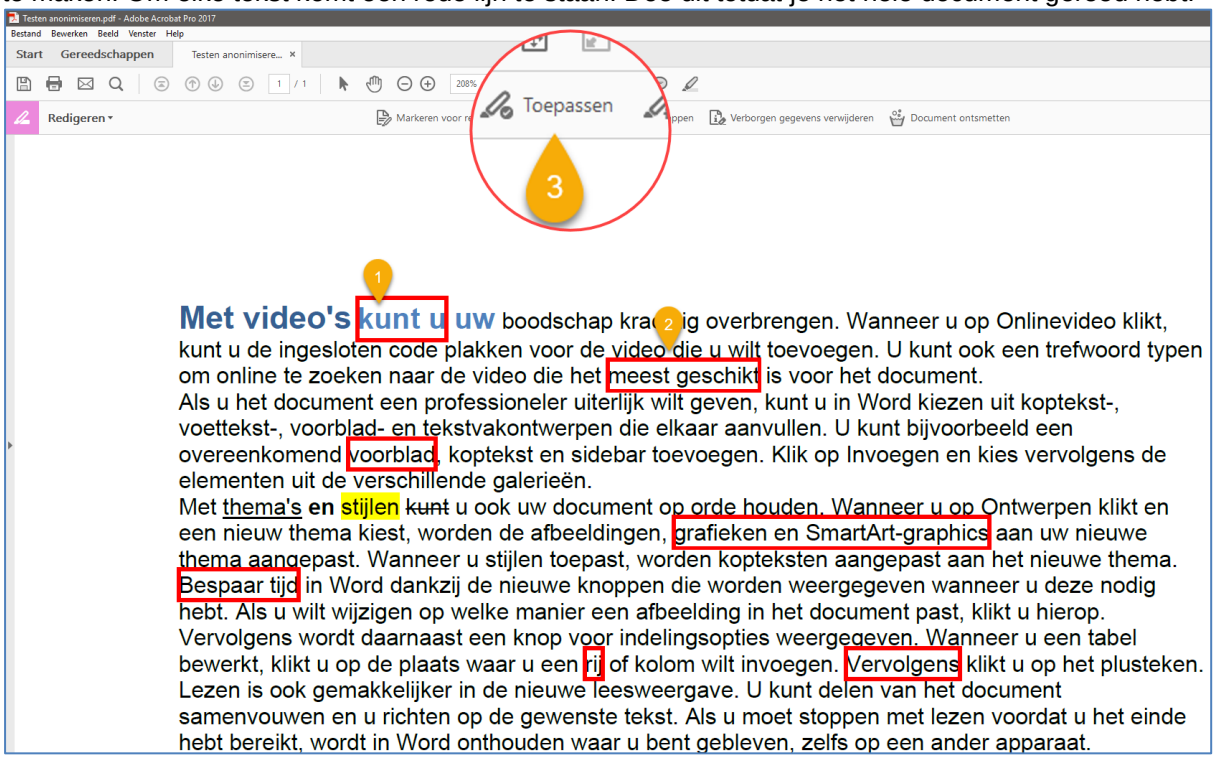


Bovenaan in het menu van Redigeren klik op de optie **Markeren voor redactie** (1) en kies de optie **Tekst en afbeeldingen** (2)

Je krijgt onderstaande pop-up melding ter informatie, klik op OK

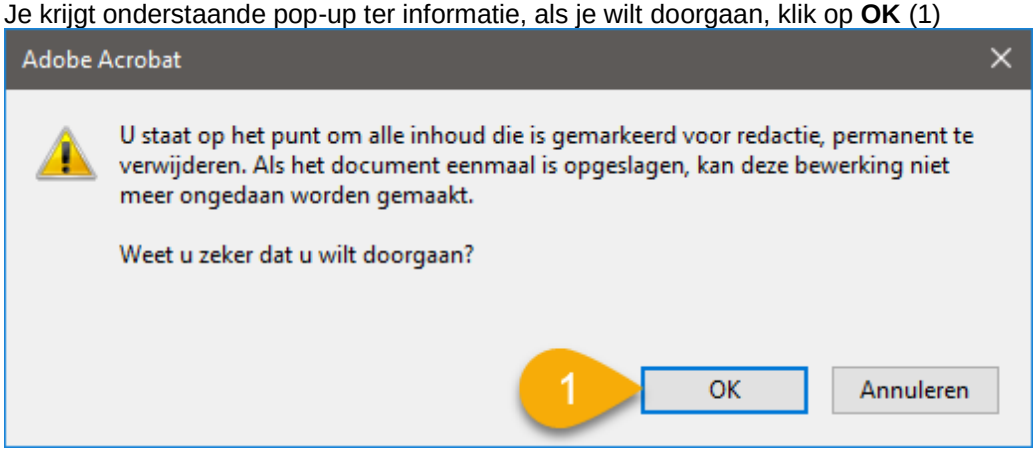


Selecteer in het document de teksten die je wilt verwijderen (1) en (2), door met je cursor een vierkant te maken. Om elke tekst komt een rode lijn te staan. Doe dit totdat je het hele document gereed hebt.

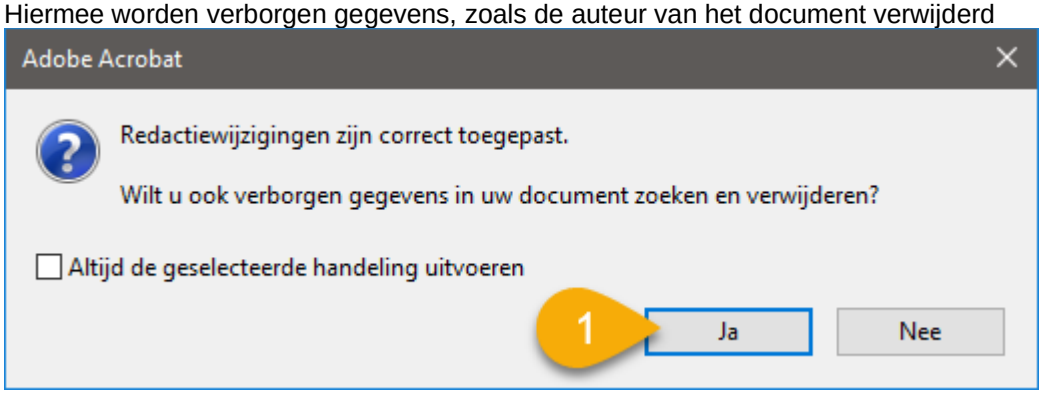


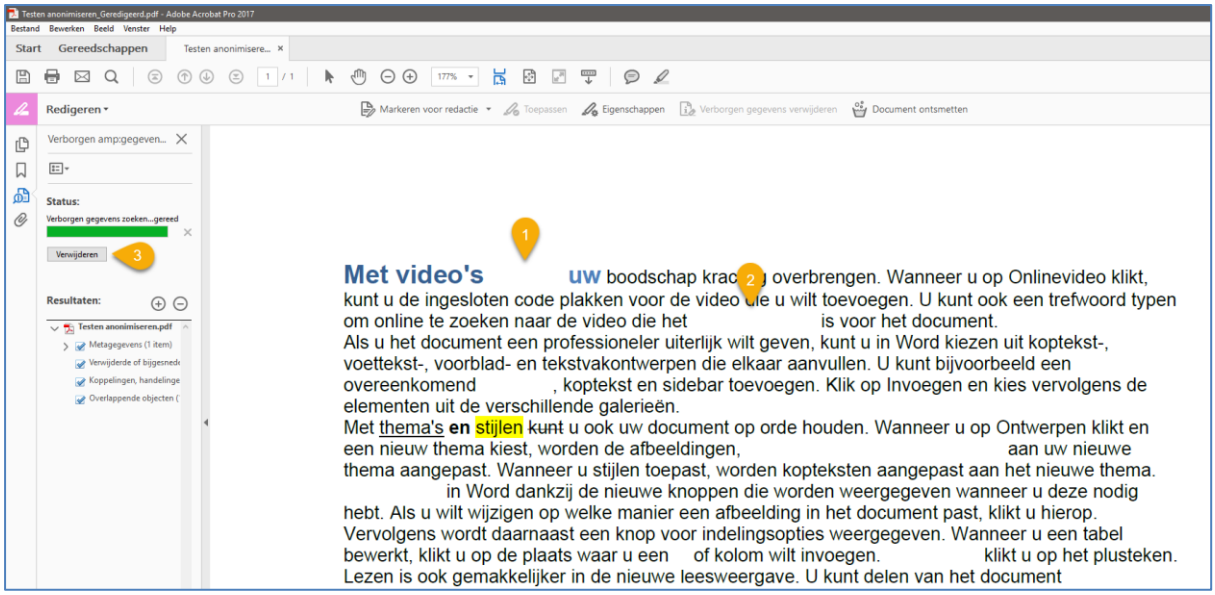
Klik daarna op de knop **Toepassen** (3) in het menu bovenaan het document.

Je krijgt onderstaande pop-up ter informatie, als je wilt doorgaan, klik op **OK** (1)



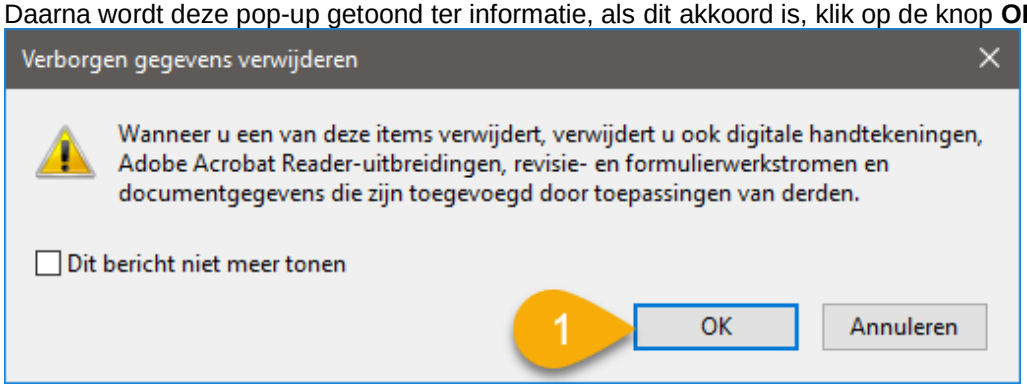
Daarna komt deze pop-up voor het verwijderen van verborgen gegevens, klik op **Ja** (1). Hiermee worden verborgen gegevens, zoals de auteur van het document verwijderd



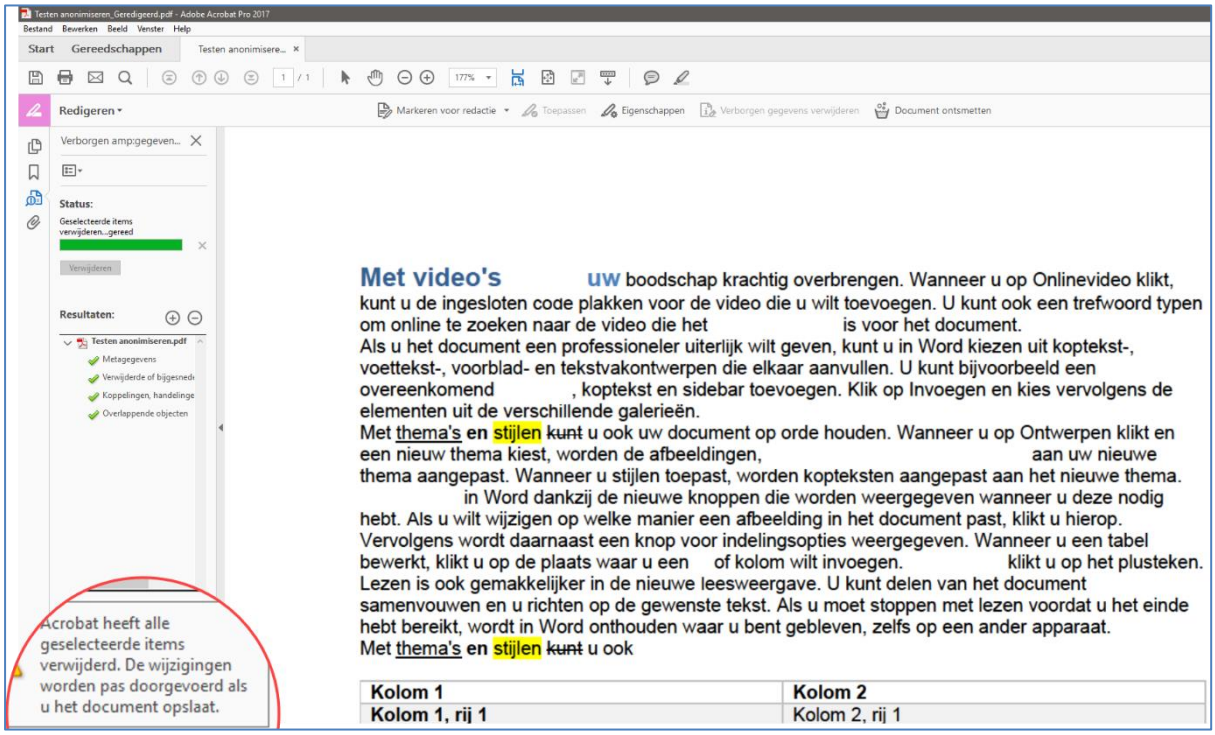


Alle geselecteerde tekst (1) en (2) wordt nu wit getoond (of zwart of de kleur naar keuze) en aan de rechterkant zie je dat het zoeken naar verborgen gegevens gereed is, klik op de knop **Verwijderen** (3)

Daarna wordt deze pop-up getoond ter informatie, als dit akkoord is, klik op de knop **OK** (1)



Rechts onderin wordt een melding getoond dat de wijzigingen worden doorgevoerd als u het document opslaat.



Sla het document op.
Let op: Standaard heeft Acrobat de achtervoegsel "_Geredigeerd" aan de bestandsnaam toegevoegd

Bron: Gevoelige inhoud verwijderen uit PDF's in Adobe Acrobat DC

FB Kantoorautomatisering, februari 2021

Bijlage 4. Anonimiseren met Bluebeam

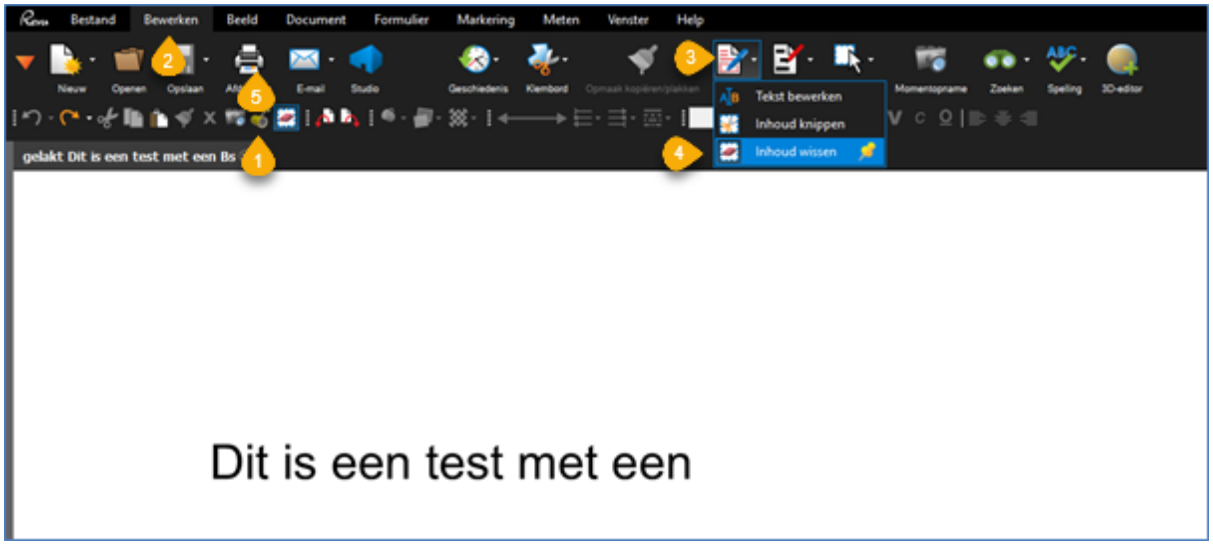
Anonimiseren met Bluebeam

Open het document in Bluebeam.
Sla het document plat met behulp van het **hamertje-icoon (1)** , zorg ervoor dat het vinkje voor Herstellen uit staat (zie afbeelding onderaan de pagina)
Ga naar het tabblad **Bewerken (2)**,
klik op het icoon **Inhoud (3)**
en klik op de optie **Inhoud wissen (4)**

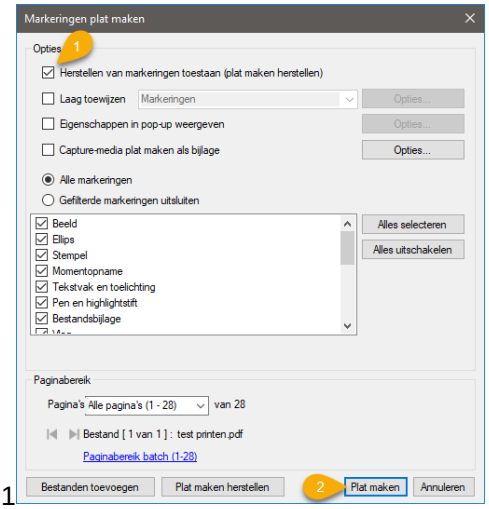
Maak met je cursor een vierkant of rechthoek, en de inhoud wordt gewist.

Eventueel eerst opslaan onder andere naam en dan bewerken.

Nadat de aanpassingen zijn doorgevoerd in het document, klik op het **printer icoon (5)** en kies voor de printer **Microsoft print to PDF** (zie afbeelding hieronder), en sla het bestand op.



Stap 1



stap 5



Bron: [Erase Content (bluebeam.com)]

FB Kantoorautomatisering, februari 2021

Bijlage 5. Procedure meldplicht datalekken DOWR

Procedure meldplicht datalekken DOWR

Uitgave : versie 4
Naam : L.M. Schieving
Mail : l.schieving@deventer.nl

Inleiding

Sinds 1 januari 2016 geldt de meldplicht datalekken. Deze meldplicht houdt in dat organisaties, zoals gemeentes, die met een ernstig datalek te maken krijgen, dit direct moeten melden bij de Autoriteit Persoonsgegevens. De Autoriteit Persoonsgegevens (AP) ziet als toezichthouder namelijk toe op de naleving van de Algemene verordening gegevensbescherming (AVG), waarin de belangrijkste regels met betrekking tot de omgang met persoonsgegevens zijn vastgelegd. Persoonsgegevens zijn alle gegevens betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Dit zijn dus niet alleen naam, adres of burgerservicenummer, maar bijvoorbeeld ook e-mailadressen, (pas)foto's en IP-adressen. In sommige gevallen moeten organisaties bij een ernstig datalek tevens een melding doen bij de mensen van wie de persoonsgegevens zijn gelekt.

Als zich een incident heeft voorgedaan waarbij persoonsgegevens verloren zijn gegaan of wanneer onrechtmatige verwerking van die gegevens heeft plaatsgevonden, of wanneer dit niet met zekerheid uitgesloten kan worden, dan spreken we over een datalek. Dit kan veroorzaakt worden door iets van buitenaf, bijvoorbeeld een hacker die de organisatie binnendringt, maar ook bijvoorbeeld door een medewerker die een laptop met daarop persoonsgegevens in de trein laat liggen. Als een ernstig datalek plaatsvindt, is een gemeente verplicht om hier zonder onnodige vertraging, en binnen 72 uur, een melding van te maken bij de Autoriteit Persoonsgegevens. De ernst van een datalek is afhankelijk van de (potentiële) impact van het datalek op de bescherming van persoonsgegevens en de persoonlijke levenssfeer van betrokkenen. Als het lek nadelige gevolgen kan hebben voor de betrokkenen waarvan persoonsgegevens gelekt zijn, moet een organisatie ook deze betrokkenen informeren. Een datalek kan vervelende situaties opleveren voor zowel de organisatie als voor de betrokkenen. Een organisatie loopt bijvoorbeeld het risico op reputatieschade en op financiële gevolgen, terwijl betrokkenen risico lopen op identiteitsfraude of discriminatie. Vanaf 25 mei 2018 kan de Autoriteit Persoonsgegevens, in geval van een ernstig datalek, organisaties boetes opleggen van maximaal 20 miljoen of 4% van de wereldwijde jaaromzet.

Een gemeente is in veel situaties verantwoordelijk voor de verwerking van (bijzondere) persoonsgegevens, waardoor de meldplicht onder de Algemene verordening gegevensbescherming van toepassing is. Omdat deze wetgeving verlangt dat, wanneer een ernstig datalek geconstateerd is, dit lek zo snel mogelijk, en op correcte wijze, gemeld wordt bij de Autoriteit persoonsgegevens en eventuele betrokkenen is het wenselijk om hier een duidelijke procedure voor te hebben.

Procedure

In dit document wordt de procedure beschreven die gevolgd dient te worden in het geval van een incident dat mogelijk een datalek tot gevolg kan hebben. Deze procedure bestaat uit een aantal te doorlopen processtappen die voor elk incident gelijk zijn. Deze procedure is van toepassing op incidenten die in de gemeente Deventer, de gemeente Olst-Wijhe en de gemeente Raalte plaatsvinden. Gezien de samenwerking tussen deze gemeentes, o.a. op het gebied van bedrijfsvoering (DOWR-samenwerking), kiezen de drie gemeentes om dezelfde procedure te volgen als het gaat om de afhandeling van incidenten.

Meldplicht

Een aantal zaken zijn van belang om deze procedure goed te laten werken. Het is belangrijk dat de medewerkers van de individuele gemeentes voldoende kennis hebben over waar ze incidenten moeten melden en weten welke acties zij bij een incident moeten ondernemen. Elke medewerker dient alert te zijn op bedreigingen met betrekking tot gegevensbescherming. De medewerkers van de DOWR ICT-servicedesk, het aangewezen centrale meldpunt voor incidentmeldingen, zijn bijvoorbeeld getraind in hoe zij met meldingen over incidenten om moeten gaan. De overige medewerkers zijn geïnstrueerd over waar en wanneer zij een melding van een incident moeten doen.

Melding incident

Een melding van een incident komt bij de DOWR ICT-servicedesk terecht doormiddel van het invullen van een meldingsformulier door een medewerker in TOPdesk. Dit formulier is digitaal te vinden onder

de knop ‘meldplicht datalekken’. Een centraal meldingspunt is van belang om het meldingsproces zoveel mogelijk te standaardiseren, om versnippering van geregistreerde meldingen te voorkomen en om een totaaloverzicht te behouden van afgehandelde meldingen. De teammanager van de medewerker die de melding bij de servicedesk zou moeten doen, ziet erop toe dat dit formulier bij een incident ook daadwerkelijk wordt ingevuld. Wanneer er een incident bij de servicedesk wordt gemeld, krijgen de Privacy Officer (PO), de privacyadviseur van de gemeente waar het incident betrekking op heeft, de Information Security Officer (ISO) en de Chief Information Security Officer (CISO) een kopie van deze melding binnen. De medewerker van de DOWR ICT-servicedesk wijst de PO van de gemeente waar het incident betrekking op heeft aan als behandelaar. Dit kan de PO van de gemeente Deventer en/of de gemeente Olst-Wijhe en/of de gemeente Raalte zijn.

Onderzoek en impactanalyse

De PO heeft een coördinerende rol op het moment dat er zich een incident heeft voorgedaan. De desbetreffende PO neemt contact op met de medewerker die de melding heeft gedaan en probeert zoveel mogelijk informatie over het incident van de medewerker te verkrijgen. De PO maakt aan de hand van deze informatie een inschatting over of er daadwerkelijk sprake is van een datalek en of er direct actie zal moeten worden ondernomen.

Wanneer het gaat om een incident, dat is ontstaan door een beveiliginginbreuk, wordt de vraag of er direct actie zal moeten worden ondernomen samen met de Information Security Officer (ISO) beantwoord. Wanneer het tevens een ICT-gerelateerd incident betreft, wordt daarbij ook het Computer Emergency Response Team (CSERT) en de Chief Information Security Officer (CISO) ingeschakeld. Het SCERT is ingesteld om snel en adequaat te kunnen reageren op dit soort incidenten. Het CSERT wordt door de CISO bij elkaar geroepen. Afhandeling van het incident door het CSERT verloopt volgens het incident management proces. De verzoeken die het CSERT uitstuurt richting de gemeentelijke organisatie om inzichtelijk te krijgen wat er precies gebeurt is, en wat kan helpen bij het dichten van het lek, dienen zo spoedig mogelijk door de organisatie opgevolgd te worden. De medewerkers van de desbetreffende gemeente dienen daarom goed op de hoogte te zijn van het belang en de urgentie van de verzoeken vanuit dit team.

Maatregelen

De PO van de betreffende gemeente is verantwoordelijk voor het ontwerpen van maatregelen die de ontstane schade minimaliseren (herstelmaatregelen) en maatregelen teneinde nieuwe vergelijkbare incidenten te voorkomen (structurele maatregelen). Wanneer het gaat om een beveiligingsincident wordt de vraag welke herstelmaatregelen er moeten worden genomen samen met de ISO beantwoord. Daarbij wordt de CISO geconsulteerd.

De teammanager(s) is/zijn verantwoordelijk voor de uitvoering van de herstelmaatregelen en de structurele maatregelen.

Melding datalek

Als de PO tot de conclusie komt dat er sprake is van een datalek is de PO van de betreffende gemeente verantwoordelijk voor het ‘onverwijld’ doen van de eerste melding bij de AP via het webformulier op de website van de AP. Ondanks dat deze processtap bij alle drie de gemeentes op gelijke wijze wordt ingevuld, blijft elke gemeente individueel aansprakelijk voor het melden van een datalek bij de AP. Wanneer er bijvoorbeeld sprake is van een incident wat alle drie de gemeentes betreft, en dit incident ook gemeld moet worden, dan doen alle drie de PO’s een melding bij de AP voor hun eigen gemeente.

Bij uitbesteding van taken waarbij sprake is van verwerking van persoonsgegevens door verwerkers blijft de desbetreffende gemeente verantwoordelijk voor het melden van een datalek. Er zijn dan ook met alle verwerkers afspraken gemaakt over de gestelde eisen op het gebied van gegevensbescherming en over het onmiddellijk melden van incidenten. In elke verwerkersovereenkomst wordt een vakafdeling van de betreffende gemeente genoemd waar een verwerker incidenten kan doorgegeven. Een medewerker van deze afdeling meldt vervolgens het incident bij de DOWR ICT-servicedesk doormiddel van het hierboven genoemde meldingsformulier. De te doorlopen stappen van de procedure zijn vanaf dat moment niet verschillend van wat hierboven al is beschreven.

De PO van de betreffende gemeente doet de melding bij de AP met behulp van de gegevens die door de gemeentelijke organisatie of de verwerker worden aangeleverd. Er wordt gewerkt conform de meldplicht datalekken van de Autoriteit Persoonsgegevens[1]. Als het gaat om een datalek, dat is ontstaan door een beveiligingsincident, ICT-gerelateerd of niet, is de I-werkorganisatie verantwoordelijk voor het aanleveren van de informatie die de betreffende PO nodig heeft om een melding te kunnen doen.

Als de eerste melding is gedaan, wordt door de desbetreffende PO direct beoordeeld of het nodig is om ook een melding te doen bij betrokkene(n). Wanneer een datalek voor de betrokkene(n) waarschijnlijk ongunstige gevolgen heeft, moet het datalek aan deze betrokkene(n) worden gemeld. Aan de hand van de impact van het datalek en de kans dat die impact optreedt, wordt bepaald of een dergelijke melding nodig is. Daarbij wordt de Functionaris Gegevensbescherming (FG) geraadpleegd. Het kan dus voorkomen dat een datalek wel bij de AP wordt gemeld, maar niet aan betrokkenen, omdat hun persoonsgegevens door bepaalde maatregelen onbegrijpelijk of ontoegankelijk zijn geworden en er dus geen sprake is van ‘waarschijnlijk ongunstige gevolgen’.

Het informeren van betrokkene(n) vindt bij voorkeur op dezelfde dag plaats. Wanneer betrokkenen moeten worden geïnformeerd, stelt de PO de directie, de strategisch communicatieadviseur en de persvoorlichter daarvan op de hoogte. Wanneer er sprake is van een datalek dat is ontstaan door een beveiligingsincident informeert de PO tevens de CISO.

De PO van de betreffende gemeente is vervolgens verantwoordelijk voor de follow-up van de melding. Indien de eerste melding aan de AP niet compleet was, wordt deze door de PO aangevuld.

Communicatie en documentatie

De berichtgeving aan betrokkene(n) is ter beoordeling van de strategisch communicatieadviseur en de persvoorlichter. De berichtgeving moet wel de wettelijk vereiste informatie bevatten. De PO wordt daarom geconsulteerd bij de vraag hoe en wat er naar betrokkene(n) moet worden gecommuniceerd. De PO verstrekt de voor de communicatie benodigde gegevens. Wanneer er sprake is van een datalek, dat is ontstaan door een ICT-gerelateerd beveiligingsincident, wordt ook de CISO geconsulteerd.

De communicatie over een datalek kan worden overgenomen door andere partijen zoals lokale, landelijke of sociale media, eigen medewerkers of ketenpartners. Als gevolg van ruis in de communicatie kan een datalek alsnog onnodig escaleren. Belangrijk is dat de desbetreffende gemeente de regie behoudt over de communicatie van een ernstig datalek dat gemeld is bij het AP en eventueel aan betrokkenen. Bij de uitwerking van de communicatiestrategie door de strategisch communicatieadviseur en de persvoorlichter vindt dan ook afstemming plaats welke doelgroepen of overige partijen worden geïnformeerd over het datalek en op welke wijze. Timing is hierbij van belang. Zeker indien de melding al heeft plaatsgevonden aan betrokkene(n). Via een persbericht stelt de gemeente de media op de hoogte, eventueel aanvullend met een persconferentie voor het stellen van vragen. Deze werkwijze wordt afgestemd op de grootte van het datalek.

Na afsluiting van een incident registreert de PO het incident in de daarvoor ingerichte digitale omgeving, samen met de eventuele ontvangstbevestiging van de melding, en de onderliggende documentatie. Deze registratie is aanvullend op dat wat in de DOWR ICT-servicedesk wordt geregistreerd. In deze servicedesk wordt namelijk vastgelegd wat voor een acties er zijn ondernomen in de periode voor de eventuele vaststelling van een datalek. De PO, of diens vervanger, documenteert daarna in de digitale omgeving de inbreuken in verband met persoonsgegevens, met inbegrip van de feiten omtrent het incident, de gevolgen daarvan, de genomen herstelmaatregelen en de genomen structurele maatregelen. De PO documenteert alleen de voor dit doel noodzakelijke gegevens.

Dit is de laatste stap van de procedure en hiermee is het proces afgerond. In de bijlage is een tabel opgenomen met de rollen en verantwoordelijkheden van de personen die bij deze procedure zijn betrokken.

[1] https://autoriteitpersoonsgegevens.nl/nl/melden/meldplicht-datalekken

Bijlage bij Procedure datalekken

Incidenten met betrekking tot persoonsgegevens
handeling ← → beveiliging

		Geen ICT	ICT
Melding incident bij ICT-servicedesk	R = teammanager(s)/ medewerker(s) I = PO/ ISO/ CISO		
Onderzoek en impactanalyse incident	R = PO	R = ISO/PO	R = ISO/PO C = CSERT/ CISO
Ontwerp te treffen maatregelen	R = PO	R = ISO/PO C = CISO	
Uitvoering maatregelen	R = teammanager(s)		
Melding datalek (AP/betrokkene(n))	R = PO C = FG A = B&W I = Directie/ strategisch communicatieadviseur/ persvoorlichter	R = PO C = FG A = B&W I = Directie/ strategisch communicatieadviseur/persvoorlichter/CISO	
Communicatie	R = Directie C = PO S = strategisch communicatieadviseur/persvoorlichter		R = Directie C = PO/CISO S = strategisch communicatieadviseur/per svoorlichter
Documentatie	R = PO A = B&W I = gemeenteraad		

R (*Responsible)*
De persoon die (feitelijk) verantwoordelijk is voor de uitvoering. Verantwoording wordt afgelegd aan de persoon die *accountable* is.

A (*Accountable*)
De persoon die (eind)verantwoordelijk is.

S (*Supportive*)
De persoon die het resultaat ondersteunt.

C (*Consulted*)
De persoon die (mede) richting geeft aan het resultaat. Hij/zij wordt voorafgaand aan beslissingen of acties geraadpleegd.

I (*Informed*)
De persoon die geïnformeerd wordt over de beslissingen.