Ministerie van Financiën

Akkoord en dank voor aanpassingen.
2e nog 1 kleine verduidelijking bij antwoord 3.
Brief getekend JvH 2/2

TER BESLISSING
Aan
de minister

SG-Cluster
Directie Digitalisering & Informatisering

Persoonsgegevens

nota

DDI 155040 beantwoording vragen van Hijum en Omtzigt (NSC) over chatarchivering

Datum
1 februari 2024

Notanummer
2024-0000155040

Bijlagen
1. Aanbiedingsbrief
2. Antwoorden
3. BEDR 117790
4. BEDR 243074
5. BEDR 318327

Aanleiding

Op 13 oktober 2023 is antwoord gegeven op vragen van de vaste commissie voor Financiën over chatarchivering en het archief voor de hotspot covid-19 bij Financiën[1]. Op 2 januari jl. hebben de leden van Hijum en Omtzigt hier aanvullende vragen over gesteld.

Beslispunten

- Bent u akkoord met de aanpassingen in de beantwoording en het versturen van de bijgaande beantwoording (bijlage 2)? Als u akkoord bent dan verzoek ik u de aanbiedingsbrief (bijlage 1) te ondertekenen.
- Bent u akkoord met het openbaar maken van de nu voorliggende beslisnota en bijgevoegde eerdere nota's (bijlagen 3, 4, 5 en 6) conform de beleidslijn Actieve openbaarmaking nota's?

Kernpunten

- De beantwoording is als volgt aangepast:
  - Uw suggesties voor tekstuele wijzigingen in vragen 3, 5, 8 en 10 zijn overgenomen.
  - In het antwoord op vraag 3 is concreter gemaakt van wie er wel en van wie er geen chatberichten zijn veiliggesteld, op zodanige manier dat dit niet terug te leiden is naar individuele ambtenaren.
  - In het antwoord op vraag 8 is nu aangegeven welke rijksbrede richtlijnen beschikbaar moeten zijn voor we chatberichten in het hotspotarchief kunnen opnemen, in plaats van alleen veilig stellen.
- De vragen van NSC gaan over de archivering van chatberichten door politieke en ambtelijke top in het algemeen en voor de hotspot Covid-19 in het bijzonder. Op uw verzoek is de beantwoording van de vragen zo concreet mogelijk en uitgebreider dan in de voorgaande versie.
- Bewindspersonen en ambtelijke leiding zijn sinds mei 2020 meerdere keren geïnformeerd dat zakelijk berichtenverkeer onder reikwijdte van Woo en Archiefwet 1995 valt. Sinds 4 oktober 2022 worden bewindspersonen geacht geen berichten meer te verwijderen. De instructies hiervoor zijn steeds aangescherpt om te voldoen aan de rijksbrede richtlijnen

[1] Kamerstuk 25295-2108 Lijst van vragen en antwoorden over het afbakeningsdocument van het ministerie van Financiën met het overzicht van beschikbare informatie over de hotspot Covid-19

- Het periodiek ophalen van chatberichten bij politieke en ambtelijke leiding is voorzien, maar de start van de dienstverlening is aanzienlijk vertraagd. Naar verwachting is april 2024 de eerste ronde klaar, waarbij bij de huidige bewindspersonen en ambtelijke leiding ook de chatberichten uit de periode van de Hotspot Covid-19 meegenomen wordt.
- Op 4 januari jl. zijn de berichten op de telefoon van mw. Kaag veiliggesteld, met terugwerkende kracht tot 1/1/2020. Waarbij ook haar berichtenverkeer als bewindspersoon bij BZ is meegenomen.
- Van het vorige kabinet zijn alleen de chatberichten van de staatssecretaris voor Toeslagen en Douane mw. Van Huffelen veiliggesteld.
- Binnen de ambtelijke leiding zijn sinds maart 2020 (aanvang hotspot Covid-19 bij FIN) op niveau van (plaatsvervangend) DG's 11 personele wisselingen geweest. Zes functionarissen zijn nog werkzaam bij Financiën, hiervan worden de chatberichten alsnog veiliggesteld. Vijf functionarissen zijn niet meer werkzaam bij Financiën. Daarvan zijn geen chatberichten veiliggesteld. 4 daarvan zijn nog in dienst van de overheid. Met hen wordt contact gelegd om te inventariseren in hoeverre berichten alsnog kunnen worden veiliggesteld.
- De beantwoording van de Kamervragen is afgestemd met de BZK/CIO Rijk voor wat betreft de rijksbrede maatregelen en met BZ voor wat betreft het veiligstellen van chatberichten van mw. Kaag als minister van BZ.

Toelichting

- FIN volgt het rijksbrede beleid ten aanzien van archivering van chatberichten van bewindspersonen.
- In 2022 is al begonnen met het uitwerken van maatregelen om chatberichten 2-maandelijks op te halen bij bewindspersonen en ambtelijke leiding. Het opzetten vergde meer doorlooptijd dan vooraf ingeschat vanwege enerzijds de stand van de techniek en anderzijds het uitwerken van privacy- en beveiligingseisen. Hier was binnen het rijk nog weinig ervaring mee en een aantal randvoorwaarden zijn, ook nu nog niet ingevuld, zoals een advies over bewaartermijnen (model selectielijst) of het schonen (opknippen van conversaties) en valideren (een toets op relevantie door de bewindspersoon of topambtenaar zelf). In de tussentijd is steeds aangegeven dat zakelijke chatberichten niet verwijderd mogen worden.
- Inmiddels kan de directie D&I starten met het ophalen van chatberichten. Verwacht wordt dat april 2024 de eerste ronde klaar is. Daarbij worden met terugwerkende kracht tot 1 januari 2020, of datum aantreden c.q. in dienst treden, chatberichten veiliggesteld. Periodiek wordt met alle betrokkenen afspraken ingepland om de aanwas van berichten veilig te stellen.
- De ondersteuning beperkt zich tot Whatsapp-, SMS- en iMessage berichten. Conversaties in andere apps, zoals Signal, kunnen niet geëxporteerd worden. Het gebruik hiervan wordt daarom vooralsnog afgeraden.

Communicatie

Woordvoering is meegenomen in de afstemming van de antwoorden.

Politiek/bestuurlijke context
Naar aanleiding van diverse adviezen over de archivering en verwijdering van chatberichten door de minister-president hebben de departementen en bewindspersonen instructie ontvangen over chatarchivering om voortijdige vernietiging van zakelijk berichtenverkeer te voorkomen.
In het begrotingsdebat AZ op 18 januari jl. zijn door NSC wederom vragen gesteld over chatarchivering van de MP.

Informatie die niet openbaar gemaakt kan worden
Niet van toepassing.

Doc nr.	Datum	Naam document
1	7-4-2022	Nota-min - Gebruik privé-apparatuur en -accounts voor zakelijke informatie
2	4-10-2022	Nota-min/stas - Veiligstellen chatberichten en sms bewindspersonen
3	12-12-2022	Nota - stasFB - Veiligstellen chatberichten en SMS
4	25-1-2024	Nota - min - Beantwoording vragen leden Van Hijum en Omtzigt over chatarchivering

Ministerie van Financiën

TER INFORMATIE
Aan
de minister

Directie Bedrijfsvoering

Persoonsgegevens

nota

Gebruik privé-apparatuur en -accounts voor zakelijke informatie

Datum
7 april 2022

Notanummer
2022-0000117790

Bijlagen
1. gedragsregeling digital
2. BR notitie over archive

Aanleiding

De voormalige minister van VWS zijn vragen gesteld over het gebruik van privé e-mailadres voor zakelijke correspondentie. Deze nota gaat in op gebruik van privémiddelen voor zakelijke correspondentie en openbaarheid en archivering.

Kern

- Uitgangspunt is: uw zakelijke correspondentie wordt na uw ambtstermijn bewaard en op termijn overgedragen aan het Nationaal Archief, waar deze informatie raadpleegbaar is.
- Sms- en WhatsApp-berichten over een bestuurlijke aangelegenheid die u tijdens uw ambtstermijn verstuurt, moet u laten archiveren en zijn opvraagbaar onder de Wet openbaarheid van bestuur (hierna: Wob). Ook als u hiervoor uw privé-telefoon gebruikt.
- De Gedragsregeling voor de digitale werkomgeving Rijksoverheid (Bijlage 1) schrijft voor dat een privé e-mailadres of telefoonnummer niet voor zakelijke correspondentie wordt gebruikt.

Toelichting

Berichtenapps

- De Afdeling Bestuursrechtspraak van de Raad van State heeft op 20 maart 2019 geoordeeld dat sms- en WhatsApp-berichten onder de reikwijdte van van de Wob vallen. Op 3 juli 2019 is in het SG-overleg aanvullend beleid vastgesteld voor het gebruik van berichtenapps en het bewaren van chatberichten binnen het Rijk. Dit beleid omvat de volgende drie speerpunten:
    - Het gebruik van berichtenapps voor formeel zakelijke communicatie wordt zoveel mogelijk beperkt;
    - Het gebruik van berichtenapps voor bestuurlijke aangelegenheden wordt ontraden;
    - Het berichtenverkeer dat toch plaatsvindt, wordt periodiek geschift. Te archveren berichten worden handmatig geëxporteerd en veiliggesteld, tenzij deze al op een andere wijze zijn vastgelegd en gearchiveerd, bijvoorbeeld in een e-mail, nota of in een verslag. Niet archiefwaardige berichten worden verwijderd.
- In de BR van 26 maart 2020 is de volgende praktische aanpak vastgesteld (bijlage 2):
    - In uw chatverkeer met ambtenaren ligt het voortouw van het vastleggen van chatberichten m.b.t. bestuurlijke besluitvorming bij de ambtenaren.

- In uw chatverkeer met andere bewindspersonen of externen wordt u geacht berichten te herkennen dat het een bestuurlijke aangelegenheid betreft en aan te geven dat dit gearchiveerd moeten worden.
- Als berichten met bestuurlijke besluitvorming consequent ook op een andere wijze worden vastgelegd kunnen bewindspersonen en BR-leden iedere week hun berichten wissen.

Transparantie en de Wob

- Alle documenten, waaronder e-mails, notities, sms- en WhatsApp-berichten etc., met daarin informatie over een bestuurlijke aangelegenheid, die bij een minister, staatssecretaris of ander bestuursorgaan berusten, moeten op verzoek openbaar worden gemaakt, tenzij de Wob een weigeringsgrond kent.
- Het zakelijk corresponderen via privé e-mailadressen en telefoonnummers is ongebruikelijk en ongewenst. Enerzijds vanwege de beveiligings- en privacy-issues die het dit met zich mee brengt. Anderzijds vanwege de openheid die de Wob stelt aan het handelen van een bewindspersoon. Weliswaar valt uw privécorrespondentie en privégebruik van telefoons en andere communicatiemiddelen niet onder de Wob, maar het zakelijk gebruik van die communicatiemiddelen wel. Dit alles tezamen maakt dat de richtlijn binnen het Rijk is dat een privé e-mailadres of telefoonnummer niet gebruikt wordt voor zakelijke correspondentie.
- Waar het gaat om staatsgeheime informatie is zonder meer niet toegestaan om via privémail of telefonisch te corresponderen.

Archivering van correspondentie en documenten

- Overheidsinformatie wordt gearchiveerd met als doel borgen van zorgvuldigheid en continuïteit van de bedrijfsprocessen en bij te dragen aan de publieke, democratische controle op het besluitvormingsproces.
- De zakelijke e-mailcorrespondentie van bewindspersonen wordt gezien als vallend onder de categorieën van overheidsinformatie die permanent bewaard wordt. Dat zijn grosso modo:
  - Voorbereiding, bepaling, evaluatie en verantwoording van beleid
  - (her)Inrichting van organisaties
  - Beleidsuitvoering die gerelateerd is aan of direct voortvloeit uit het voor het Koninkrijk der Nederlanden bijzondere tijdsomstandigheden en incidenten. Hierbij gaat het om hotspots zoals de toeslagenaffaire of de covid-19 pandemie.
- Uw privécorrespondentie via zakelijke media valt niet onder archiefwaardig materiaal. Echter, er kan niet gegarandeerd worden dat in de totaliteit van uw mailbox geen privémails in het archief belanden. Mede om die reden wordt afgeraden privé te corresponderen via uw zakelijk mailaccount. Dit geldt ook voor de privé correspondentie via de zakelijke telefoon.
- Archief blijft gedurende 20 jaar op het departement, na 20 jaar[1] wordt het archief overgebracht naar het Nationaal Archief en daarmee in principe openbaar. Aan die openbaarheid kunnen beperkingen gesteld worden, vergelijkbaar met beperkingsgronden die de Wob kent.

Informatie die niet openbaar gemaakt kan worden

Niet van toepassing.

[1] In het wetsvoorstel voor de Archiefwet 2021 wordt deze termijn verkort naar 10 jaar

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Gedragsregeling voor de digitale werkomgeving [Algemene Versie]

Versie	1.0
Datum	September 2021
Status	Definitief

Inhoud

Inleiding

Zonder informatie kunnen we ons werk niet doen. Delen van informatie binnen en buiten de overheid hoort daarbij. Die informatie moet dan wel correct, actueel en natuurlijk ook vindbaar zijn.
De overheid heeft een publieke taak en transparant zijn naar de samenleving is een kernwaarde. We maken informatie waar mogelijk openbaar en geven inzicht in besluitvorming.
Als je goed omgaat met informatie draag je dus bij aan de betrouwbaarheid, controleerbaarheid en zorgvuldigheid van de rijksoverheid. Burgers en bedrijven verwachten dit ook van ons.

Belangrijke bijkomende aspecten zijn informatiebeveiliging en privacy. We zijn erg afhankelijk van informatie en we werken met persoonsgegevens en andere vertrouwelijke informatie. Het tijdstip waarop en de plek waar we werken is steeds flexibeler. Daarnaast zijn we steeds vaker een doelwit van cybercriminelen met geavanceerde digitale aanvallen gericht op spionage, sabotage en zelfs terrorisme. Zorgvuldig omgaan met informatie betekent dus ook veilig en privacy-verantwoord.

Ons gedrag is dus van groot belang. Met technische en organisatorische maatregelen beperken we al veel risico's, maar dat is niet voldoende. Deze gedragsregeling beschrijft wat je kunt doen om goed om te gaan met informatie zodat die volledig, actueel en vindbaar is en wat je kunt doen om te zorgen dat die informatie veilig en de privacy gewaarborgd blijft. Als we met zijn allen deze regels toepassen, kunnen we beter ons werk doen en worden we digitaal weerbaarder.

Het past bij de eed of belofte waarin je hebt toegezegd om je te gedragen zoals 'een goed ambtenaar betaamt'. Het past ook bij de betrouwbaarheid die de maatschappij van de overheid verwacht. Je houden aan deze regels is dus niet vrijblijvend; die plicht volgt ook uit wet- en regelgeving zoals de Archiefwet, AVG, Voorschrift Informatiebeveiliging Rijksdienst en BIO. Een fout maken of je vergissen kan iedereen overkomen, maar bij opzet en nalatigheid kan het leiden tot personele maatregelen.

De opbouw van het document is als volgt:
- positionering van het document waaronder de scope;
- goede omgang met informatie;
- beveiligingsaspecten in verschillende werksituaties: op kantoor, thuis, onderweg;
- privacy-aspecten;
- omgang met risico's zoals cybercriminaliteit.

Het document eindigt met enkele bijlagen, waaronder een overzicht van gerelateerde documenten. Naar deze documenten wordt in de tekst verwezen met een getal tussen vierkante haken, bv [1].

Laten we er met elkaar voor zorgen dat informatie volledig, actueel en vindbaar is en dat we op een veilige en verantwoorde manier werken. Zo kunnen incidenten worden voorkomen. Help elkaar hierbij zoveel mogelijk. Zo dragen we bij aan de betrouwbaarheid van de Rijksoverheid.

1 Positionering en scope

1.1 Scope

Deze gedragsregeling gaat vooral over digitale informatie en informatiesystemen. Het gaat daarbij om het werken met informatie zodat die volledig, actueel en vindbaar is. En het gaat ook om een veilige en privacy verantwoorde manier van werken. Digitaal werken raakt aan het werken met papieren informatie en fysieke beveiliging. Die onderwerpen komen beperkt aan bod.

Deze gedragsregeling geldt niet alleen voor Rijks- en Defensieambtenaren maar voor alle leidinggevenden en medewerkers die voor de Rijksoverheid werkzaamheden uitvoert en daarbij gebruik maakt van de digitale werkomgeving van de Rijksoverheid. Dit zijn de eigen medewerkers en ook uitzendkrachten en andere externen, medewerkers van zakelijke partners, stagiaires, trainees en vrijwilligers. Deze groep wordt verder aangeduid met (rijks)medewerkers.

Dit document beperkt zich tot regels die voor iedere medewerker gelden. De volgende zaken vallen buiten scope:
- regels voor staatsgeheime informatie, inclusief bedreigingen door statelijke actoren en georganiseerde misdaad;
- specifieke regels voor reizen naar risicolanden;
- informatie waarvoor andere bijzondere regels gelden, zoals medische informatie.

Deze situaties vergen heel specifieke regels die op een klein deel van ons van toepassing zijn.

1.2 Gerelateerde documenten

De regels in dit document zijn gebaseerd op vastgesteld beleid. Dit document vervangt alle gedragsregelingen op het gebied van de digitale werkomgeving van voor 2017. Hierop gelden twee uitzonderingen:
- *Gedragscode Integriteit Rijk [1]*: Dit omvat afspraken op het gebied van integriteit en helpt bij het maken beslissingen op dit gebied.
- *Handreiking Online Communicatie Rijksambtenaren [2]*: hierin staat hoe je integer en professioneel gebruik maakt van online voorzieningen waaronder social media.

Voor werkinstructies, handleidingen en dergelijke wordt naar achterliggende documenten verwezen (zie bijlage 3).

1.3 Eigen versie van de gedragsregeling

Organisaties binnen de Rijksoverheid kunnen een eigen versie van de gedragsregeling digitale werkomgeving uitbrengen:

- In de bijlagen kunnen organisaties aanvullingen doen voor de eigen contactpersonen, voorzieningen en verwijzingen.
- Organisaties binnen de rijksoverheid kunnen in samenspraak met hun medezeggenschap ook aanvullende (zwaardere) regels vaststellen (lichter is niet toegestaan), bijvoorbeeld omdat de organisatie veel vertrouwelijke informatie verwerkt of omdat de organisatie extra gevoelig is voor incidenten en negatieve berichtgeving in de media.

Als een organisatie een eigen versie maakt, wordt de naam van de organisatie toegevoegd in de titel op de voorpagina.

1.4 Personele processen

Iedere rijksmedewerker is zelf verantwoordelijk voor zijn eigen gedrag en de keuzes die hij maakt. Het aan de gedragsregeling houden is belangrijk en niet vrijblijvend [23]. Fouten en vergissingen maken is menselijk. Maar je niet aan deze regels houden kan een blijk zijn van disfunctioneren, plichtsverzuim en niet-integer gedrag.

Als een rijksmedewerker zich niet aan de gedragsregels houdt, kan dat diens leidinggevende aanleiding zijn om dat te bespreken. Dit kan leiden tot nadere afspraken, een training en bij ernstiger situaties tot een aantekening in je personeelsdossier en integriteitonderzoek [24]. Dit is iets tussen jou en je leidinggevende en loopt via de daarvoor vastgestelde procedures.

1.5 Beheer van het document

Voortdurend komt er nieuwe wet- en regelgeving, zoals de Wet Open Overheid (Woo) en de nieuwe Archiefwet. En ook zijn er programma's zoals Hybride werken, Ambtelijk Vakmanschap en Verbetering Informatiehuishouding (IHH). Deze leiden tot nieuwe en vernieuwde gedragsregels. Het is daarom belangrijk dat het document actueel blijft. Dit geldt ook voor verwijzingen naar de achterliggende documenten. Er zijn twee type wijzigingen op dit document:

- Wijzigingen waarbij hoofdregels, zie het overzicht vanaf pagina 25, veranderen. In dat geval veranderen de regels en is brede afstemming noodzakelijk en hernieuwde instemming van de GOR Rijk. Voor Defensie loopt dit via Centrale medezeggenschapscommissie Defensie;
- Tekstuele wijzigingen waarbij een toelichting, een link of een voorbeeld wordt aangepast. Deze wordt vastgesteld door de CIO rijk en gaat ter informatie naar het CIO-beraad en de GOR Rijk.

2 Omgaan met informatie: goed en vindbaar

2.1 Wees open en transparant

Maak informatie openbaar volgens de afspraken binnen jouw organisatie.
De overheid heeft een publieke taak en daarbij zijn openheid en transparantie naar de maatschappij kernwaarden. Dit doen we als overheid vanuit onszelf en ook naar aanleiding van wetgeving zoals de Wob (Wet openbaarheid van bestuur) en de privacywetgeving.
Openbaar maken is dus belangrijk en moet zorgvuldig gebeuren zodat die informatie betrouwbaar is [3]. Het is dus niet de bedoeling dat je zelf informatie over je werk op het internet zet of vragen van journalisten beantwoordt. Iedere organisatie heeft hiervoor regels en procedures opgesteld. Hier zijn vaak juristen, beleidsmedewerkers, woordvoerders en communicatiespecialisten bij betrokken [4].

2.2 Opslaan van informatie: maak het vindbaar

Sla informatie op zodat jij en anderen kunnen terugvinden: op de juiste locatie en met een duidelijke naam.
Informatie slaan we op zodat jij en je collega's deze weer kunnen terugvinden en opnieuw kunnen gebruiken. Collega's kunnen niet bij informatie in jouw mailbox, je persoonlijke schijf of op je telefoon.
Maak intern afspraken over het opslaan van informatie, bv over naam van het bestand, het onderwerp, versienummer, auteur e.d. Gebruik de Rijkshuisstijl bij het opstellen van documenten: die hebben een plek voor dergelijke informatie. Documenten sla je op de gedeelde netwerkschijf op of in een 'document-managementsysteem' (DMS) zoals DigiDoc en DigiJust. [5]. Hiermee voorkom je tijdrovende speurtochten naar informatie.

Ga je binnenkort uit dienst? Draag je werkzaamheden en je informatie op tijd over. Als je steeds je informatie goed opslaat, is dat zo gebeurd!

Werk je met personeelsdossiers? Tip: werk die één voor één af, dan voorkom dat stukken van de één in het dossier van de ander komen.

Je persoonlijke schijf gebruik je voor persoonlijke informatie die niet voor anderen bedoeld is.

2.3 Houd je samenwerkruimtes en netwerkschijven netjes

Maak afspraken over wie en hoe je samenwerkingsruimtes en netwerkschijven netjes houdt.

Voorkom verweesde netwerkschijven en samenwerkruimtes, waar niemand zich verantwoordelijk voor voelt. Spreek (intern) met elkaar af waar je de informatie opslaat, op welk moment en vooral wie de informatie in het archief deponeert als de samenwerking eindigt. Met name wanneer in tijdelijke projecten en samenwerkingsverbanden dossiers ontstaan, wordt het deponeren naar het archief vaak vergeten.

> Werk je in groepsverband intensief aan een document met daardoor veel versies? Tip: neem de datum op in de naam van het document.

2.4 Bestempel informatie als vertrouwelijk

Rubriceer en merk je documenten: ontvangers zien dan dat een document (extra) vertrouwelijk is.
Zorg dat je weet wat het belang van de informatie die je hanteert. Sommige informatie is gevoelig en mag alleen in kleine kring gedeeld worden. Geef vertrouwelijke documenten een rubriceringsniveau en/of een merking mee. In de Rijkshuisstijl [5] kan je dit aangeven.
Benoem het eventueel ook nog aanvullend in de tekst van een mail. Hierdoor weten de ontvangers van informatie dat de inhoud (extra) vertrouwelijk is. Ze kunnen dan zelf ook passende maatregelen nemen.

> Op zoek naar de Rijkshuisstijlsjablonen? Tip: Deze zijn vaak onderdeel van de werkplek bv als menu in Word of als menu-item via het Windows-logo.

Vraag de afzender of je gerubriceerde of gemerkte informatie mag delen.
Als je informatie ontvangt die gerubriceerd of gemerkt is, gelden daar extra maatregelen voor. Doorgaans mag je niet zelf besluiten om die informatie met een ander te delen. Toch kan het voor het werk nodig zijn om deze informatie te delen met een collega. Vraag dan toestemming aan de afzender.

2.5 Archivering

Archivering gebeurt niet altijd vanzelf. Weet wat jij actief moet doen in het archiveringsproces.
De overheid is eigenaar van alle informatie die de overheid produceert of ontvangt bij het uitvoeren van haar taken. Informatie van de overheid valt onder de Archiefwet: documenten, informatie in applicaties, email, WhatsApp, sms en papieren post. Met de archiefwet en selectielijsten wordt vastgesteld hoe lang we informatie minimaal bewaren. Dit verschilt per proces, applicatie en het type document. Archiveren wordt in bepaalde gevallen automatisch geregeld. Dit geldt bijvoorbeeld voor informatie in applicaties. In andere gevallen moet je zelf een actieve rol hebben. Dit geldt vaak voor documenten op het netwerk. Zorg daarom dat je weet

hoe archivering werkt binnen jouw organisatie en wat je zelf actief moet doen. Op deze manier voldoen we aan de vereisten van volledigheid, toegankelijkheid en beschikbaarheid.

2.6 Respecteer intellectueel eigendom

Voor informatie en afbeeldingen die je van het internet of andere media haalt, gelden drie regels:

- *Pas bronvermelding toe;*
- *Gebruik zoveel mogelijk rechtenvrij materiaal;*
- *Schaf waar nodig betaald materiaal aan.*

Op het internet staat veel informatie, filmpjes, muziek en afbeeldingen die voor het werk nuttig zijn. Dit materiaal kan beschermd worden door het auteursrecht.
Soms is materiaal rechtenvrij en mag je dat gratis gebruiken met bronvermelding. In zoekmachines zoals Google, kan je je resultaten daarop filteren.
Via de Mediatheek Rijksoverheid is het ook mogelijk om beeldmateriaal op te vragen. Zij beheren overeenkomsten met beeldbanken [6].
Als je het toch beschermd materiaal nodig hebt, moet je het laten aanschaffen.

2.7 Help elkaar

Voorkom incidenten: help elkaar, stel vragen en maak de ander bewust de goede omgang met informatie.
In de drukte van alle dag is het makkelijk om iets te vergeten en een fout te maken. Help elkaar bijvoorbeeld door de computer voor de ander te vergrendelen en vertel hem dat als hij er weer is. Verwijder een mailtje dat niet voor jou bedoeld is en meldt dit bij de afzender. Als je denkt dat een collega niet weet hoe hij iets moet doen, laat het een keer zien.
Door elkaar op die manier te helpen, voorkomen we dat zaken misgaan. Als je dit lastig vindt, zijn er natuurlijk ook andere mogelijkheden om iets aan te kaarten, zoals dit melden bij je leidinggevende of een vertrouwenspersoon.

3 Veilig werken op kantoor

3.1 Gebruik de zakelijke ICT-voorzieningen

Gebruik zakelijke ICT-voorzieningen om je werk uit te voeren.
Om je werk te kunnen doen, krijg je toegang tot informatie, applicaties en ICT-voorzieningen. Als je iets mist, kan je aanvullende zaken aanvragen via je leidinggevende. In bijlage 1 staat een overzicht van veilige ICT-voorzieningen. Jouw eigen organisatie heeft mogelijk (ook) andere voorzieningen en regels rond het gebruik van eigen apparatuur: vraag daarnaar bij de servicedesk, je collega's of je leidinggevende. Commerciële voorzieningen toepassen, kan risico's met zich meebrengen (zie 8.4).

3.2 Wachtwoorden: maak het anderen niet te gemakkelijk

Leen je account en wachtwoord niet uit en gebruik wachtwoorden die niet makkelijk te raden zijn.
Je krijgt toegang tot ICT-voorzieningen op basis van een persoonlijke gebruikersnaam. Je account en wachtwoord zijn van jou en die leen je niet uit. Dit geldt ook voor je toegangspas, zoals de Rijkspas, om toegang te krijgen tot gebouwen. Jij bent verantwoordelijk voor wat er met jouw account wordt gedaan.

> Ben je nieuwsgierig hoe veilig onze voorzieningen zijn? Op eigen houtje hacken mag niet. Tip: ga op zoek naar teams die dit als taak hebben. Die zijn altijd op zoek naar enthousiaste collega's!

In bepaalde situaties, zoals bij thuiswerken, moet je ook een 2-factor authenticatie gebruiken [8]. Je gebruikt naast je wachtwoord een tweede middel, bijvoorbeeld een sms-code, om je te identificeren. Hierdoor kunnen anderen niet in jouw account te komen.

Veel wachtwoorden? Gebruik een wachtwoordenkluis.
Er zijn nog diverse voorzieningen en applicaties met een eigen wachtwoord. Al die wachtwoorden onthouden is moeilijk. Veel rijksorganisaties hebben daarom een 'wachtwoordenkluis' zoals KeePass. [9] Hierin kan je alle wachtwoorden veilig opslaan. Ook kunnen die wachtwoorden voor je bedenken zodat je steeds andere wachtwoorden gebruikt.

3.3 Weg van je werkplek: opgeruimd staat netjes!

Vergrendel je computer, laptop, tablet of telefoon.
Vergrendel als je apparatuur als je wegloopt van je (thuis) werkplek. Zo voorkom je dat een bezoeker, collega of huisgenoot toegang krijgt tot jouw email, documenten en systemen (voorbeeld P-Direkt). Je zakelijke telefoon en tablet vergrendel je door kort op de aan/uitknop te drukken. Hoe je je de computer en laptop vergrendelt, varieert:

- via het slotje in je scherm;
- via ctrl+alt+del en daarna de spatiebalk;
- via de toetscombinatie Windowslogo + L

Eenmaal terug op de werkplek, kun je na het intypen van het wachtwoord of de pincode weer verder.

Berg papieren op in een gesloten lade, locker of kast.
Als je een langere tijd van je (thuis)werkplek weggaat, berg dan papieren op in een gesloten lade, locker of kast. Daarmee voorkom je dat een bezoeker, collega of huisgenoot toegang krijgt tot die documenten. Op flexplekken zorg je zo dat je collega aan een opgeruimd bureau kan werken.

3.4 Privégebruik zakelijke ICT-voorzieningen

Hou privégebruik van zakelijke ICT-voorzieningen beperkt.
Beperkt privé gebruik van ICT-voorzieningen is toegestaan. De voorwaarde is dat het je eigen werk en dat van je collega's niet hindert. Sommige rijksorganisaties hebben hiervoor aanvullende regels.

> Stuur je een privé mailtje of sla je een privé document op, op het werk? Tip: zet deze in een aparte map 'Prive': dan is dit duidelijk voor je collega's en bij een formeel informatieverzoek.

Surf bewust: blijf weg bij riskante sites
Het bezoeken van sommige sites is op het werk niet toegestaan, ook niet beperkt. Dit betreft bijvoorbeeld pornografische, extremistische, terroristische en goksites. Integriteit is een grondhouding en is een belangrijk onderdeel van de manier waarop je je functie uitoefent [1]. Blijf dus weg bij dergelijke sites.
Sommige sites zijn om andere redenen ongewenst. Op het internet komen ook malafide websites voor, bijvoorbeeld waar je gratis films, muziek en software kan krijgen. Je loopt daar extra risico's op virussen en je kan auteursrechten schenden (zie 2.5).

3.5 Gevonden printjes: ruim ze voor elkaar op

Printjes bij de printer: geef ze aan de eigenaar of gooi ze in de papiercontainer.
Ook als je met je toegangspas print, kunnen printjes langere tijd bij de printer liggen. Dit kan komen door vergeetachtigheid, door een printerstoring of door verzending naar de verkeerde printer.
Geef gevonden printjes aan de eigenaar of gooi ze in de beveiligde papiercontainer. Die staat meestal in dezelfde ruimte als de printer.

> Loopt de printer vast? Tip: verwijder de opdracht via het lokale menu van de printer.

3.6 Incidenten: meld en los op

Als je een beveiligingsincident veroorzaakt, meld dit en help waar mogelijk bij het oplossen.
Fouten maken en je vergissen is menselijk. Je kunt bijvoorbeeld klikken op een verkeerde link in een mailbericht, een document achterlaten in het OV of je telefoon kan worden gestolen. Fouten maken kan, ervan leren moet.

Als er iets misgaat of dreigt mis te gaan, (1) meld je dit en (2) los je het op/laat je het oplossen.
Hoe dit werkt, verschilt per organisatie en is afhankelijk van het type incident. In bijlage 2 staan de gegevens voor contactpersonen en de servicedesk die gelden voor jouw organisatie.

Je zakelijke toestel gestolen of kwijt? Meld je toestel ook bij Apple of Google als gestolen of zoek [10]

Bij diefstal en verlies van mobiele apparatuur moet je dit melden bij de servicedesk. Soms moet je ook aangifte doen. Overleg dit met je leidinggevende.

4 Veilig samenwerken

4.1 Vertrouwelijke email: hou het intern

Mail vertrouwelijke informatie alleen naar Rijksmedewerkers.
Binnen de rijksoverheid kunnen we veilig mailen, omdat we de informatie over een beveiligd netwerk sturen. Buiten de rijkoverheid is dat niet het geval. Mail die over het internet verstuurd wordt, is niet beveiligd tenzij je extra maatregelen neemt. Stuur dus geen vertrouwelijke informatie via het internet.

Stuur geen mail naar je privé mailadres.
Ook deze mail is onderweg niet beveiligd. Bovendien is privé-apparatuur in het algemeen niet veilig genoeg. Stuur dus geen mail naar huis, maar maak gebruik van de thuiswerkvoorziening, de zakelijke tablet of de samenwerkruimte [11]. Stuur dus ook niet (standaard) vergaderverzoeken naar je privé-mailadres.

Kies het juiste mailadres.
Een tikfout is zo gemaakt en namen worden in de mail aangevuld. Let dus op naar wie je mail stuurt. Gaat het toch mis en betreft het vertrouwelijke informatie? Meld dit als incident, vraag die persoon het mailtje direct te verwijderen en dat te bevestigen.

> Bij het intypen van een mailadres wordt de naam automatisch aangevuld. Soms staat hier een oud of verkeerd mailadres.
> Tip: ga achter dat mailadres staan en klik op het kruisje: dan komt die niet meer terug.

Versleutel documenten.
Mail je toch vertrouwelijke documenten naar een externe zakelijke partner? Versleutel de documenten dan vooraf met een goed wachtwoord. Daar zijn voorzieningen voor zoals 7Zip, Eclips en LUNA [12]. Als je die niet kent of niet goed weet hoe je ze moet gebruiken, vraag een collega om hulp. Andere mogelijkheden om gegevens te delen staan in 4.2 en 4.3.

4.2 Aangetekende papieren post

Aangetekende papieren post is soms een goed alternatief om informatie te versturen.
De papieren post is wettelijk goed beschermd met het briefgeheim. Op schending hiervan staan sancties, waaronder boetes en zelfs gevangenisstraffen. Door informatie aangetekend te versturen, kan papieren post soms een nuttig en veilig alternatief zijn.
In het bezorgproces raakt een poststuk weleens zoek: meld dit als incident (zie 3.6).

4.3 Veilig delen van (grote) bestanden

Wissel (grote) bestanden met de samenwerkruimte of andere veilige voorzieningen.
Gebruik het DMS of de netwerkschijf om bestanden te delen met directe collega's. Dit werkt niet voor collega's elders binnen de overheid of met zakelijke partners. Hiervoor maak je gebruik van de samenwerkruimte. Deze is ook toegankelijk voor partners buiten de rijksoverheid.
Diverse Rijksorganisaties hebben eigen voorzieningen voor bestandsuitwisseling, zoals SecureTransfer [13] en de Bestandenpostbus [14]. Deze hebben niet de risico's van commerciële toepassingen zoals Dropbox en WeTransfer (zie 8.4).
Sommige Rijksorganisaties stellen beveiligde USB-sticks ter beschikking. Die zijn soms een praktisch alternatief. Draag de stick met het bestand dan wel persoonlijk over.

4.4 Berichtenapps en sms: voor informeel gebruik

Sms – alleen voor algemene mededelingen
Sms is steeds minder veilig: de inhoud kan onderschept worden. Voor een tijdelijke beveiligingscode, zoals voor thuiswerken, is het wel geschikt. Gebruik het zelf alleen voor algemene mededelingen die niet vertrouwelijk zijn. Melden dat je iets later bent of 'ik bel je zo terug' als je een telefoontje niet kunt opnemen, is bijvoorbeeld prima.

Berichtenapps - voor informeel gebruik
De inhoud van berichten in en gesprekken met WhatsApp, Signal en Threema zijn veilig en alleen toegankelijk voor de zender en ontvangers. Gebruik berichten-apps alleen voor informele zaken, zoals een interessant artikel delen, een hulpvraag stellen of sparren met collega's. Gebruik ze *niet* voor persoonsgegevens en voor formele zaken, zoals bestuurlijke aangelegenheden: app met beleid maar niet over beleid.
De berichten (en bijlages) staan namelijk alleen lokaal op jouw toestel. Hierdoor kunnen we niet centraal WOB- en AVG-verzoeken beantwoorden en is de informatie niet vindbaar voor anderen.
Voor de berichtenapps is Rijksbreed geen standaard vastgesteld. Sommige rijksorganisaties hebben dit wel gedaan: informeer binnen je organisatie of er specifieke regels zijn [15].

Toch formeel ingezet? Sla het op.
Tijdens een crisis e.d. kunnen berichten-apps toch voor formele zaken zijn ingezet. Sla de berichten op die van belang zijn voor besluitvorming. Gebruik hiervoor de instructies van jouw organisatie [16]. Dit is van belang voor onderzoek en evaluatie achteraf en ook voor Wob-verzoeken.

4.5 Video-vergaderen met de officiële voorzieningen

Gebruik Webex of de videovoorzieningen die jouw organisatie gebruikt.
Overleggen en vergaderen zijn steeds vaker digitaal. Niet iedere voorziening is veilig of gaat zorgvuldig om met jouw persoonsgegevens. Gebruik daarom de voorzieningen die jouw organisatie aanbiedt. Rijksbreed is dit Webex [17] en sommige organisaties hebben ook eigen voorzieningen.

Uitnodiging van een zakelijke partner
Als een betrouwbare externe partner je uitnodigt via een andere voorziening zou dit voldoende veilig moeten zijn. Voor gecontracteerde leveranciers is dit onderdeel van het Programma van Eisen.
Als je twijfelt, kan je het voorstel doen om de vergadering via de voorziening van jouw organisatie te laten lopen. Ook kan je afspreken om heel vertrouwelijke zaken niet te bespreken.

5 Veilig thuiswerken

5.1 Belastbaarheid: let op jezelf en op elkaar

Hanteer vaste werktijden en een aparte werkplek.
Thuiswerken kan leiden tot overbelasting. Werk en privéleven raken met elkaar vervlochten. Alles speelt zich dicht bij elkaar af en soms zelfs in dezelfde ruimte. Als je je niet prettig voelt bij de situatie, bespreek dit dan met je collega's, je leidinggevende, preventie-medewerker of eventueel een vertrouwenspersoon. Het helpt ook om thuis vaste werktijden te hanteren en daarna je apparatuur uit te zetten of uit het zicht te leggen. Het hebben van een aparte werkplek zorgt er ook voor dat je niet de hele dag op één plek zit.

Neem (samen) pauze.
Kom regelmatig los van je scherm. Neem pauze en maak bijvoorbeeld een wandeling. Dit kan eventueel ook met een collega, want contact houden is belangrijk. Ook digitaal kan je samen koffiedrinken. Dan kan je het over andere zaken dan je werk hebben, bijvoorbeeld over hoe het gaat.

5.2 Zorg voor een veilige thuiswerkplek

Bijna alle kantoorwerkzaamheden kan je ook thuis doen. Je kan met je organisatie in gesprek gaan om een Arbo verantwoorde thuiswerkplek in te richten. Thuiswerken brengt ook een verantwoordelijkheid met zich mee. Zorg er bijvoorbeeld voor dat je de werkplek thuis vergrendeld als je wegloopt en belangrijke documenten opbergt. Voorkom bij overleggen dat iedereen kan meeluisteren.

5.3 Gebruik privé-apparatuur: geen zakelijke informatie

Houd zakelijke informatie op zakelijke apparatuur.
Van privé-apparatuur is de veiligheid niet gegarandeerd. Ook is bekend dat deze vaak virussen hebben en andere beveiligingsissues. Zet dus geen documenten via de mail of een USB-stick op je privé-apparaat. Maak gebruik van de zakelijke apparatuur (smartphone, laptops, tablet etc). Wel is het bij de meeste organisaties toegestaan om met je eigen computer gebruik te maken van de thuiswerkomgeving (zoals Flex2Rijk en Connect). In het ontwerp hiervan is rekening gehouden met het gebruik van privé-apparatuur. In sommige organisaties wordt privé-apparatuur breder ingezet. Hiervoor zijn kaders opgesteld. Check wat voor jou van toepassing is.

> Zakelijk en privé: hou je software en virusscanner actueel en voer updates uit.

5.4 Defecte apparatuur: verwijder gegevens

Verwijder zakelijke gegevens voordat je privé-apparatuur laat repareren.

Als je apparatuur laat repareren, verwijder eerst van zakelijke gegevens op het apparaat. Voor zakelijke apparatuur is dit eenvoudig. Je levert het in via de servicedesk en in hun processen wordt dit geregeld. Op privé apparatuur staan als het goed is geen zakelijke documenten maar misschien wel contactgegevens. Verwijder zakelijke informatie voorafgaand aan de reparatie. Doe dit ook als je privé-apparatuur verkoopt of weggooit.

> Wil je gegevens op je mobiele telefoon of tablet verwijderen? Tip: gebruik de optie 'terugzetten naar fabrieksinstellingen'.

6 Veilig werken onderweg

6.1 Veilig mobiel werken met de zakelijke voorzieningen

Je kan je voorzieningen en apparatuur veilig onderweg gebruiken.
Je kan onderweg veilig werken via de thuiswerkomgeving op je laptop, tablet of telefoon. Hiermee kun je je mail bekijken en versturen en kan je bij andere zakelijke informatie.

6.2 Werk digitaal

Print zo min mogelijk en werk zoveel mogelijk digitaal.
Wil je mobiel werken? Doe dit dan zoveel mogelijk digitaal. Als je met geprinte documenten of notitieboekjes werkt, is de kans groter dat je deze verliest en de informatie direct zichtbaar is. Je kunt onderweg inloggen op de digitale werkomgeving op je laptop, tablet of telefoon. De thuiswerkomgeving brengt je naar de veilige omgeving van je organisatie.

6.3 Mail en agenda onderweg: gebruik de tablet

Gebruik de zakelijke tablet of smartphone om thuis of onderweg te mailen.
Met een zakelijke tablet of smartphone kan je mail afhandelen, afspraken bekijken en ook documenten lezen. Hiervoor worden apps gebruikt zoals BlackBerry en Mobile Iron. Dit werkt snel en eenvoudig en je hebt geen laptop nodig. Zeker onderweg is dat heel praktisch. Veel organisaties beschikken over dergelijke mogelijkheden: vraag hiernaar bij jouw organisatie (zie bijlage 1).

6.4 Ongewenst meeluisteren: hou afstand of bel later

Bel je in het openbaar? Houd dan afstand tot anderen of stel het gesprek uit.
In het openbaar luisteren anderen mee, ook bijvoorbeeld in de lift. Let dus op wat je er bespreekt. Zoek een rustig plekje op en houd afstand tot anderen. Ook kan je aan je gesprekspartner voorstellen om het gesprek later te voeren: niet alles heeft haast.

6.5 Ongewenst meekijken: je buren gluren

Zorg dat anderen niet kunnen meekijken op je scherm.
Ga ervan uit dat je buurman in trein, café of andere openbare plekken meekijkt: mensen zijn nieuwsgierig. Als iemand naast of achter je zit, zorg dan dat je geen vertrouwelijke informatie op je scherm hebt staan.

Werk je veel in het OV of in het openbaar? Tip: vraag een privacy-scherm aan, dan kunnen je buren niet meer meegluren.

6.6 Veilig internetverbindingen: vertrouwde wifi of 4G

Werk via vertrouwde wifi, je persoonlijke hotspot of 3G/4G/5G.
In rijkskantoren is gov-roam [18] beschikbaar en sommige rijksorganisaties hebben een eigen veilig wifi-netwerk. Werk daarbuiten via VPN of de 4G-simkaart in je laptop of telefoon. Je kunt ook je telefoon instellen als een wifi-hotspot om daarmee op je laptop te werken. [19].

Verwijder openbare wifi-netwerken na gebruik
Soms moet je toch via een openbaar wifi-netwerk werken (toegang zonder wachtwoord). Het is belangrijk dat je na gebruik het wifi-netwerk weer uit je opgeslagen netwerken verwijderd. [20] Cybercriminelen kunnen namelijk misbruik maken van opgeslagen openbare wifi-netwerken. [21]

6.7 Veilig op vakantie: laat je werk thuis!

Zakelijke mobiele apparaten mee op vakantie? Weet dan waar je op moet letten.

Laat je werkapparatuur thuis.
Als je op vakantie bent, ben je vrij. Het is vaak niet nodig dat je bereikbaar moet zijn. Laat daarom je werkapparatuur thuis. Voor dienstreizen naar het buitenland gelden aparte regels [1].

Buiten Europa: pas op met datagebruik.
Als je in overleg met je leidinggevende toch je zakelijke apparatuur meeneemt op vakantie, pas dan op met datagebruik. Binnen de EU gelden dezelfde voorwaarden als in Nederland. Maar buiten de EU kunnen hoge tarieven gelden. Hou het gebruik dan strikt zakelijk.

7 Omgaan met persoonsgegevens en privacy

7.1 Vaak goed geregeld en bespreek aandachtspunten

Ga ervan uit dat je persoonsgegevens rechtmatig gebruikt. Twijfel je hierover en zie je een risico? Spreek het uit!
We werken dagelijks met persoonsgegevens, d.w.z. gegevens die direct of indirect te herleiden zijn tot een persoon. Dit doen we met een goede reden, bijvoorbeeld om onze wettelijke taken te kunnen uit voeren of voor onze interne processen.
De overheid heeft veel aandacht voor privacy, maar het kan toch voorkomen dat er meer gegevens dan nodig verwerkt worden of dat deze langer dan nodig bewaard blijven. Maak je je hier zorgen over? Bespreek dit dan in je team of vraag het aan een privacy-specialist in je organisatie.

> Beoordeel je brieven en CV's van sollicitanten? Tip: Verwijder ze binnen vier weken na afloop van de procedure conform de richtlijn van de AP.

Als je voor je werk persoonsgegevens gebruikt, mag je ze niet zomaar gebruiken voor een ander doel.
Soms lijkt het een goed idee om persoonsgegevens die je al hebt ook voor een iets ander doel inzetten. Dat mag als dat nieuwe doel voldoende past bij het oorspronkelijke doel waarvoor de gegevens zijn verzameld. Om dit te beoordelen, bespreek je dit in je team of met een privacy-specialist.

7.2 Deel en bespreek gedoseerd persoonsgegevens

Deel en bespreek niet meer informatie over personen dan nodig voor je werk en voor het werk van de collega.
Ook zonder privacywetgeving is het vanzelfsprekend dat je zorgvuldig met persoonsgegevens omgaat. Je wilt zelf ook graag dat een ander zorgvuldig omgaat met jouw gegevens. Als het voor je werk en van je collega nodig is om persoonsgegevens te delen en daarover te praten, is dat prima. Echter, deel en bespreek niet meer informatie over personen dan nodig voor dat doel. Met trots en plezier praten over je werk is uitstekend, maar pas op welke (persoons)gegevens je daarbij deelt.

> Rapportages bevatten meestal geen persoonsgegevens. Tip: stuur de brongegevens niet mee: die bevatten vaker persoonsgegevens.

7.3 Voorkom datalekken: werk veilig

Pas de regels voor informatiebeveiliging toe, dan bescherm je ook persoonsgegevens en voorkom je datalekken.

Een belangrijk privacy-onderwerp is het goed beschermen van persoonsgegevens. Je moet ze kunnen gebruiken voor je werk, maar anderen moeten er niet zomaar bij kunnen. Door veilig om te gaan met gegevens bescherm je de privacy van burgers en medewerkers. De clean desk policy, de papiercontainer, nadenken wat je bespreekt in de openbare ruimte etc. dragen ook bij aan privacybescherming.

> Wat is een datalek? Een datalek ontstaat als de verkeerdere personen toegang, krijgen tot persoonsgegevens en wanneer persoonsgegevens vernietigd worden zonder dat dit de bedoeling is.

7.4 Datalekken melden: klein en groot

Meld een datalek, ook als ze klein zijn, volgens de procedures die gelden binnen jouw organisatie.
Ook als je heel zorgvuldig werkt, kan je toch een datalek veroorzaken. Dit kan ook buiten je schuld zijn als bijvoorbeeld post zoekraakt met daarin persoonsgegevens.
Datalekken zijn informatiebeveiligingsincidenten en moet je melden volgens de procedures in jouw organisatie (zie ook 3.6). Meld wanneer persoonsgegevens bij de verkeerde persoon terecht komt. Doe dit ook als het risico voor de betrokkenen beperkt is. Door consequent te melden, zien we ook waar ruimte is voor verbetering in proces, systeem en instructie. In de verdere afhandeling wordt ervoor gezorgd dat impactvolle datalekken gemeld worden bij de Autoriteit Persoonsgegevens (AP). Het is belangrijk dat je een potentieel datalek direct meldt zodat we deze tijdig kunnen melden bij de AP. Ook is de administratie op orde bij vragen van de AP de administratie op orde.

7.5 Jouw privacy op het werk

Ga naar de servicedesk als je vragen hebt over jouw privacy op het werk.
Op het werk heb je ook recht op privacy, bijvoorbeeld met betrekking tot je mail en je home directory/persoonlijke schijf. Sommige handelingen met ICT worden digitaal gelogd en gemonitord. Het voornaamste doel hiervan is ICT-beheer waaronder het oplossen van verstoringen en het detecteren van dreigingen. Verder kunnen loggegevens worden ingezien met heel goede redenen en via vastgestelde procedures, zoals voor AVG-inzageverzoeken of integriteitsonderzoek. Heb je vragen over je eigen privacy? Stel ze bij de Servicedesk. Als zij jouw vraag niet kunnen beantwoorden, verwijzen ze je door naar de juiste collega.

8 Pas op voor cybercriminelen, let op je gegevens

8.1 Virussen en betrouwbare software

Installeer op je telefoon en tablet alleen maar apps vanuit de Appstore en Playstore.
In de erkende appstores (App Store, Google Play, BlackBerry World, Windows Store, etc.) staan betrouwbare apps. Apps die van andere plekken komen, kunnen virussen e.d. bevatten. Virussen kunnen documenten op slot zetten waardoor organisaties langdurig niet kunnen werken en het herstel daarvan is kostbaar.

Installeer op de laptop alleen software rechtstreeks van de leverancier.
Sommige medewerkers kunnen zelf software op hun computer of laptop installeren. Populaire software kan je overal downloaden en soms krijg je daarbij gevaarlijke extra's. Installeer alleen software die rechtstreeks van de leverancier komt of via een link op de website van de leverancier.

Ondanks dat we goed beschermd zijn en ook als je goed oplet, kan het misgaan. Meld dat (zie 3.6).

8.2 Phishing: trap er niet in!

Laat niet zomaar je gegevens achter. Bij twijfel: neem rechtstreeks contact op met de afzender.
Cybercrminelen willen graag inloggegevens en financiële gegevens (bv. creditcard) van je organisatie. Dit doen ze via phishing: via een link in een mailtje kom je op een website terecht die bijna niet van echt te onderscheiden is. Daar moet je dan inloggen en gegevens achterlaten. Vervolgens ben je je gegevens kwijt en kunnen die misbruikt worden voor identiteitsfraude. Cybercriminelen vallen met phishingmails ook organisaties aan. Er zijn phisingmails die virussen verspreiden en bijvoorbeeld bestanden op slot zetten met losgeld als doel.

> Wil je beter phishingmails leren herkennen. Op het internet is daar veel informatie over. Enkele voorbeelden staan achterin [22]

Klik dus nooit zomaar op linkjes in mailtjes. Als je toch denkt dat het een 'echt' bericht is, klik dan niet op de link, maar ga zelf naar de website en log daar in. Of neem zelf rechtstreeks contact op per telefoon of mail. Phishing kan grote gevolgen hebben voor de organisatie waarin je werkt. Dagelijks worden organisaties door dergelijke software platgelegd en het herstel kost veel tijd en geld.

8.3 Social engineering en Digitale oplichting

Vraagt een collega plotseling om geld? Bel hem!
Cybercriminelen misbruiken je gegevens hebben om geld mee te verdienen. Ze doen zich bijvoorbeeld als jou voor ('social engineering') en vragen je vrienden, familie of collega's om geld. Phishing leidt zo tot digitale oplichting. Als je zo'n bedelbericht (of mail) krijgt, bel die persoon dan op om te controleren of er echt iets aan de hand is of dat hij slachtoffer is van cybercriminelen.

> Cybercriminelen willen je WhatsApp-account overnemen. Tip: stel 'verificatie in twee stappen' in via instellingen/account.

8.4 Gratis software en apps kunnen kostbaar zijn

Maak gebruik van de standaard voorzieningen.
Het internet is zoveel mogelijk vrij toegankelijk. Je kan dus gebruik maken van allerlei handige gratis diensten. Handig is niet altijd veilig. Daarnaast kan je zo het eigenaarschap kwijtraken van je gegevens. Maak dus zoveel mogelijk gebruik van de veilige voorzieningen (zie bijlage 1).

Geef je gegevens niet zomaar weg voor een gratis app.
Een gratis dienst is nooit echt gratis: de aanbieders van die diensten moeten ook geld verdienen. Soms is dat simpelweg door reclame-inkomsten. Soms handelen ze in je gegevens en heb je daar bij het installeren van de app toestemming voor gegeven. Geef je gegevens niet zomaar weg voor een handige app, maar denk na of het je dat wel waard is.

> In-app aankopen kunnen veel geld kosten. Tip: zet in de instellingen aan dat je altijd toestemming moet geven voor aankopen.

Overzicht gedragsregels

Wees open en transparant: Maak informatie openbaar volgens de afspraken binnen jouw organisatie

Opslaan van informatie: maak het vindbaar: Sla informatie op zodat jijzelf en anderen deze kunnen terugvinden: op de juiste locatie en met een duidelijke naam.

Houdt je samenwerkruimtes en netwerkschijven netjes: Maak afspraken over wie en hoe je samenwerkingsruimtes en netwerkschijven netjes houdt.

Bestempel informatie als vertrouwelijk
- Rubriceer en merk je documenten: ontvangers zien dan dat een document (extra) vertrouwelijk is.
- Vraag de afzender of je gerubriceerde of gemerkte informatie mag delen.

Archivering: Archivering gebeurt niet altijd vanzelf. Weet wat jij actief moet doen in het archiveringsproces.

Respecteer intellectueel eigendom
Voor informatie en afbeeldingen die je van het internet of andere media haalt, gelden drie regels:
- Pas bronvermelding toe;
- Gebruik zoveel mogelijk rechtenvrij materiaal;
- Schaf waar nodig betaald materiaal aan.

Help elkaar: voorkom incidenten door elkaar te helpen. Stel vragen en maak de ander van regels en gedrag bewust.

Gebruik je zakelijke ICT-voorzieningen voor je werk: ga na welke voorzieningen jouw organisatie heeft**.**

Wachtwoorden: maak het anderen niet te gemakkelijk.
- Leen je account en wachtwoord niet uit en gebruik wachtwoorden die niet eenvoudig te raden zijn.
- Gebruik een wachtwoordmanager om je wachtwoorden veilig in op te slaan.

Weg van je werkplek: zet de boel op slot:
- Vergrendel je computer, laptop, tablet of telefoon.
- Berg papieren documenten op in een gesloten lade, locker of kast.

Privégebruik zakelijke ICT-voorzieningen
- Hou het privégebruik van de zakelijke ICT-voorzieningen beperkt.
- Surf bewust en blijf weg bij riskante sites.

Gevonden printjes: ruim ze voor elkaar op: geef ze aan de eigenaar of gooi ze in de beveiligde papiercontainer.

Incidenten: meld en los op: als je een beveiligingsincident veroorzaakt of ziet, meld dit en help waar mogelijk bij het oplossen.

Vertrouwelijke email: hou het intern
- Mail vertrouwelijke informatie alleen naar Rijksambtenaren.
- Stuur geen mail naar je privé mailadres.
- Versleutel documenten als je buiten de rijksoverheid mailt.

Aangetekende papieren post is soms een goed alternatief voor het digitaal versturen van informatie.

Veilig delen van (grote) bestanden: gebruik samenwerkruimte of andere veilige voorzieningen.

Berichtenapps en sms: voor informeel gebruik:
- Gebruik sms alleen voor algemene mededelingen.
- Gebruik de app alleen voor informele mededelingen en overleg.
- Toch formeel ingezet? Sla het op!

Video-vergaderen met de officiële voorzieningen: Gebruik Webex en de videovoorzieningen die jouw organisatie gebruikt.

Belastbaarheid: let bij thuiswerken op jezelf en op elkaar
- Hanteer vaste werktijden en een aparte werkplek.
- Neem (samen) pauze.

Zorg voor een veilige thuiswerkplek

Gebruik privé-apparatuur: sla geen zakelijke informatie op, maar hou zakelijke informatie op zakelijke apparatuur.

Defecte apparatuur: Verwijder eventuele zakelijke gegevens voordat je privéapparatuur laat repareren.

Veilig mobiel werken onderweg: gebruik gewoon de zakelijke voorzieningen en apparatuur.

Werk onderweg digitaal: werk zo min mogelijk van papier.

Alleen mail en agenda onderweg: gebruik de zakelijke tablet of smartphone.

Bellen in het openbaar: hou afstand tot anderen of stel het gesprek uit.

Werken in het openbaar: zorg dat anderen niet kunnen meekijken op je scherm.

Gebruik veilig internetverbindingen:
- Werk via vertrouwde wifi, je persoonlijke hotspot of 4G.
- Verwijder openbare wifi-netwerken na gebruik.

Veilig op vakantie: laat je werk thuis!
- Laat je werkapparatuur thuis.
- Toch mee? Pas op met datagebruik buiten de EU.

Privacy is vaak goed geregeld: twijfel je hierover en zie je een risico? Bespreek het met je team of leidinggevende. Gebruik persoonsgegevens voor het oorspronkelijke doel en niet zomaar voor iets anders.

Deel en bespreek gedoseerd persoonsgegevens: doe dit zover dat logisch is voor jouw werk en voor het werk van de collega.

Voorkom datalekken: hou je aan de regels voor informatiebeveiliging en dan bescherm je ook persoonsgegevens.

Meld datalekken: gebruik de procedures van jouw organisatie om datalekken te melden. Doe dit ook als het een klein datalek is.

Jouw privacy op het werk: ga naar de servicedesk als je vragen hebt over jouw privacy op het werk: zij helpen je verder.

Voorkom virussen en andere malware:
- Installeer op je telefoon en tablet alleen maar apps vanuit de Appstore en Playstore.
- Installeer op de laptop alleen software rechtstreeks van de leverancier.

Trap niet in phishing: laat niet zomaar je gegevens achter. Als je twijfelt of het echt is, neem dan rechtstreeks contact op met de afzender.

Pas op met digitale oplichters: Vraagt een vriend plotseling digitaal om geld of vertrouwelijke informatie? Bel hem eerst om te checken of het klopt.

Gratis software en apps kunnen kostbaar zijn
- Maak gebruik van de standaard voorzieningen.
- Geef je gegevens niet zomaar weg voor een gratis app.

Bijlage 1 – Veilige voorzieningen

Rijksbrede voorzieningen

Voorziening	Rubricering	Bijzonderheden
Samenwerkingsruimte i-SWF intern	DepV/BBN2	
Samenwerkingsruimte e-SWF extern	DepV/BBN2	
Mail	DepV/BBN2, mits binnen rijksoverheid, zie 4.1	
Mail + Eclips* of LUNA*	DepV of STG-C	
Harde schijf encryptie/ Safeguard*	DepV	
Mobiele telefoon/tablet: Blackberry Work-apps	DepV	
USB-sticks: Ironkey*, datAshur* en Kobil*	DepV	

* op basis van evaluatie door de AIVD, https://www.aivd.nl/onderwerpen/informatiebeveiliging/beveiligingsproducten/geevalueerde-producten, en er moet dus voldaan worden aan de betreffende inzetadviezen.

Organisatie specifieke voorzieningen

Voorziening	Rubricering	Bijzonderheden
[Naam van de voorziening]	*[tot welk niveau biedt het bescherming]*	

Bijlage 2 – Contactgegevens

Servicedesk <eigen organisatie>
- Telefoonnummer
- Mailadres
- Webpagina

Vragen over informatiebeveiliging
- Beveiligingsautoriteit (BVA): <naam, telefoonnummer, mailadres>
- Beveiligingscoördinator (BVC): <naam, telefoonnummer, mailadres>
- Chief Information Security Officer (CISO): <naam, telefoonnummer, mailadres>
- Informatiebeveiligingsfunctionaris/Security Officer: <naam, telefoonnummer, mailadres>
- Security Operations Center (SOC): <naam, telefoonnummer, mailadres>

Vragen over privacy
- Chief Privacy Officer (CPO): <naam, telefoonnummer, mailadres>
- Functionaris Gegevensbescherming (FG): <naam, telefoonnummer, mailadres>
- Privacy Jurist: <naam, telefoonnummer, mailadres>
- Privacy Officer: <naam, telefoonnummer, mailadres>

Vragen over archivering en duurzame opslag
- Archivaris: <naam, telefoonnummer, mailadres>

Vragen over openbaarmaking gegevens en WOB
- Afdeling communicatie: <mailadres, telefoonnummer>
- Coördinator WOB: <naam, mailadres, telefoonnummer>
- WOB-jurist: <naam, mailadres, telefoonnummer>

Bijlage 3 – Verwijzingen naar achterliggende documenten

[1] Gedragscode Integriteit Rijk,
https://www.rijksoverheid.nl/documenten/richtlijnen/2017/12/01/gedragscode-integriteit-rijk-gir

[2] Handreiking Online Communicatie Rijksambtenaren
https://www.rijksoverheid.nl/documenten/rapporten/2010/06/30/uitgangspunten-online-communicatie-rijksambtenaren

[3] Kenniskaart werken met informatie
Kenniskaart werken met informatie: waarom is belangrijk en wat willen we bereiken: https://www.informatiehuishouding.nl/projecten/medewerker-aan-informatie/Producten+%26+publicaties/instrumenten/2019/09/17/kenniskaart-werken-met-overheidsinformatie

[4] Instructie voor openbaar maken:
Handreiking: Actief openbaar maken doe je zo! | Instrument | Rijksprogramma voor Duurzaam Digitale Informatiehuishouding

[5] Rijkshuisstijl
http://portal.rp.rijksweb.nl/irj/portal/?NavigationTarget=HLPFS://cisrijksportaal/cisfacilitair/ciscommunicatie/cismiddelen/cishuisstijl/cisrijkshuisstijlgids

[6] Beeldbankfotografie
http://portal.rp.rijksweb.nl/irj/portal/?NavigationTarget=HLPFS://cisrijksportaal/cisfacilitair/ciscommunicatie/cisrijksbrede_inkoop_van_communicatiediensten_1/cisfotografie/cisfotostock

[7] instructie wachtwoorden, op te vragen bij auteurs.

[8] Instructie flex2rijk: https://www.ssc-ict.nl/documenten/handleidingen/2020/06/08/handleiding---flexibel-werken-met-een-software-token

[9] instructie Keepass: https://www.ssc-ict.nl/documenten/handleidingen/2019/07/09/handleiding-keepass

[10] Instructie voor diefstal/verloren telefoon/tablet
- Apple: https://support.apple.com/nl-nl/HT201472
- Android:
  https://support.google.com/accounts/answer/6160491?hl=nl

[11] Instructie voor samenwerkruimten:
http://portal.rp.rijksweb.nl/irj/portal/?NavigationTarget=HLPFS://cisrijksportaal/cisfacilitair/cisicteninformatievoorziening_1/cissamenwerkfunctionaliteit_4/cissamenwerkruimten&NavigationContext=HLPFS://cisrijksportaal/cisfacilitair/cisicteninformatievoorziening_1/cissamenwerkfunctionaliteit_4

[12] instructie voor Luna, Eclipse, 7Zip, op te vragen bij auteurs

[13] Instructie Securetransfer: DAP (rijkscloud.nl)

[14] instructie bestandenpostbus: Bestandenpostbus (rijksweb.nl)

[15] Handreiking mbt berichtenapps:
https://www.informatiehuishouding.nl/Producten+%26+publicaties/richtlijnen/2018/02/07/beleidslijn-berichtenapps
https://www.informatiehuishouding.nl/app-met-beleid

[16] Handreiking opslaan chatberichten:
App met beleid; niet over beleid | Rijksprogramma voor Duurzaam Digitale Informatiehuishouding
[17] instructies voor Webex: Rijksportaal (rijksweb.nl),
Best Practices For Working Remotely (webex.com)
Helpcentrum van Webex

[18] Aanvragen WIFI:
http://portal.rp.rijksweb.nl/irj/portal/?NavigationTarget=HLPFS://cisrijksportaal/cisfacilitair/cisicteninformatievoorziening_1/ciswifi__rijksbreed_/ciswifi__rijksbreed_2&NavigationContext=HLPFS://cisrijksportaal/cisfacilitair/cisicteninformatievoorziening_1/ciswifi__rijksbreed__ en
http://portal.rp.rijksweb.nl/irj/portal/?NavigationTarget=HLPFS://cisrijksportaal/cisfacilitair/cisicteninformatievoorziening_1/ciswifi__rijksbreed_/cisbzk_turfmarkt

[19] Gebruik hotspot
Instructie voor instellen telefoon als hotspot apple en android en voor verwijderen opgeslagen wifi-netwerken.

- Android: https://www.youtube.com/watch?v=VBriRsmPAds
- iPhone: https://www.youtube.com/watch?v=cSdl6rCIoTk

[20] Instructie verwijderen wifi-netwerken

- Apple: https://www.youtube.com/watch?reload=9&v=qeFYCvcXakA
- Google/Android: https://www.youtube.com/watch?v=50eblYQIF2w

[21] Handreiking mbt Wifi thuis van NSCS:
https://www.ncsc.nl/documenten/publicaties/2019/mei/01/wifi-onderweg-gebruik-een-vpn

[22] Herkennen phishing
https://www.youtube.com/watch?v=Ls0LBmmhOvY en
www.veiliginternetten.nl

[23] Burgerlijk wetboek, Artikel 7:677 en 678
Wetboek-online.nl | Burgerlijk Wetboek Boek 7 | Artikel 677 (wetboek-online.nl) en Wetboek-online.nl | Burgerlijk Wetboek Boek 7 | Artikel 678 (wetboek-online.nl)

[24] Integriteitsschendingen en Baseline Intern persoonsgericht onderzoek na een integriteits- of beveiligingsincident (BIPO): Rijksportaal (rijksweb.nl)

Ministerie van Financiën

TER BESLISSING VOOR DE BR
Aan
De leden van de Bestuursraad

Directie Juridische Zaken
Directie Bedrijfsvoering
Directie Communicatie
Inlichtingen

Persoonsgegevens

Datum
26 maart 2020

Notitienummer
2020-0000061554

Auteur

Persoonsgegevens

Van

Kopie aan

notitie

Archivering van chatberichten

Aanleiding

In de BR van 18 november 2020 is gesproken over de instructie van het SGo (zie bijlage 1) omtrent het archiveren van chatberichten. De BR heeft naar aanleiding van deze bespreking gevraagd om een verdere uitwerking van deze instructie. In deze notitie komt aan de orde hoe de medewerkers en bewindspersonen van het Ministerie van Financiën dienen om te gaan met het archiveren van chatberichten, enkele punten over de bedrijfsvoering en de communicatie over dit onderwerp.

Beslispunt

De leden van de BR worden gevraagd om in te stemmen met de volgende werkwijze indien chatberichten met betrekking tot bestuurlijke besluitvorming moeten worden opgeslagen:

- Iedere ontvanger en/of verzender moet zelf de berichten exporteren naar zijn of haar mail en vervolgens sturen naar de dossierhouder die het opslaat.
- Wanneer de dossierhouder deelnemer is van het chatgesprek, slaat de dossierhouder de relevante berichten op. Het vastgelegde bestuurlijke besluit moet worden afgestemd met de verantwoordelijk directeur.
- Als de dossierhouder niet aan het gesprek deelneemt, maak dan afspraken over wie de berichten doorzet naar de dossierhouder. De dossierhouder zorgt ervoor dat het chatbericht wordt opgeslagen.
- De dossierhouder is: De eigenaar van het dossier waar het chatbericht betrekking op heeft. Dit kan ook een DG of directeur zijn.

Toelichting

Het gebruik van berichtenapps zoals Whatsapp en Signal voor bestuurlijke besluitvorming wordt afgeraden.

Om wat voor soort berichten gaat het?

Berichten die betrekking hebben op bestuurlijke besluitvorming en de toekomstige reconstructie ervan. Dat wil zeggen:

a) Het bericht met het besluit zelf;

En ter verheldering van a):

b) De berichten die duidelijk maken wat het onderwerp is waarop een besluit wordt genomen;

c) De berichten die duidelijk maken wat de onderbouwing is van het besluit;
d) De relevante informatie die eraan voorafging en als aanleiding kunnen gelden voor het besluit.[1]

Moeten chatberichten m.b.t. bestuurlijke besluitvorming altijd worden opgeslagen?

Als de informatie uit de berichten in een ander document, zoals een notitie in Digidoc of in een e-mail, wordt vastgelegd en opgeslagen, hoeven deze chatberichten niet te worden bewaard.

- Vermijd bestuurlijke besluitvorming via chatberichtenapps. Als het toch gebeurt, maak dan afspraken over wie de inhoud van de berichten m.b.t. bestuurlijke besluitvorming overhevelt naar een ander document dat wordt vastgelegd en opgeslagen, zoals een e-mail of een notitie. Dan hoeven de chatberichten niet meer te worden gearchiveerd.
- Het vastleggen van de inhoud van besluitvormingsberichten wordt gedaan door de dossierhouder als deze deelnemer is van het chatgesprek. Het vastgelegde bestuurlijke besluit moet worden afgestemd met de verantwoordelijk directeur.
- Als de dossierhouder niet aan het gesprek deelneemt, maak dan afspraken over wie de berichten doorzet naar de dossierhouder. De dossierhouder zorgt ervoor dat de bestuurlijke besluitvorming wordt vastgelegd en opgeslagen.
- Chatberichten kunnen worden gewist op het moment dat een chatbericht op de juiste manier is gearchiveerd of op het moment dat de inhoud van het chatbericht ergens anders is vastgelegd, zoals in een document in Digidoc of een e-mail.

Wanneer moeten chatberichten worden opgeslagen?

- Als de inhoud van een chatbericht m.b.t bestuurlijke besluitvorming niet is vastgelegd in een document of e-mail, moeten deze berichten apart worden gearchiveerd. Zie het stappenplan hieronder voor de instructies.
- Een situatie die voorkomen dient te worden is dat er een Wob-verzoek binnenkomt, en dat er op dat moment nog niet gearchiveerde of niet overgehevelde berichten op telefoons staan die zien op dit Wob-verzoek.
- Overhevelen mag dan niet meer, omdat er dan een standstill beginsel in werking treedt (*zie ook bullet 4 bij de volgende vraag*). In die gevallen dient ieder de relevante chatberichten aan te leveren aan de relevante dossierhouder.

Welke richtlijnen gelden voor bewindspersonen en de BR-leden?

De Wob geldt voor iedereen en chatberichten vallen onder de Wob. Praktisch vraagt dit om de volgende aanpak voor de politieke en ambtelijke top:

- In chatverkeer tussen bewindspersonen en DG's, directeuren en anderen ligt het voortouw van het vastleggen van chatberichten m.b.t. bestuurlijke besluitvorming bij DG's, directeuren en medewerkers.
- In chatverkeer tussen bewindspersonen of BR-leden onderling wordt hen verzocht om zelf dit soort berichten te herkennen en afspraken te maken over hoe deze worden opgeslagen en door wie (voorkeur heeft wel de dossierhouder).[2]
- Als berichten met bestuurlijke besluitvorming op de juiste manier worden overgeheveld/'gewit' kunnen bewindspersonen en BR-leden iedere week hun berichten wissen.

[1] Het gaat hierbij niet om: afstemmen over een woordvoeringslijn; een nadere toelichting vragen op een kwestie/document; afspreken om met elkaar te bellen; een presentatie of werkbezoek toezeggen of weigeren; een oordeel geven over iemand of iets; persoonlijke conversaties over bijvoorbeeld thuiswerken, ziekmeldingen, verjaardagen en familie; partijpolitieke chatconversatie; verwijzingen naar/toelichtingen op artikelen en internetberichten.

[2] De dossierhouder kan ook een DG of directeur zijn.

Hoe worden deze richtlijnen gecommuniceerd binnen Financiën?
De richtlijnen omtrent het archiveren van chatberichten m.b.t. bestuurlijke besluitvorming gelden voor alle medewerkers binnen Financiën (ook externen). Er is een communicatieplan en de middelen zijn in de maak. Ook staan er informatiepunten (zie tabel) klaar om te helpen met specifieke vragen.

Type vragen	***Communicatiemiddel en -inzet***	***Informatiepunten***

Bewustwording + Algemene vragen over onderwerp	• Artikel op Rijksportaal met bijlages en een FAQ Daarna met regelmaat onder de aandacht brengen d.m.v. interviews, poll etc.
	• Via leidinggevende:
	  ○ Via een e-mail;[3] &
	  ○ Periodiek aandacht voor vragen vanuit een MT
	• Opnemen in introductieprogramma nieuwe medewerkers
		Telefoon + ICT = SSC-ICT mailbox
		Digidoc vragen = docdirekt mailbox
		Juridische inhoudelijke vragen = wobverzoekendjz@minfin.nl

Vragen over het exporteren van berichten	• PDF met instructies voor iPhone en Samsung, per chatberichtenapp.	SSC-ICT
Vragen over opslaan van berichten	• PDF met instructies over stappenplan en uitleg per stap	Voor Digidoc: Doc-Direkt servicepunt (informatieenarchiefdiensten@minbzk.nl of 070 342 6903)

Hoe moeten chatberichten m.b.t. bestuurlijke besluitvorming gearchiveerd worden?
Chatberichten met besluitvorming die niet wordt overgeheveld via Digidoc of via e-mail, kunnen door middel van het volgende stappenplan gearchiveerd worden. Een visuele instructie wordt hiervoor beschikbaar. Tevens is hierbij ondersteuning mogelijk (zie hierboven).

1.	**Identificeren**: Het herkennen van de inhoud van een chatbericht als zijnde bestuurlijke besluitvorming.
2.	**Selecteren**: Het vaststellen dat de informatie rondom de bestuurlijke besluitvorming in het chatbericht moet worden bewaard, omdat het niet op andere wijze is vastgelegd in het DMS.
3.	**Exporteren**: Het overbrengen van het chatbericht of de chatberichten uit de berichtenapp naar een daarvoor aangewezen locatie.
4.	**Verzending**: Verzenden van de chatberichten naar de juiste dossierhouder
5.	**Opslaan**: Het vastleggen van de informatie uit het chatbericht in het DMS.

Consequenties van niet goed archiveren van berichten met bestuurlijke besluitvorming

- Een departement behoort zijn informatiehuishouding op orde hebben. Het wissen van niet juist vastgelegde bestuurlijke besluitvorming kan daarom juridische, organisatorische en bestuurlijke gevolgen hebben. Uiteindelijk kan ook een bewindspersoon ter verantwoording worden geroepen over het niet op orde hebben van zijn of haar informatiehuishouding.
- Daarnaast wordt er ook gechat met derden. Voorkomen dient te worden dat chatberichten m.b.t. bestuurlijke besluitvorming bij Financiën niet goed worden vastgelegd, maar dat deze informatie bij derden wel is gearchiveerd.
- Uit de Wob – bevestigd in de Rijksbrede instructie – volgt dat de documenten die op dat moment beschikbaar zijn onder het verzoek vallen. Er treedt dan een standstill in: berichten kunnen niet worden

[3] Directeuren wordt verzocht om een door de CIO opgestelde informatiemail te versturen aan de eigen medewerkers. Naar verwachting wordt deze mail 6 april a.s. naar directeuren verstuurd.

gewist. Bij de inventarisatie van de documenten die onder een Wob-verzoek vallen, wordt vervolgens beoordeeld of de chatberichten onderdeel vormen van het Wob-besluit.

Ministerie van Financiën

TER BESLISSING
Aan
de minister
de staatssecretaris van Financiën - Fiscaliteit en Belastingdienst
de staatssecretaris van Financiën - Toeslagen en Douane

SG Cluster
Directie Bedrijfsvoering

Persoonsgegevens

nota

Veiligstellen chatberichten en sms bewindspersonen

Datum
4 oktober 2022

Notanummer
2022-0000243074

Bijlagen
1. Instructie BZK
2. Nota aan BR

Aanleiding

Op 3 oktober 2022 heeft de Inspectie Overheidsinformatie en Erfgoed (hierna: Inspectie OE) het rapport "De archivering van chatberichten bij het ministerie van Algemene Zaken" gepubliceerd. Naar aanleiding van de bevindingen en aanbevelingen in het rapport heeft het kabinet medegedeeld dat de chatberichten van alle kabinetsleden veiliggesteld en bewaard zullen worden in afwachting van advies over aanpassing van de rijksbrede chatinstructie.

Beslispunt

We adviseren voor het veiligstellen gebruik te maken van ondersteuning vanuit de eenheid Informatisering (hierna: BEDR/I). Als u hiervan afziet dan zult u het veiligstellen zelf moeten organiseren.

- U wordt gevraagd aan te geven of u gebruik van wilt maken van ondersteuning bij het maandelijks veiligstellen van uw chatberichten.

Kernpunten

- U wordt door BZK geadviseerd zich aan de volgende uitgangspunten te houden bij het gebruik van SMS en berichtenapps:
  - Beperk het gebruik van SMS en berichtenapps voor zakelijke communicatie.
  - Scheid privé, partij politieke en zakelijke communicatie. Maak bij voorkeur gebruik van een zakelijke telefoon én een privé-telefoon.
  - Zorg ervoor dat 'automatisch verwijderen van berichten' uitgezet is.
  - Verwijder geen berichten van de eigen telefoon totdat het beleid rond SMS en chatberichten is aangepast. Nb: partijcorrespondentie en privé-berichten mogen desgewenst wel worden verwijderd,.
  - Maak binnen de organisatie afspraken met welke frequentie berichten worden veiliggesteld en wie dit doet.

  Deze uitgangspunten zijn door BZK met alle departementen gedeeld.
- De BR is op 8 juli geïnformeerd over de noodzaak voor het veiligstellen van zakelijke chatberichten. De BR leden en hun plaatsvervangers kunnen op basis van vrijwilligheid gebruik maken van I-ondersteuning voor het maandelijks ophalen van berichten.
- Om de toezegging van het kabinet in te vullen, wordt u geadviseerd, net als de BR-leden, gebruik te maken van de mogelijkheid om maandelijks de chatberichten op uw zakelijke telefoon veilig te laten stellen. Indien u daarmee instemt zal hiervoor via het secretariaat een afspraak gemaakt worden.

Toelichting

Archivering van chatberichten

- De zakelijke correspondentie van bewindspersonen, waaronder chatconversaties via sms of bijv. Whatsapp, valt onder de reikwijdte van de Archiefwet, de Wet open overheid (hierna: Woo) en de Wet parlementaire enquêtes (hierna: Wpe). Dit is ook van toepassing op de zakelijke correspondentie tussen bewindspersonen onderling.
- Om die reden adviseren wij u een strikte scheiding aan te brengen: gebruik uw zakelijke telefoon voor zakelijke correspondentie en uw privé telefoon voor privé en partijpolitieke correspondentie.
- BEDR/I kan het veiligstellen van sms- en WhatsAppberichten voor u verzorgen. De berichten zijn daardoor beschermd tegen verwijdering en beschikbaar voor informatieverzoeken.
- Het veiligstellen gebeurt met de standaard exportfunctie van bijv. Whatsapp. De veiliggestelde chatberichten worden op een usb-stick bewaard in de kluis van het gerubriceerd archief.
- Er kan niet gegarandeerd worden dat in de totaliteit van uw chatverkeer helemaal geen privé of partijpolitieke conversaties veilig gesteld worden. Omgekeerd valt zakelijke correspondentie op een privételefoon ook onder de reikwijdte van Woo en Archiefwet.
- Om privé- en partijpolitieke correspondentie via de zakelijke telefoon zo veel mogelijk uit te sluiten kunt u zelf aangeven van welke contacten geen conversaties geëxporteerd hoeven worden. Bij twijfel of vermenging van zakelijke, partijpolitieke en privé berichten worden de conversaties vooralsnog geheel veiliggesteld.
- Indien u onverhoopt toch zakelijke conversaties op uw privételefoon heeft dan kunt u dit bij de i-ondersteuning aangeven. Hier kunt u dan ook een, eenmalige, export van laten maken.
- Verwijder geen berichten, zelfs al is de verwijdering rechtmatig, bijvoorbeeld omdat het geen zakelijke informatie is, dan kan het alsnog de schijn hebben van achterhouden van informatie. De verwijdering van niet zakelijke berichten zal op controleerbare wijze plaats vinden bij de daadwerkelijke archivering.
- Dit betreft een tijdelijke werkwijze. Wanneer de rijksbrede instructie gereed komt, brengt BEDR/I de procedure hiermee in overstemming. Gedurende de tijdelijke werkwijze veiliggestelde berichten die daar volgens de instructie voor in aanmerking komen, zullen dan digitaal gearchiveerd worden. Andere berichten worden verwijderd.

Wet open overheid

- Sms en chatberichten zijn opvraagbaar onder de Woo. Het raadplegen en leveren van berichten voor bijvoorbeeld een Parlementaire Enquête of Woo-verzoek geschiedt na toestemming van de directeur BOA.
- Verzamelen van chatberichten voor een informatieverzoek gebeurt door medewerkers bij BEDR. Het doornemen van de verzamelde chats op relevantie, en het lakken, geschiedt door ambtelijke ondersteuning bij BOA (eventueel in samenwerking met uw P-gv. Alle medewerkers hebben een vertrouwensfunctie.
- Wanneer een Woo-verzoeker chatberichten opvraagt, wordt altijd getoetst of deze op grond van de Woo openbaar gemaakt kunnen worden of dat er een uitzonderingsgrond van toepassing is.
- Het spreekt voor zich dat u tijdig en vooraf wordt geïnformeerd als berichten van u worden geopenbaard.

Politiek/bestuurlijke context

- Naar aanleiding van een publicatie en debat in de Tweede Kamer op 19 mei jl. over de archivering en verwijdering van chatberichten van de minister president heeft de Inspectie OE een onderzoek ingesteld naar de archivering van chatberichten bij AZ. Het rapport hierover is op 3 oktober jl. gepubliceerd.
- De Inspectie OE oordeelt dat de werkwijze van de minister president in lijn is met de rijksbrede Instructie bewaren chatberichten, maar dat deze instructie niet voldoet aan de Archiefwet. De Inspectie OE beveelt de minister van BZK aan deze met de wet in lijn te brengen. Een advies hierover wordt voor het einde van het jaar verwacht.
- Tot die tijd is besloten voor de in deze nota beschreven werkwijze, om te voldoen aan de wet en om tegemoet te komen aan de wensen van de Kamer.

Informatie die niet openbaar gemaakt kan worden

Niet van toepassing.

Chatberichtenarchivering

voor bewindspersonen

Inleiding

De Inspectie Overheidsinformatie en Erfgoed heeft onderzoek gedaan naar de archivering van chatberichten bij het ministerie van Algemene Zaken. In haar rapport van 3 oktober 2022 oordeelt de Inspectie dat de huidige Instructie bewaren chatberichten (de chatinstructie) niet voldoet aan de eisen van de eisen van de Archiefwet en doet de aanbeveling de instructie daarmee in lijn te brengen.

Met de aanbieding van het inspectierapport aan de Kamer door AZ (mede namens OCW en BZK) is aangegeven dat de regeringscommissaris informatiehuishouding als ook het Adviescollege Openbaarheid en Informatiehuishouding zich over dezelfde materie buigen waarbij het Adviescollege door de minister van Binnenlandse Zaken en Koninkrijksrelaties is gevraagd om alle onderzoeken in samenhang te bezien. Dat advies wordt voor het einde van het jaar verwacht waarna het kabinet op de kortst mogelijke termijn hier nader op zal reageren.

In afwachting daarvan wordt onderzocht op welke wijze de chatinstructie aanpassing vergt. In deze tussenfase worden de chatberichten van de leden van het kabinet bewaard ten behoeve van veiligstelling en archivering en worden er dus geen chatberichten verwijderd. Met uitzondering van partij-politieke en privé-berichten, die vallen immers niet onder de reikwijdte van de Archiefwet zoals de Inspectie zelf ook concludeert (paragraaf 2.4.7, p.13)

Uitgangspunten

- **Beperk het gebruik** van SMS en berichtenapps.
- **Scheid** privé, partij politieke en zakelijke communicatie.
  Maak bij voorkeur gebruik van een zakelijke telefoon én een privé-telefoon
- Zorg ervoor dat **'automatisch verwijderen van berichten' uitgezet** is.
- **Verwijder geen berichten van de eigen telefoon** totdat het beleid rond sms en chatberichten is aangepast (Nb: partijcorrespondentie en privé-berichten mogen desgewenst wel worden verwijderd)
- **Maak binnen de organisatie afspraken** (en leg die vast) met welke frequentie berichten worden veiliggesteld en wie dit doet. Informatiespecialisten kunnen hier ondersteuning bij bieden.

Tijdelijke instructie (tot het beleid is aangescherpt)

Voor de tussenfase is ten behoeve van de bewindspersonen een instructie gevraagd voor het gebruik, opslaan en veilig stellen van de sms- en chatberichten voor de periode tot de nieuwe handreiking/instructie chatberichten is vastgesteld. Gedurende deze periode worden sms- en chatberichten niet verwijderd.

Deze instructie beschrijft hoe de functie "automatisch verwijderen" correct kan worden ingesteld op de mobiele telefoon.

Correcte instelling voor "Automatisch verwijderen - uit"

Het uitzetten van de functie automatisch in Whatsapp en Signal verwijderen gaat als volgt:

Bij Whatsapp:

1. Open de app Whatsapp
2. Ga naar "instellingen" [Rechtsonder]
3. Ga naar Accounts
4. Ga naar Privacy
5. Zoek naar "Berichten met vervaldatum"
6. Zet de optie Standaardtimer voor berichten op **'UIT**

Bij Signal:

1. Open de app Signal
2. Klik op je eigen foto [Linksboven]
3. Ga naar "instellingen"
4. Ga naar "Privacy"
5. Zoek naar "Verlopende berichten"
6. Zet de optie "Standaard-tijdspanne voor toekomstige gesprekken" op **'UIT'**

Chatberichtenarchivering

voor ondersteuners

Instructie voor opslaan van sms en chatberichten

Deze instructie beschrijft hoe sms- en chatberichten kunnen worden opgeslagen.

Het opslaan van chatberichten (inclusief meta-data) via de export van Whatsapp gaat als volgt:

Whatsapp Export voor Android (Samsung):

1. Open de app **WhatsApp**.
2. Tik op het tabblad Chats…
3. Open het gesprek dat u wilt **exporteren** naar uw mail. Doe dit door op de naam van de contactpersoon te tikken.
4. Tik rechtsboven op het pictogram van de **drie puntjes**.
5. Tik op Meer > Tik op Chat **exporteren**.
6. Tik op "**niet bijvoegen**" of "**bijvoegen**" van media, waardoor bijlagen in de chat wel/niet worden veiliggesteld.
7. Tik op het **Email icoontje**
8. Het chatgesprek wordt omgezet naar een zip-bestand en staat in de bijlage van de e-mail. Typ achter 'Aan' uw **eigen mailadres** of het adres van een centraal email **postbus**.
9. **Verstuur** de **mail** zoals u gewend bent.
10. Ga naar uw eigen email en download de foto met screenshot(s)
11. Sla de foto op in een beveiligde/beheerde applicatie van de organisatie bv. het Document Management Systeem.

Whatsapp Export voor IOS (iPhone):

1. Open de app **WhatsApp**.
2. Tik op het tabblad Chats…
3. Open het gesprek dat u wilt exporteren naar uw mail. Doe dit door op de naam van de contactpersoon te tikken.
4. Tik bovenaan in het scherm op de **naam** van de persoon.
5. Tik op Exporteer chat, scrol naar onder in het instellingenscherm.
6. Tik op Voeg media bij om de uitgewisselde foto's, video's en documenten mee te sturen. Wilt u dat niet, tik dan op Zonder media.
7. Tik op E-mail.
8. Het chatgesprek wordt omgezet naar een zip-bestand en staat in de bijlage van de e-mail. Typ achter 'Aan' uw **eigen mailadres** of het adres van een centraal email **postbus**.
9. **Verstuur** de **mail** zoals u gewend bent.
10. Ga naar uw eigen email en download de foto met screenshot(s)
11. Sla de foto op in een beveiligde/beheerde applicatie van de organisatie bv. het Document Management Systeem.

Het opslaan van **SMS en Signal** chatberichten (exclusief meta-data) via de screenshot van mobiele telefoons gaat als volgt:

Screenshot voor SMS en Signal voor alle telefoons:

1. Open de app SMS of Signal
2. Open de chatconversatie.
3. Maak screenshots van de sms- of chatberichten.
4. Ga op de mobiele telefoon naar de app waarin foto's worden opgeslagen
5. Selecteer de foto of foto's van de screenshot(s).
6. Verstuur de foto(s) via de zakelijke email naar het eigen email adres of het adres van een centraal email postbus.
7. Download de foto met screenshot(s) uit uw e-mailbox of het centrale email postbus.
8. Sla de foto op in een beveiligde/beheerde applicatie van de organisatie bv. het Document Management Systeem.

Ministerie van Financiën

TER BESPREKING
Aan
de leden van de Bestuursraad

SG-Cluster
Directie Bedrijfsvoering

Persoonsgegevens

nota

Archiveren SMS en chatberichten

Datum
24 juni 2022

Notanummer
2022-0000153254

Bijlagen
geen

Afgestemd met
- PIOO
- BOA
- DJZ
- BVA

Aanleiding

In de Tweede kamer zijn op 16 mei jl. vragen gesteld over het gebruik van sms-berichten en het verwijderen daarvan door de minister-president. De manier waarop de MP omgaat met zijn sms-berichten, lijkt op de werkwijze uit de beleidslijn 'Bewaren appberichten' zoals ook de bewindspersonen (hierna: bwp) bij FIN wordt geadviseerd. Tijdens het plenaire debat in de Tweede Kamer van 19 mei bleek de werkwijze van de MP bepaald niet onomstreden. Op 14 juni jl. heeft de Tweede Kamercommissie voor binnenlandse zaken een rondetafel-bijeenkomst gehouden over de vraag of de beleidslijn en uitwerking ervan in de RDDI-handreiking 'Bewaren appberichten' stroken met de Archiefwet en de Woo. Het voorgaande toont aan dat dit onderwerp in het brandpunt van de (politieke) belangstelling staat. Om die reden wordt in deze nota ingegaan op vraag hoe de beleidslijn bij FIN is geïmplementeerd en hoe hier feitelijk uitvoering aan wordt gegeven. Deze nota bevat tevens een advies over de vervolgstappen.

Kern

- In maart-mei 2020 is de beleidslijn 'Bewaren chatberichten' door de BR vastgesteld. De beleidslijn is van toepassing op alle ambtenaren van het departement en op de bewindspersonen. De beleidslijn is, voor het beleidsdepartement voorzien van werkinstructies en FAQ's, gecommuniceerd op het Rijksportaal en via alle directeuren.
- De minister is op 11 april jl. in de bwp-staf geïnformeerd over het gebruik van privémiddelen voor zakelijke correspondentie in relatie tot openbaarheid en archivering. Ter voorbereiding is de nota over 'archivering van chatberichten' gedeeld met alle deelnemers van de bwp-staf.
- In Digidoc zijn bij controle slechts enkele chatberichten aangetroffen[1]. Medewerkers zijn sinds maart 2020 niet op grote schaal overgegaan tot het archiveren van conversaties. Dit is niet op voorhand als onjuist te betitelen, maar roept – indachtig de recente politieke discussie – vragen op over: a. de naleving van de beleidslijn en b. over de volledigheid en betrouwbaarheid van het archief van FIN kernministerie.

[1] Kanttekening: deze berichten zijn moeilijk te vinden, omdat ze niet als een aparte informatiecategorie opgenomen worden, maar als een e-mail, plaatje, pdf of een csv bestand.

- Naar aanleiding van de discussie in de Tweede kamer over het sms-gebruik van de minister-president onderzoekt de Inspectie Overheidsinformatie en Erfgoed of AZ in strijd met de Archiefwet heeft gehandeld. De uitkomst van het onderzoek kan tot aanpassing van interdepartementale beleidslijn leiden. Dit zal naar verwachting einde van het jaar zijn.
- Interdepartementaal is door Rijksprogramma Duurzame Digitale Informatiehuishouding (RDDI) in maart jl. ten aanzien van de implementatie van de beleidslijn geconcludeerd dat een specifiekere invulling van het beleid met een centrale aanpak wenselijk is. Dit is nog niet geconcretiseerd.
- De Tweede Kamer deed in het debat van 19 mei jl. een duidelijke oproep om te komen tot een uniforme werkwijze (aangenomen motie van het lid motie Ellian (VVD), Kamerstukken II 2021/22, 35 925 III, nr. 24), maar drong nog niet aan op het wekelijks uitlezen en veiligstellen van telefoons (verworpen motie van het lid Dassen (Volt), Kamerstukken II 2021/22, 35 925 III, nr. 22). Om die reden adviseren wij u om niet al te ferm voor de troepen uit te willen lopen.
- Tegelijkertijd blijkt duidelijk uit het debat van 19 mei jl. dat de persoonlijke selectie van te archiveren en te verwijderen berichten de politieke en ambtelijke top kwetsbaar maakt. Om die reden kunnen wij ons voorstellen dat Financiën op dit vlak wel een stap wil zetten. Hiervoor zijn wij te rade gegaan bij andere departementen (SZW, BZK, VWS). Een deel van de bewindspersonen of BR-leden kiest voor het – op basis van vrijwilligheid – laten uitlezen van een telefoon en het veiligstellen van berichten door de organisatie. Die veiliggestelde berichten kunnen op een later moment door de bewindspersoon of door het BR lid zelf worden doorzocht. Op basis van vrijwilligheid kan ambtelijk FIN dat voor hen doen.
- Voor de Parlementaire Enquête Fraudebeleid en Dienstverlening (PEFD) is recentelijk gestart met een pilot voor het ondersteunen van de verzameling van chatberichten bij bwp en BR. Dit kan voor sms- en WhatsAppberichten op iPhones[2] door een back-up van de berichten te maken op een laptop. Waarbij berichten alleen worden veiliggesteld, selectie en archivering zijn nu nog buiten scope. De berichten zijn zo beschikbaar voor informatieverzoeken. De werkwijze wordt door de eenheid Informatisering en BOA tijdens het zomerreces verder uitgewerkt. De procedure moet voldoen aan de vereisten van uit AVG en BIO. Voor het raadplegen en het mogen leveren van de berichten van BR-leden ten behoeve van bijvoorbeeld een Parlementaire Enquête geschiedt middels de procedure *Raadplegen digitaal berichtenverkeer* uit het personeelsreglement.

[2] Voor andere apps of besturingssystemen is dit mogelijk middels apps op de telefoon zelf.

Advies
Gegeven dat de beleidslijn nog gaat worden aangepast (a.g.v. de discussie in de TK), zal dat impact gaan hebben op de nog in te voeren nieuwe werkwijze. De bestuursraad wordt derhalve geadviseerd:

- pas over te gaan tot aanpassing van de werkwijze bij FIN als de beleidslijn in interdepartementale context is aangepast. De huidige werkwijze derhalve voorlopig te handhaven, aangevuld met enkele maatregelen die nu ook al door enkele andere departementen worden gehanteerd:
  - Het op basis van vrijwilligheid periodiek veiligstellen van sms- en chatberichten van de bwp door de eenheid Informatisering.
  - De BR-leden worden in staat gesteld vrijwillig van dezelfde dienstverlening gebruik maken en hun berichten veilig te laten stellen.

Managers en medewerkers van Financiën worden nogmaals geïnformeerd over het gebruik van berichtenapps en de archivering ervan, middels communicatie op het Rijksportaal en in de roadshow Informatiebeheer (zie nota BEDR 155226 gebruik email en persoonlijke schijven).

Toelichting

De Afdeling Bestuursrechtspraak van de Raad van State heeft op 20 maart 2019 geoordeeld dat sms- en WhatsApp-berichten vallen onder de reikwijdte van de Wob (na 1 mei 2022: Woo). Op 3 juli 2019 is in het SG-overleg aanvullend beleid vastgesteld voor het gebruik van berichtenapps en het bewaren van chatberichten binnen het Rijk. Dit beleid omvat de volgende drie speerpunten:

1. Het gebruik van berichtenapps voor formeel zakelijke communicatie wordt zoveel mogelijk beperkt;
2. Het gebruik van berichtenapps voor bestuurlijke aangelegenheden wordt ontraden;
3. Het berichtenverkeer dat toch plaatsvindt, wordt periodiek geschift. Te archiveren berichten worden handmatig geëxporteerd en veiliggesteld, tenzij deze al op een andere wijze zijn vastgelegd en gearchiveerd, bijvoorbeeld in een e-mail, nota of in een verslag. Niet archiefwaardige berichten worden verwijderd. Als berichten niet worden geschift, vastgelegd of gearchiveerd, mogen berichten, zonder overduidelijk privékarakter, in ieder geval niet worden verwijderd.

Discussie over de beleidslijn in het publieke domein en TK
De discussie spitst zich toe op enerzijds de smalle definitie van te archiveren berichten, namelijk alleen de berichten over *bestuurlijke besluitvorming*. Een term die de Archiefwet niet kent. Vanuit de Archiefwet geldt dat alle vastgelegde zakelijke informatie gearchiveerd moet worden.
Anderzijds zijn er vragen over de rechtmatigheid van het ongecontroleerd verwijderen van berichten. De Archiefwet staat vernietigen van zakelijke informatie slechts toe mits dit informatietype in een selectielijst staat. De Woo verbiedt verwijdering, zolang er een informatieverzoek loopt.
Zelfs al is de verwijdering van berichten door bwp rechtmatig, bijvoorbeeld omdat het geen zakelijke informatie is, dan nog kan het de schijn hebben van achterhouden van informatie.\

Invulling beleidslijn bij andere departementen
Bij andere departementen (o.a. SZW, BZK, VWS) worden berichten van BR-leden en bewindspersonen al actief veiliggesteld en gearchiveerd.
Bij VWS worden in het kader van de archivering van de Covid-19 pandemie relevante chatberichten van ongeveer 120 sleutelfiguren maandelijks opgehaald en gearchiveerd. Dit is een dagtaak voor één ondersteunend medewerker.

Advies t.a.v. gebruik

- Zie af van het gebruik van berichtenapps om bestuurlijke aangelegenheden te bespreken: "App met beleid, niet over beleid";
- Gebruik je privételefoon niet voor zakelijke communicatie, als je dat wel doet bij gebruik van 1 telefoon, gebruik dan verschillende apps voor privé en voor zakelijk gebruik;
- Gebruik geen timers of andere opties die berichten na een periode automatisch verwijderen (na veiligstellen en archivering kunnen desgewenst alle berichten worden verwijderd op de telefoon);

Informatie die niet openbaar gemaakt kan worden

Niet van toepassing.

Ministerie van Financiën

TER ADVISERING
Aan
de minister
de staatssecretaris van Financiën - Fiscaliteit en Belastingdienst
de staatssecretaris van Financiën - Toeslagen en Douane

SG Cluster
Directie Bedrijfsvoering

Persoonsgegevens

nota

Veiligstellen chatberichten en SMS

Datum
12 december 2022

Notanummer
2022-0000318327

Bijlagen
BEDR 243074

Aanleiding

In de bijgevoegde nota BEDR 243074 bent u geïnformeerd over de noodzaak om chatberichten periodiek veilig te stellen en de mogelijkheid om dit middels een periodieke export van berichten te laten uitvoeren. Bij FIN is voorgesteld dit te doen door de chatberichten te exporteren, waarbij de telefoon even uit handen gegeven wordt. In recent interdepartementaal overleg heeft BZK aangegeven dat er nog een tweede manier is om berichten veilig te stellen. Om die reden leggen wij u (allen) deze twee mogelijkheden voor.

Advies

U wordt gevraagd aan te geven of u gebruik wilt maken van veiligstellen van chatberichten middels:

1. Periodieke export of
2. Automatische opslag van een back-up in de iCloud, waar naast uzelf ten minste 1 medewerker van het ministerie (bijvoorbeeld P-gv. eveneens toegang toe heeft.

26.01.23
kies
voor 2 en
naast mij
heeft P-gv.
toegang.
Dnee

Kernpunten

- Werkbaar alternatief. Naast de mogelijkheid van periodieke export is het tijdelijk ook mogelijk om chat- en smsberichten veilig te stellen als automatische back-up in de iCloud. Dit is toegestaan vanuit BZK onder voorwaarde dat een ambtenaar, bijvoorbeeld de politiek adviseur, toegang heeft tot deze back-up. Zo berusten de berichten niet alleen bij u, maar ook onder (een vertegenwoordiger van) de organisatie.
- Tijdelijk. De bestaande beleidslijnen rondom het archiveren van berichten zullen in de toekomst nog aangepast gaan worden. Wanneer het beleid opnieuw is vastgesteld kan niet meer volstaan worden met veiligstellen in de iCloud. De aldaar tijdelijk veiliggestelde berichten moeten daarna worden gearchiveerd; uiteraard voor zover deze berichten o.b.v. de aangepaste beleidslijn zijn aan te merken als archiefwaardig. Voor nieuwe berichten geldt daarna hetzelfde.
- Wij herhalen om die reden dat het aanbeveling verdient om terughoudend gebruik te maken van berichtenapps.
- Vrijstelling. Zeker is dat privéberichten vrijgesteld zijn van veiligstellen (en archivering). Partijpolitieke conversaties zijn ook een uitzondering, maar moeilijker om eenduidig te identificeren.

Toelichting

iCloud: Alternatief voor het uitlezen of exporteren van chatberichten
Zoals u heeft kunnen lezen in de nota BEDR 243074 geldt dat berichten veiliggesteld moeten worden tot er een aangepaste beleidslijn voor het archiveren van chatberichten is. Dit volgt uit een toezegging van de MP aan de Tweede Kamer. Door BZK is hieraan de voorwaarde verbonden dat de berichten uit het persoonlijke domein van de bewindspersoon zijn gehaald en onder het beheer van ministerie zijn geplaatst.

Vanuit BZK is inmiddels aangegeven dat ook gebruik gemaakt mag worden van de mogelijkheid om sms- en chatberichten automatisch naar een back-up in de iCloud weg te schrijven, mits een ambtenaar van het ministerie toegang tot de back-up heeft. Dit is tijdelijke oplossing tot vanuit BZK nadere instructies beschikbaar zijn. Indien u van deze optie gebruik wilt maken, dan kan dat mits bijvoorbeeld uw politiek adviseur toegang krijgt tot de back-up. Om automatische back-up mogelijk te maken moeten de instellingen van de telefoon aangepast worden. Hiervoor kan de VIP ondersteuning ingezet worden.

Overheidsinformatie: berichten die de onder Archiefwet vallen
Naar verwachting zal het adviescollege Openbaarheid en Informatiehuishouding het door BZK gevraagde advies op donderdag 19 januari 2023 uitbrengen, de verwachting is dat BZK snel daarna met de aangepaste beleidslijn en werkinstructies voor de archivering van berichtenverkeer komt. Waarover u te zijne tijd geïnformeerd wordt.

Bij beide methodieken van veiligstellen geldt dat er vooralsnog geen berichten verwijderd mogen worden, behalve privé of partijpolitieke berichtenverkeer, omdat die niet onder de Archiefwet vallen. Hieronder volgen generieke uitgangspunten voor het archiveren, die mogelijk nog worden verbijzonderd in de geactualiseerde beleidslijn. Naar onze mening is dat laatste onontkoombaar. Voorop blijft staan dat terughoudend gebruik gemaakt moet worden van berichtenapps.

Overheidsorganen archiveren met als doel de reconstructie van overheidshandelen mogelijk te maken. Voor dit doel is de archivering belangrijk van berichten die betrekking hebben op de inhoud en de uitvoering van beleid en regelgeving van FIN en de besluitvorming daarover.

Praktische invulling
Concreet betekent dit dat al het berichtenverkeer over, de uitvoering van en besluitvorming over, beleid en regelgeving van FIN valt onder de noemer overheidsinformatie en moet als zodanig gearchiveerd worden. Het gaat dan concreet om:

a) berichtenverkeer met ambtenaren;
b) berichtenverkeer met andere bewindspersonen;
c) berichtenverkeer met P-gv. over voorliggende beleidsvoorstellen;
d) berichtenverkeer met externen, zoals burgers, belangenorganisaties, bedrijven en andere overheden.

Uitgesloten van archivering zijn:

e) het berichtenverkeer met de eigen politieke partijgenoten,- organen;
f) het berichtenverkeer over privé aangelegenheden met familie, vrienden, maar ook met ambtenaren of externe contacten.

Bij de inventarisatie voorafgaand aan het ophalen van het berichtenverkeer zal u gevraagd worden welke contacten per definitie onder categorie e en f vallen. Deze kunnen op voorhand van veiligstellen en archivering uitgesloten worden en mogen van de telefoon verwijderd worden.

Het berichtenverkeer (categorie a t/m d) dat uiteindelijk veiliggesteld is, wordt nog geschoond volgens de archiveringscriteria uit de aangepaste beleidslijn. Dit gebeurt door archiefmedewerkers op het moment van daadwerkelijke archivering.

Eventueel gebruik privé telefoon
Uitgangspunt is dat de zakelijke telefoon gebruikt wordt voor het zakelijke berichtenverkeer. Als een bewindspersoon ervoor kiest hiervoor een privételefoon te gebruiken dan ontslaat dit de bewindspersoon niet van de verantwoordelijkheid om deze berichten te archiveren. De bewindspersoon moet zelf aangeven dat dergelijke berichten er zijn. Bij de archivering kan ondersteuning geboden worden.

Eenheid van kabinetsbeleid
Sommige departementen gebruiken de eenheid van kabinetsbeleid als argument om berichtenverkeer tussen bewindspersonen niet openbaar te maken onder de Woo. Dit is echter geen belemmering om dergelijke berichten veilig te stellen of te archiveren.

Archiveren betekent niet dat deze informatie per definitie openbaar wordt. Berichten worden voor openbaar maken altijd beoordeeld op relevantie en of er wettelijke uitzonderingsgronden van toepassing zijn.

Politiek/bestuurlijke context
Naar aanleiding van een publicatie en debat in de Tweede Kamer op 19 mei jl. over de archivering en verwijdering van chatberichten van de minister president heeft de Inspectie OE een onderzoek ingesteld naar de archivering van chatberichten bij AZ. Het rapport hierover is op 3 oktober jl. gepubliceerd.

Informatie die niet openbaar gemaakt kan worden
Niet van toepassing.

Even kopje met

Persoonsgegevens

Ministerie van Financiën

Goede slag gemaakt, zo
nog enkele opmerkingen
for redactioneel tekst.
tbd

TER BESLISSING
Aan
de minister

SG-Cluster
Directie Digitalisering & Informatisering

Persoonsgegevens

nota

Beantwoording vragen leden Van Hijum en Omtzigt (beiden NSC) over chatarchivering

Datum
25 januari 2024

Notanummer
2024-0000048234

Bijlagen
1. Aanbiedingsbrief
2. Antwoorden
3. BEDR 117790
4. BEDR 243074
5. BEDR 318327

Aanleiding

Op 13 oktober 2023 is antwoord gegeven op vragen van de vaste commissie voor Financiën over chatarchivering en het archief voor de hotspot covid-19 bij Financiën[1]. Op 2 januari jl. hebben de leden van Hijum en Omtzigt hier aanvullende vragen over gesteld.

Beslispunten

- Bent u akkoord met het versturen van de bijgaande beantwoording (bijlage 2)? Als u akkoord bent dan verzoek ik u de aanbiedingsbrief (bijlage 1) te ondertekenen.
- Graag uw akkoord voor het openbaar maken van de nu voorliggende nota en 3 eerdere nota's (bijlagen 3, 4 en 5) aangaande chatarchivering, conform de beleidslijn Actieve openbaarmaking nota's.

Kernpunten

- De vragen gaan over de archivering van chatberichten door politieke en ambtelijke top in het algemeen en voor de hotspot Covid-19 in het bijzonder.
- Bewindspersonen en ambtelijke leiding zijn sinds mei 2020 meerdere keren geïnformeerd dat zakelijk berichten verkeer onder reikwijdte van Woo en Archiefwet 1995 vallen. De instructies hiervoor zijn meerdere keren aangescherpt.
- Het periodiek ophalen van chatberichten is voorzien, maar de uitrol is vertraagd. Naar verwachting is eind Q1/Begin Q2 2024 de eerste ronde afgerond, waarbij ook de chatberichten uit de periode van de Hotspot Covid-19 meegenomen wordt.
- Op 4 januari jl. zijn de berichten op de telefoon van mw. Kaag veiliggesteld, met terugwerkende kracht tot 1/1/2020.
- Van het vorige kabinet zijn alleen de chatberichten van de staatssecretaris voor Toeslagen en Douane veiliggesteld.
- Binnen de ambtelijke leiding zijn sinds maart 2020 (aanvang hotspot Covid-19 bij FIN) op niveaus van (plaatsvervangend) DG's 11 personele

[1] Kamerstuk 25295-2108 Lijst van vragen en antwoorden over het afbakeningsdocument van het ministerie van Financiën met het overzicht van beschikbare informatie over de hotspot Covid-19

wisselingen geweest. Zes functionarissen zijn nog werkzaam bij Financiën, hiervan worden de chatberichten alsnog veiliggesteld. Vijf functionarissen zijn niet meer werkzaam bij Financiën. Daarvan zijn geen chatberichten veiliggesteld. Met hen wordt contact gelegd hierover om te inventariseren in hoeverre berichten alsnog kunnen worden veiliggesteld.
- De beantwoording van de Kamervragen is afgestemd met de BZK/CIO RIJK voor wat betreft de rijksbrede maatregelen en met BuZa voor wat betreft het veiligstellen van chatberichten van mw. Kaag als minister van BuZa.

Toelichting
- FIN volgt het rijksbrede beleid ten aanzien van archivering van chatberichten van bewindspersonen.
- In 2022 is al begonnen met het uitwerken van maatregelen om chatberichten 2-maandelijks op te halen bij bewindspersonen en ambtelijke leiding. Het opzetten vergde meer doorlooptijd dan vooraf ingeschat vanwege enerzijds de stand van de techniek en anderzijds het uitwerken van privacy- en beveiligingseisen. Hier was binnen het rijk nog weinig ervaring mee en een aantal randvoorwaarden zijn, ook nu nog niet ingevuld, zoals een advies over bewaartermijnen (model selectielijst) of het schonen (opknippen van conversaties). In de tussentijd is steeds aangegeven dat zakelijke chatberichten niet verwijderd mogen worden.
- Inmiddels kan de directie D&I starten met het ophalen van chatberichten. Verwacht wordt dat eind Q1/Begin Q2 2024 de eerste ronde klaar is. Daarbij worden met terugwerkende kracht tot 1 januari 2020, of datum aantreden c.q. in dienst treden, chatberichten veiliggesteld. Periodiek wordt met alle betrokkenen afspraken ingepland om de aanwas van berichten veilig te stellen.
- De ondersteuning beperkt zich tot Whatsapp-, SMS- en iMessage berichten. Conversaties in andere apps, zoals Signal, kunnen niet geëxporteerd worden. Het gebruik hiervan wordt daarom vooralsnog afgeraden.

Communicatie
Woordvoering is meegenomen in de afstemming van de antwoorden.

Politiek/bestuurlijke context
Naar aanleiding van diverse adviezen over de archivering en verwijdering van chatberichten door de minister-president hebben de departementen en bewindspersonen instructie ontvangen over chatarchivering om voortijdige vernietiging van zakelijk berichtenverkeer te voorkomen.
In het begrotingsdebat AZ op 18 januari jl. zijn door NSC ook vragen gesteld over chatarchivering van de MP.

Informatie die niet openbaar gemaakt kan worden
Niet van toepassing.