18 februari 2022

Juridisch advies Archivering sociale media (fase 1)

Versie	Definitief
Voor	Rijksprogramma voor Duurzaam Digitale Informatiehuishouding
Door	ICTRecht B.V. mr. Jay Remmelzwaal mr. Dimmen Smolders

ICTRECHT
adviesbureau

Inhoudsopgave

1. Inleiding 3
2. Samenvatting 7
3. Wettelijk kader: Archiefwet, Wet openbaarheid van bestuur en Grondwet 11
3.1 De Archiefwet 11
3.2 De Wet openbaarheid van bestuur 12
3.3 Artikel 68 Grondwet 12
4. Toetsing aan de AVG 14
4.1 Doel en grondslag 14
4.2 Informatieplicht en rechten van betrokkenen 15
4.3 Maatregelen 17
5. Voorwaarden sociale media-platforms 20

1. Inleiding

Anno 2021 zijn sociale media platforms[1] zoals Twitter, Instagram en Facebook niet meer weg te denken als communicatiekanaal van veel bewindslieden en rijksambtenaren. Sociale media zijn een middel waarmee de overheid snel, direct en interactief informatie, ideeën en ervaringen kan uitwisselen met de maatschappij.

Naast kansen brengt de inzet van sociale media ook uitdagingen met zich mee voor de overheid. De informatie op sociale media moet eenvoudig terug te vinden zijn en duurzaam toegankelijk voor de periode dat het moet worden bewaard. Geen gemakkelijke opgave, zo blijkt in de praktijk.

Het berichtenverkeer op sociale media kenmerkt zich als een niet beheerde communicatiestroom, die ongestructureerd vanuit verschillende functionarissen binnen en buiten de overheid plaatsvindt. Daarbij worden commerciële platformen gebruikt en geldt uiteenlopende wet- en regelgeving. De communicatie op sociale media maakt geen onderdeel uit van de ICT-infrastructuur van de overheid en de informatie bevindt zich in een juridisch grijs gebied. Gevolg is dat de overheid geen of beperkte controle heeft over (her)gebruik, opslag, toegang en vindbaarheid van informatie op sociale media.

In de huidige overheidspraktijk ontbreekt het aan gestandaardiseerde werkwijzen, technische oplossingen en praktische beleidskaders. Er zijn nog geen voorzieningen voor het duurzaam toegankelijk maken van informatie op sociale media. De Inspectie Overheidsinformatie en Erfgoed (voorheen Erfgoedinspectie) heeft in 2016 gerapporteerd dat de overheid zich niet goed raad weet met de uitingen op sociale media. Er wordt nog te vaak vanuit gegaan dat deze uitingen niet vallen onder de werking van de Archiefwet, of er wordt vanuit gegaan dat duurzame toegankelijkheid van sociale media niet nodig of mogelijk is.

Project Archiveren sociale media bij het Rijk

Om Rijksorganisaties te ondersteunen bij het duurzaam toegankelijk maken van sociale media is in september van vorig jaar door het Rijksprogramma voor Duurzaam Digitale Informatiehuishouding (RDDI) gestart met het project *Archiveren sociale media bij het Rijk*. Centraal staat het bundelen van kennis, ontwikkelen van kennisproducten en uitwerken van een geschikte methodiek(en) voor het duurzaam toegankelijk maken van sociale media bij de Rijksoverheid.

Het uiteindelijke doel van het project is Rijksorganisaties in staat te stellen om de duurzame toegankelijkheid van sociale media eenvormig in te regelen, waarmee de informatie beschikbaar komt voor onder andere kennisdeling en verantwoording en ook wordt voldaan aan de wettelijke verplichtingen.

[1] Zogenaamde 'direct messaging apps', zoals WhatsApp en Facebook Messenger, vallen niet onder de reikwijdte van dit project.

Het RDDI heeft aan ons, ICTRecht, gevraagd om juridisch advies over archivering van sociale media-content door Rijksorganisaties.[2] Doel hiervan is om te komen tot een werkwijze voor het duurzaam toegankelijk maken van sociale media-content, in lijn met de Archiefwet 1995 (hierna: Archiefwet),[3] de Wet openbaarheid van bestuur (hierna: Wob),[4] artikel 68 Grondwet en de Algemene verordening gegevensbescherming (hierna: AVG). De AVG is van toepassing op de sociale media-content, wanneer deze persoonsgegevens bevat van individuen. Dit zijn bijvoorbeeld namen of gebruikersnamen, beeldmateriaal waar een individu herkenbaar op staat of andere informatie die iets zegt over een individu, in posts of reacties op sociale media.

Het type account bepaalt niet de aard van de inhoud: zowel persoonlijke, hybride als corporate accounts kunnen overheidsinformatie bevatten. De selectie van overheidsinformatie die bewaard moet worden onder de relevante wetgeving, komt in dit advies (fase 1) niet aan de orde. In fase 2 wordt het juridisch kader voor die selectie opgesteld, en in fase 3 het praktisch kader.

Projectplanning juridisch advies

Het RDDI heeft de wens om het advies gelaagd aan te pakken. Om aan deze wens te voldoen hebben wij het juridisch advies onderverdeeld in 3 fases. Hieronder wordt beschreven op welke handelingen de adviezen per fase betrekking hebben.

Fase 1 betreft het veiligstellen van sociale media-content op een veilige, centrale locatie, om vervolgens de te archiveren informatie daaruit te kunnen halen. Het advies in deze fase ziet dus uitdrukkelijk niet op het duurzaam toegankelijk maken van de openbare sociale media-content en ook niet op de reacties van derden en de privéberichten.

Fase 2 betreft het juridisch kader waarbinnen Rijksorganisaties dienen te handelen bij het duurzaam toegankelijk maken van de beschikbare sociale media-content (inclusief content van derden en privéberichten) door Rijksorganisaties. Denk hierbij aan waardering en selectie, ontsluiting, preservering, toegang, vernietiging of overbrenging naar het Nationaal Archief.

Fase 3 betreft het praktisch kader voor Rijksorganisaties, bij het verzamelen, duurzaam toegankelijk maken, en/of vernietigen van sociale media-content. In deze fase zal aan de hand van het juridisch kader een handleiding worden opgesteld voor deze handelingen.

Dit is het eerste advies, betreffende fase 1. Het vraagstuk in dit advies betreft het veiligstellen van sociale media-content op een veilige, centrale locatie, om

---

2 In dit advies wordt uitgegaan van het begrip van sociale media en content zoals omschreven in het Verslag Verkenning sociale media bij het Rijk, 22 februari 2021, versie 0.9. Zie: https://www.informatiehuishouding.nl/projecten/archiveren-sociale-media/Producten+%26+publicaties/verslagen/2020/03/30/verslag-verkenning-sociale-media-bij-het-rijk.

3 Naar verwachting treedt in 2023 de nieuwe Archiefwet 2021 in werking. Dit advies zal onder de nieuwe Archiefwet 2021 hetzelfde zijn als onder de Archiefwet 1995.

4 Op 1 mei 2021 treedt de Wet openbare overheid (Woo) in werking. De Wob zal dan worden ingetrokken. Dit advies zal onder de Woo hetzelfde zijn als onder de Wob.

vervolgens de informatie duurzaam toegankelijk te maken.[5] Dit advies ziet niet op het archiveren van de sociale media-content. Het vraagstuk over het archiveren van sociale media-content zal besproken worden in fase 2 en fase 3. Niettemin is het wel belangrijk om al bij het veiligstellen van de sociale media-content rekening te houden met de voorwaarden van archiveren.

Toepassingsgebied Fase 1

Dit advies dient om de vraag te beantwoorden, of de sociale media-content op accounts van bewindspersonen integraal kan worden veiliggesteld, om vervolgens binnen de totale hoeveelheid informatie de archiefbescheiden duurzaam toegankelijk te maken.

Omdat de huidige bewindspersonen naar verwachting snel zullen aftreden, zullen veel van hun huidige sociale media-accounts binnenkort niet meer bestaan, niet meer onder controle van het betreffende ministerie zijn of 'blanco' worden gemaakt voor gebruik door de opvolger (afhankelijk van het type account). Daarom is de wens van alle departementen om op zo kort mogelijke termijn de openbare content op de betreffende accounts (technisch) veilig te stellen op een centrale, afgeschermde digitale locatie. In een opvolgende fase zal dan rijksbreed worden gewerkt aan het duurzaam toegankelijk maken (lees: archiveren) van de content. Reacties van burgers zullen niet worden meegenomen tijdens het veiligstellen en worden in deze fase van het advies dus buiten beschouwing gelaten.

Voor dit advies worden drie typen sociale media-accounts onderscheiden: persoonlijke, hybride of corporate accounts. Een persoonlijk account wordt niet of nauwelijks ambtelijk ondersteund. Een corporate account is een volledig ambtelijk ondersteund corporate bewindsliedenaccount. Tussen deze uitersten bevindt zich de hybride variant. In de hybride variant plaatst de bewindspersoon (of de politiek assistent) zelf geregeld content, maar is er in meer of mindere mate ook sprake van ambtelijke ondersteuning.[6]

Het type account bepaalt niet de aard van de inhoud: zowel persoonlijke, hybride als corporate accounts kunnen overheidsinformatie bevatten. De selectie van overheidsinformatie die wel of niet bewaard moet worden onder de relevante wetgeving en het beleid bij departementen komt in dit advies (fase 1) niet aan de orde. In fase 2 wordt het juridisch kader voor die selectie opgesteld, en in fase 3 het praktisch kader.

Bij het veiligstellen van sociale media-content is het van belang dat wordt voldaan aan vigerende wet- en regelgeving waaronder de Archiefwet, de Wob en artikel 68 Grondwet. Overheidsorganen zijn op grond van de Archiefwet verplicht om de archiefbescheiden die bestemd zijn om onder het overheidsorgaan te berusten, te bewaren. Daarnaast kunnen burgers op grond van de Wob, in het belang van een goede en democratische bestuursvoering, een informatieverzoek doen ten aanzien

[5] Zie de website van het Nationaal Archief over de begrippen "waarderen" en "selecteren": https://www.nationaalarchief.nl/archiveren/waardering-selectie-en-vernietigen

[6] Zie voor de hier gehanteerde omschrijvingen van "persoonlijke", "hybride" en "corporate" sociale media-accounts de notitie *Bewindslieden op de sociale media*, vastgesteld door de VoRa op 21 januari 2021. Zie: https://www.communicatierijk.nl/documenten/publicaties/2021/03/08/bewindslieden-op-sociale-media.

van bestuurlijke aangelegenheden.[7] Verder hebben ministers en staatsecretarissen een inlichtingenplicht op grond van 68 Grondwet.

Het veiligstellen van sociale media-content raakt ook aan privacy, meer specifiek de AVG. Sociale media-content bevat namelijk persoonsgegevens. De AVG bevat bepalingen over de voorwaarden waaronder je persoonsgegevens mag verwerken. De AVG heeft in dat verband tevens een speciale positie gecreëerd voor het verder verwerken van persoonsgegevens met het oog op archivering in het algemeen belang.

Publicatierechten (auteursrechten, portretrechten en merkenrechten) kunnen verder een beperking vormen voor het rechtmatig veiligstellen van sociale media-content. Het veiligstellen brengt immers een vorm van verveelvoudiging met zich mee. Het verveelvoudigen van sociale media-content waarop publicatierechten van derden rusten, mag alleen met toestemming (licentieverlening) of wanneer er een beperking op het publicatierecht van kracht is. Gezien de niet-publieke aard van het veiligstellen, de noodzaak van snel veiligstellen en de latere mogelijkheid om eventuele content waarop publicatierechten rusten beperkt beschikbaar te maken, brengt dit echter geen onmiddellijk praktisch risico met zich mee.

Opbouw van dit advies

In dit advies hebben wij getoetst in hoeverre het juridisch gezien mogelijk is om sociale media-content veilig te stellen, en onder welke voorwaarden. Het vervolg van dit advies is als volgt opgebouwd:

- In hoofdstuk 2 is het advies samengevat. Deze samenvatting kan ook aan de betrokken Rijksorganisaties worden verstrekt, ter korte samenvatting van dit advies;
- In hoofdstuk 3 wordt ingegaan op het wettelijke kader van de Archiefwet, Wet openbaarheid van bestuur en de Grondwet;
- In hoofdstuk 4 wordt het veiligstellen van sociale media-content getoetst aan de AVG. Hier ligt het zwaartepunt van het advies, aangezien er een inbreuk wordt gemaakt op privacy, en er passende waarborgen getroffen dienen te worden;
- In hoofdstuk 5 wordt tot slot de beoogde werkwijze getoetst aan de voorwaarden van de belangrijkste sociale media-platforms.

[7] Artikel 3 lid Wet openbaarheid van bestuur.

Er is een zwaarwegend belang aanwezig voor het veiligstellen van sociale media-content van Rijksorganisaties, in het bijzonder ministeries en individuele bewindslieden. Dit veiligstellen dient wel te gebeuren binnen de kaders van overige wet- en regelgeving.

De aard van de sociale media-content bepaalt of deze onder de archiefplicht valt of niet. Het type sociale media-account (persoonlijk, hybride of corporate) speelt daarbij een ondergeschikte rol. Content van alle typen accounts dient daarom te worden veiliggesteld voor zover mogelijk, tenzij een (persoonlijk of hybride) account in het geheel geen overheidsinformatie bevat.

Het veiligstellen kan gebeuren zonder de toestemming van de bewindspersoon, omdat het veiligstellen noodzakelijk is om te voldoen aan de publieke taak van het betreffende ministerie.

Rijksorganisaties dienen te voldoen aan de eisen rond de informatieplicht en rechten van betrokkenen (zie §4.2) en bij het veiligstellen dienen daarnaast aanvullende maatregelen te worden doorgevoerd om aan de AVG te voldoen (§4.3).

Tot slot dient bij het veiligstellen aandacht uit te gaan naar de voorwaarden van de sociale media-platforms zoals omschreven in hoofdstuk 5.

Het belang van veiligstellen: Archiefwet, Wet openbaarheid van bestuur en Grondwet

Het veiligstellen van sociale media-content dient te worden bekeken tegen de achtergrond van het wettelijke kader van de Archiefwet, de Wob en de Grondwet.

De belangrijkste bepaling van de Archiefwet is dat overheden hun informatie in goede, geordende en toegankelijke staat moeten brengen en bewaren. De informatie moet dus makkelijk te vinden en te raadplegen zijn. Ook moeten overheden zorgen voor de vernietiging van informatie die daarvoor in aanmerking komt.

In de Archiefwet 1995 staan onder andere regels voor:

- de materiële verzorging en toegankelijkheid van archiefbescheiden (hoe makkelijk de informatie is in te zien);
- het bewaren en vernietigen van informatie;
- het vervangen van archiefstukken door reproducties (bijvoorbeeld een scan of kopie);
- het uitlenen of in eigendom overdragen van informatie;
- het overbrengen van informatie naar een archiefbewaarplaats zoals het Nationaal Archief;

- de openbaarheid van overheidsinformatie.[8]

In de context van publicaties op sociale media door Rijksorganisaties, valt alle informatie als archiefbescheiden onder de archiefplicht. Op grond van de Archiefwet zijn overheidsorganen verplicht om hun informatie die valt onder de archiefplicht in 'goede, geordende en toegankelijke staat' te bewaren en tijdig te vernietigen.[9] Doordat tot op heden sociale media-content van Rijksorganisaties vrijwel niet actief wordt veiliggesteld en gearchiveerd, is er sprake van een voortdurend contrast met de Archiefwet, zo benadrukt de Inspectie Overheidsinformatie en Erfgoed al lange tijd. Het voldoen aan de Archiefwet vormt een zwaarwegende reden om de nu beschikbare sociale media-content veilig te stellen met het oog op archivering in het algemeen belang.

Wanneer sociale media gebruikt wordt voor het uitvoeren van overheidstaken, valt de daarop geplaatste informatie onder de reikwijdte van de Wob. Als er een Wob-verzoek wordt ingediend, kan het zijn dat de content die op de sociale media-kanalen wordt gepubliceerd daarom beschikbaar moet zijn voor openbaarmaking in de zin van de Wob. De Wob verplicht overheidsorganisaties niet om informatie te bewaren: het bewaren en vernietigen wordt geregeld via het archiefwettelijk instrument de selectielijst. Bovendien hoeven documenten die naar hun aard reeds publiek zijn, zoals bij openbare berichten op sociale media het geval is, bij een Wob-verzoek niet nogmaals openbaar te worden gemaakt.[10] Met dien verstande dat documenten die publiek waren en later zijn verwijderd, mogelijk weer openbaar gemaakt moeten worden op grond van de Wob.

Volgens artikel 68 Grondwet hebben de ministers en staatssecretarissen tot slot een inlichtingenplicht aan het parlement. Deze plicht strekt zich ook uit tot documenten.[11] Daarmee is artikel 68 Grondwet kortom één van de pijlers van het parlementair democratisch stelsel.[12]

Toetsing aan de AVG van de verwerking van persoonsgegevens

Doel en grondslag

Persoonsgegevens dienen voor een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doel te worden verwerkt. Het doel van het veiligstellen van sociale media-content kan worden omschreven als: "*het veiligstellen van sociale-media content met het oog op duurzame toegankelijkheid".*

Naast de aanwezigheid van een doel dient het veiligstellen van sociale media-content rechtmatig te zijn. De AVG noemt expliciet dat *een verdere verwerking met het oog op archivering in het algemeen belang* als een met de aanvankelijke doeleinden verenigbare verwerking wordt beschouwd. Bij een verdere verwerking

8 Zie de website van het Nationaal Archief over het doel van de Archiefwet: https://www.nationaalarchief.nl/archiveren/kennisbank/wet-en-regelgeving.

9 Artikel 3, en artikel 5 lid 1, Archiefwet 1995.

10 Raad van State 12 juli 2017 – ECLI:NL:RVS:2017:1874.

11 Dit onderwerp is benoemd in Kamerstukken II 2001/02, 28 362, nr. 2, p. 3/4. Er is al jarenlang discussie over de precieze reikwijdte van de inlichtingenplicht. Zie het ongevraagd advies van de Raad van State Bijlage Kamerstukken II 2019/20, 35300, nr. 78 (15 juni 2020). In een reactie van de regering op dit ongevraagde advies geeft de regering aan in te stemmen met de analyses van de Raad.

12 Kamerstukken II 2001/02, 28 362, nr. 2, p. 1.

met het oog op archivering in het algemeen belang, wat het beoogde veiligstellen van sociale media-content omvat, is geen andere afzonderlijke rechtmatige grondslag vereist, dan die op grond waarvan de verzameling van persoonsgegevens werd toegestaan.

De verdere verwerking met het oog op archivering in het algemeen belang, het veiligstellen van sociale media-content, kan uiteindelijk "varen" op de grondslag voor het publiceren van de sociale media-content. Er zal altijd een rechtmatige grondslag aanwezig moeten zijn op basis waarvan de verzameling van persoonsgegevens werd toegestaan bij de publicatie van sociale media-content.

Informatieplicht en rechten van betrokkenen

De Rijksorganisatie dient het algemeen publiek te informeren over de verwerking van persoonsgegevens, die voortvloeit uit het veiligstellen van sociale media-content. Dit gebeurt middels de openbare privacyverklaring op de website van elke Rijksorganisatie die sociale media gebruikt.

De Rijksorganisatie dient ook rekening te houden met eventuele verzoeken om uitoefening van de wettelijke rechten met betrekking tot de persoonsgegevens in de sociale media-content. Zo kunnen zij verzoeken om de verwerkte persoonsgegevens in te zien, te corrigeren, te verwijderen, de verwerking te beperken en om overdraagbaarheid van de persoonsgegevens. Ook kan een betrokkene bezwaar maken tegen een verwerking van persoonsgegevens in het algemeen belang. In alle gevallen dient de Rijksorganisatie binnen de wettelijke termijn van één maand te reageren op de verzoeken. Afhankelijk van de complexiteit van de verzoeken en van het aantal verzoeken kan die termijn indien nodig met nog eens twee maanden worden verlengd. Zover dat mogelijk en verplicht is, dienen verzoeken te worden ingewilligd.

Maatregelen

De Rijksorganisatie dient al bij het veiligstellen van de sociale media-content rekening te houden met de relevante wetgeving. Daarom adviseren wij om reeds bij het veiligstellen van alle sociale media-content een zorgvuldige afweging te maken tussen het doel van het voldoen aan de Archiefwet en bescherming van persoonsgegevens, en de passende waarborgen te treffen zoals omschreven in 4.3.

Voorwaarden sociale media-platforms

Bij het veiligstellen van sociale media-content krijgt een Rijksorganisatie te maken met de voorwaarden van de sociale media-platforms. Als het (technisch) mogelijk is om de sociale media-content veilig te stellen zonder het accepteren van de voorwaarden, dan vormen de voorwaarden geen beletsel om de sociale media-content veilig te stellen.[13]

Dit is anders wanneer voor toegang tot de sociale media-content een account dient te worden aangemaakt. In deze gevallen worden de voorwaarden van het betreffende sociale media-platform geaccepteerd. Twitter, Facebook, Instagram en LinkedIn nemen in hun voorwaarden als uitgangspunt dat er geen gegevens mogen

[13] Er zijn oplossingen in de markt die veiligstelling- of archivering van sociale media beschikbaar maken, waarbij het niet nodig is om de voorwaarden van de sociale media platformen te accepteren. Hierbij kan gedacht worden aan oplossingen die gebruik maken van o.a. harvesting, capture en/of API technieken.

worden verzameld. Om niet in strijd met de voorwaarden te handelen kan een Rijksorganisatie met de sociale media-platforms in contact treden om specifieke afspraken te maken (toestemming te verkrijgen) ten aanzien van het veiligstellen van sociale media-content.

Mocht een Rijksorganisatie niet de benodigde afspraken willen of kunnen maken met de sociale-media platforms, dan stelt een Rijksorganisatie de sociale media-content in strijd met de voorwaarden van de sociale media-platforms veilig (wanprestatie). Het risico bestaat dat de sociale-media platforms in reactie daarop maatregelen nemen zoals omschreven in hoofdstuk 5.

3. Wettelijk kader: Archiefwet, Wet openbaarheid van bestuur en Grondwet

3.1 De Archiefwet

Overheidsorganen hebben op grond van de Archiefwet 1995 (Archiefwet) de plicht om alle archiefbescheiden te bewaren, en eventueel over te brengen naar een archiefbewaarplaats of te vernietigen, conform vastgestelde selectielijsten. Alle informatie die door overheidsorganen wordt opgemaakt of ontvangen, die bestemd is onder het overheidsorgaan te berusten, ongeacht de vorm, valt onder de definitie van archiefbescheiden.[14] In de context van publicaties op sociale media door Rijksorganisaties betekent dit, dat alle gepubliceerde berichten inclusief tekst, digitaal beeldmateriaal en eventuele andere informatie, alsmede de opmerkingen bij berichten, als archiefbescheiden onder de archiefplicht vallen, waarbij in een selectielijst wordt vastgesteld welke informatie voor vernietiging in aanmerking komt en welke informatie (blijvend) bewaard wordt.

Op grond van de Archiefwet zijn overheidsorganen verplicht om hun informatie in 'goede, geordende en toegankelijke staat' te brengen en te bewaren[15] en, indien van toepassing, tijdig te vernietigen.[16] Voor de verschillende categorieën overheidsinformatie worden bewaartermijnen conform de Archiefwet vastgelegd in selectielijsten. De bewaartermijn kan variëren van relatief kort, zoals één maand tot één jaar, tot permanent na publicatie van overheidsinformatie. Categorieën informatie met een beperkte bewaartermijn dienen na afloop daarvan te worden vernietigd. Permanent te bewaren informatie is informatie die blijvend van maatschappelijke en historische waarde is. Deze moet na twintig jaar worden overgebracht naar een archiefbewaarplaats en wordt daar in principe openbaar en raadpleegbaar. Informatie die persoonsgegevens bevat mag alleen worden bewaard wanneer dat noodzakelijk is in het algemeen belang, zie ook hoofdstuk 4. Iedere sociale media-uiting bevat in beginsel persoonsgegevens. Dit geldt in beginsel voor iedere sociale media-uiting, omdat deze persoonsgegevens bevat.

Na ontstaan van de informatie zijn er op basis van de Archiefwet dus twee mogelijkheden: de informatie wordt bewaard totdat de bewaartermijn in de selectielijst is verstreken, en wordt daarna vernietigd, of na twintig jaar overgebracht naar een archiefbewaarplaats.

Op dit moment voldoen Rijksorganisaties, op een uitzondering na, niet aan de Archiefwet, als het aankomt op het bewaren van gepubliceerde informatie op sociale media.[17] De Inspectie Overheidsinformatie en Erfgoed hamert er reeds sinds 2012 op, dat het niet bewaren van gepubliceerde informatie op sociale media door Rijksorganisaties in strijd is met de Archiefwet.[18] Deze voortdurende overtreding brengt een zwaarwegend belang mee om met spoed over te gaan tot het

14 Artikel 1 c. 1° Archiefwet 1995.
15 Artikel 3 Archiefwet 1995.
16 Artikel 5 lid 1 Archiefwet 1995.
17 Dit is geconstateerd door de Erfgoedinspectie (nu Inspectie Overheidsinformatie en Erfgoed), zie het "Rapport Erfgoedinspectie: Webarchivering bij de centrale overheid" (2016) en het rapport "Wel digitaal, nog niet duurzaam".
18 Zie het rapport van de Inspectie Overheidsinformatie en Erfgoed "Een dementerende overheid 2.0?" (2021).

veiligstellen en selecteren van sociale media-content, met het oog op archivering in het algemeen belang.

3.2 De Wet openbaarheid van bestuur

De Wet openbaarheid van bestuur (Wob) dient het belang van een goede en democratische bestuursvoering en een recht op openbaarmaking van informatie. In artikel 3 lid 1 van de Wob staat dat ieder bestuursorgaan (in de zin van de Algemene wet bestuursrecht) verzocht kan worden om informatie uit documenten die te maken heeft met bestuurlijke aangelegenheden openbaar te maken.

Een document in de zin van de Wob wordt gedefinieerd als:

> *"een bij een bestuursorgaan berustend schriftelijk stuk of ander materiaal dat gegevens bevat."*

De wet en de rechtspraak leggen het begrip "document" ruim uit. In dit verband heeft de Raad van State in maart 2019 geoordeeld dat WhatsApp-berichten, sms-jes en gelijksoortige chatberichten, die bij het uitvoeren van overheidstaken gebruikt zijn, onder de reikwijdte van de Wob vallen.[19]

Ook wanneer sociale media gebruikt wordt voor het uitvoeren van overheidstaken, kan de daarop gepubliceerde en verzamelde informatie onder de reikwijdte van de Wob vallen. Als er een Wob-verzoek binnenkomt, dient de content die op de sociale media-kanalen wordt gepubliceerd, en onder de reikwijdte van verzoek valt, voor het uitvoeren van overheidstaken daarom bij de Rijksorganisaties beschikbaar te zijn voor openbaarmaking in de zin van de Wob. Dit geldt ook voor content van derden en privéberichten. Documenten die naar hun aard reeds publiek zijn, zoals bij openbare berichten op sociale media het geval is, hoeven bij een Wob-verzoek niet nogmaals openbaar te worden gemaakt.[20]

Het bestuursorgaan kan openbaarmaking van informatie achterwege laten wanneer zich (een of meerdere) van de in artikel 10 en 11 Wob genoemde uitzonderingsgronden voordoen, waaronder uitzonderingen die zien op de bescherming van persoonlijke levenssfeer.[21] Deze uitzondering ziet op het verstrekken van de informatie, niet op het bewaren ervan.

3.3 Artikel 68 Grondwet

Volgens artikel 68 Grondwet hebben de ministers en staatssecretarissen een actieve inlichtingenplicht aan het parlement. Kamerleden kunnen daarnaast vragen stellen, waarna er een plicht rust op de ministers en staatssecretarissen om de gevraagde inlichten te geven. Deze plicht strekt zich ook uit tot documenten.[22] Het parlement kan zijn controletaak niet uitvoeren als het niet over de daarvoor noodzakelijke

19 Raad van State 20 maar 2019, ECLI:NL:RVS:2019:899.

20 Raad van State 12 juli 2018 – ECLI:NL:RVS:2017:1874.

21 Artikel 10 lid 1 sub d Wet openbaarheid van bestuur; Artikel 10 lid 2 sub e) Wet openbaarheid van bestuur en artikel 11 Wet openbaarheid van bestuur.

22 Dit onderwerp is benoemd in Kamerstukken II 2001/02, 28 362, nr. 2, p. 3/4. Er is al jarenlang discussie over de precieze reikwijdte van de inlichtingenplicht. Zie het ongevraagd advies van de Raad van State Bijlage Kamerstukken II 2019/20, 35300, nr. 78 (15 juni 2020). In een reactie van de regering op dit ongevraagde advies geeft de regering aan in te stemmen met de analyses van de Raad.

informatie beschikt. Daarmee is artikel 68 Grondwet kortom één van de pijlers van het parlementair democratisch stelsel.[23]

[23] Kamerstukken II 2001/02, 28 362, nr. 2, p. 1.

4. Toetsing aan de AVG

4.1 Doel en grondslag

Doel

Persoonsgegevens dienen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden te worden verwerkt.[24] Dit betekent dat een Rijksorganisatie voorafgaand aan het veiligstellen van sociale media-content gemotiveerd moet uitleggen waarom de gegevensverwerking plaatsvindt. Het doel van het veiligstellen van sociale media-content is om informatie duurzaam toegankelijk te maken, met het oog op archivering in het algemeen belang.

Persoonsgegevens mogen niet verder worden verwerkt op een wijze die onverenigbaar is met de oorspronkelijke doeleinden.[25] In dit geval zijn de 'oorspronkelijke doeleinden' de reden(en) van een Rijksorganisatie om de informatie te publiceren. Ten aanzien van archiveren in het algemeen belang heeft de AVG een speciale positie gecreëerd. De AVG noemt expliciet dat *een verdere verwerking met het oog op archivering in het algemeen belang* als een met de aanvankelijke doeleinden verenigbare verwerking wordt beschouwd.[26] Daaruit vloeit voort dat het archiveren in het algemeen belang geen nieuw verwerkingsdoel oplevert, maar rechtmatig kan plaatsvinden in het verlengde van het oorspronkelijke verwerkingsdoel.

Grondslag

Naast de aanwezigheid van een welbepaald, uitdrukkelijk en gerechtvaardigd doel dient het veiligstellen van sociale media-content rechtmatig te zijn. Dit betekent dat er een wettelijke grondslag moet zijn om de inbreuk op de privacy van de betrokkenen te rechtvaardigen.[27] Het veiligstellen van sociale media-content is dus rechtmatig als er een wettelijke grondslag in de zin van de AVG bestaat voor deze verwerking.

Het veiligstellen van sociale media-content is, zoals hierboven onder 'Doel' beschreven, een verdere verwerking met het oog op archivering in het algemeen belang, en is daarom verenigbaar met het aanvankelijke doeleinde. Bij een verdere verwerking met het oog op archivering in het algemeen belang is geen andere afzonderlijke rechtmatige grondslag vereist, dan die op grond waarvan de oorspronkelijke verwerking van persoonsgegevens plaatsvindt.[28] Er is dus geen nieuwe grondslag nodig voor het veiligstellen van de sociale media-content.

De sociale media-content van de gebruikers bij Rijksorganisaties verschilt qua inhoud en gebruik.[29] Als de sociale media-content is ontstaan uit en/of tijdens een overheidstaak, dan kan de noodzakelijkheid voor de uitvoering van een publieke taak van algemeen belang als rechtmatige grondslag worden aangewezen voor het

---

24 Artikel 5 lid 1 (b) Algemene verordening gegevensbescherming.
25 Idem.
26 Overweging 50 Algemene verordening gegevensbescherming en artikel 5 lid 1 (b) Algemene verordening gegevensbescherming.
27 Artikel 6 lid 1 Algemene verordening gegevensbescherming.
28 Overweging 50 Algemene verordening gegevensbescherming en *Kamerstukken* II 2017/18, 34 851, nr. 3, p. 38.
29 Verslag Verkenning sociale media bij het Rijk, 22 februari 2021, versie 0.9, § 3.8.

publiceren van de sociale media-content.[30] Dit neemt echter niet weg dat in (incidentele) gevallen een andere grondslag aanwezig kan zijn, wanneer de verwerking niet noodzakelijk is voor de uitvoering van een publieke taak van algemeen belang. Bijvoorbeeld in het geval dat de betrokkene toestemming heeft gegeven voor het publiceren van beeldmateriaal.[31]

Voor de oorspronkelijke verzameling en eventuele publicatie van persoonsgegevens zal altijd een rechtmatige grondslag aanwezig moeten zijn, om deze te mogen archiveren in het algemeen belang. De Raad van State heeft in 2017 geoordeeld dat een bewaarplicht op grond van de Archiefwet geen excuus is om onder alle omstandigheden persoonsgegevens te bewaren die oorspronkelijk niet mochten worden verwerkt.[32] Aan de bewaarplicht op grond van de Archiefwet wordt pas toegekomen als persoonsgegevens in overeenstemming met de AVG worden verwerkt.[33] De sociale media-content mag dus alleen worden gearchiveerd als er eerder ook al een rechtmatige grondslag aanwezig was voor de publicatie van de sociale media-content, zoals in de voorgaande alinea wordt beschreven. In dat verband is het met het oog op de archiefplicht extra belangrijk dat een Rijksorganisatie maatregelen neemt om te zorgen dat alle persoonsgegevens bij de creatie van de content rechtmatig worden verwerkt.

4.2 Informatieplicht en rechten van betrokkenen

Informatieplicht

Rijksorganisaties dienen betrokkenen, waaronder bewindspersonen, te informeren over de verwerking van persoonsgegevens met het oog op archivering in het algemeen belang. In het algemeen geldt, bij een verwerking voor een ander doel dan waarvoor de persoonsgegevens zijn verzameld, dat de informatie over de nieuwe verwerking voorafgaand verstrekt dient te worden aan de betrokkenen.[34] Bij een verwerking met het oog op archivering in het algemeen belang geldt daarvoor echter een uitzondering, wanneer vooraf informeren onmogelijk is of een onevenredige inspanning vereist. De informatie over de verwerking dient in dat geval openbaar te worden gemaakt.[35]

Het is vooraf niet bekend van wie persoonsgegevens worden verwerkt op de sociale media-pagina's van Rijksorganisaties. Bovendien vindt de archivering nu plaats met terugwerkende kracht (hoewel dit in de toekomst wellicht 'by design' kan plaatsvinden, zie de volgende alinea). De informatie over de verwerking kan dus alleen maar worden gericht aan het algemene publiek. Dit betekent dat elke Rijksorganisatie de (eventuele) verwerking van persoonsgegevens als onderdeel van sociale media-content, specifiek met het oog op archivering in het algemeen belang, moet behandelen in de openbare privacyverklaring. Dit doel, de wettelijke grondslag (zie §4.1), de bewaartermijn, eventuele ontvangers van de persoonsgegevens, informatie over eventuele ontvangers buiten de Europese Economische Ruimte en alle andere verplichte informatie dient dus te worden beschreven in de privacyverklaring van elke Rijksorganisatie die gebruik maakt van sociale media.

30 Artikel 6 lid 1 e) Algemene verordening gegevensbescherming.
31 Artikel 6 lid 1 a) Algemene verordening gegevensbescherming.
32 Raad van State 23 augustus 2017, ECLI:NL:RVS:2017:2232.
33 Rechtbank Rotterdam 18 maart 2020, ECLI:NL:RBROT:2020:2257.
34 Artikelen 13 en 14 Algemene verordening gegevensbescherming.
35 Artikel 14 lid 5 (b) Algemene verordening gegevensbescherming.

In de toekomst kan archivering mogelijk 'by design' plaatsvinden. Dat betekent dat de stappen van het archiveren al in het ontwerp van het creëren of verzamelen van overheidsinformatie op sociale media zullen zijn ingebakken. Wanneer het naleven van de archiefwet in de processen wordt ingebakken, dient ook steeds te worden beoordeeld of het mogelijk is om de archivering in het algemeen belang, middels de juiste processtappen en technische instellingen, volgens de uitgangspunten van 'privacy by design' en 'privacy by default' te laten plaatsvinden.[36]

Rechten van betrokkenen

Betrokkenen hebben een aantal rechten ten aanzien van de verwerking van hun persoonsgegevens. Zo kunnen zij verzoeken om de verwerkte persoonsgegevens in te zien, te corrigeren, te verwijderen en de verwerking te beperken. Ook kan een betrokkene bezwaar maken tegen een verwerking van persoonsgegevens op grond van de uitvoering van een publieke taak van algemeen belang (zie §4.1 onder Grondslag). Hieronder wordt beschreven in welke gevallen, en hoe, Rijksorganisaties aan zulke verzoeken dienen te voldoen.

In de veilig te stellen sociale media-content bevinden zich zowel archiefbescheiden als overige informatie, zijnde privé-content die niet onder de archiefwet valt. De status van archiefbescheiden bepaalt in hoeverre de rechten van betrokkenen van toepassing zijn. In het toepassingsbereik van dit advies (fase 1, aangaande het veiligstellen) geldt echter dat de veiliggestelde informatie niet onder één van de beperkingen van de rechten van betrokkenen kan vallen. Op archiefbescheiden die nog niet in een archiefbewaarplaats zijn opgenomen, zijn deze rechten immers onverminderd van toepassing. Wel kunnen er andere specifieke beperkingen zijn op de uitoefening van rechten, zo kan een wettelijke bewaarplicht een beperking vormen op het recht op gegevenswissing, waardoor het recht op gegevenswissing niet van toepassing is. Hieronder wordt nader ingegaan op de situaties waarbij de rechten van betrokkenen beperkt of niet van toepassing zijn, wat in latere fases van belang zal zijn.

Op archiefbescheiden die in een archiefbewaarplaats zijn opgenomen, zijn het recht op inzage, het recht op correctie, het recht op beperking van de verwerking (deels) en het recht op overdraagbaarheid niet van toepassing.[37]

Hoewel het algemene inzagerecht, zoals hierboven beschreven, niet van toepassing is op archiefbescheiden in een archiefbewaarplaats, is het recht op inzage wel van toepassing op archiefbescheiden die voor vernietiging zijn aangewezen of nog niet zijn overgebracht naar een archiefbewaarplaats: op verzoek dient een betrokkene inzage te krijgen in die archiefbescheiden, waarin persoonsgegevens van diegene zijn opgenomen. Dit geldt niet wanneer verzoeken om inzage zodanig ongericht zijn, dat deze in redelijkheid niet kunnen worden ingewilligd.[38]

Het recht op correctie van persoonsgegevens geldt niet voor archiefbescheiden. Met het oog op de integriteit van de archiefbescheiden is correctie op verzoek van een betrokkene ook niet wenselijk. Een betrokkene heeft echter wel het recht om,

[36] Artikel 25 Algemene verordening gegevensbescherming.
[37] Artikel 45 lid 1 Uitvoeringswet Algemene verordening gegevensbescherming.
[38] Artikel 45 lid 2 Uitvoeringswet Algemene verordening gegevensbescherming.

in geval van onjuiste persoonsgegevens, zijn eigen lezing aan de desbetreffende archiefbescheiden toe te voegen.[39]

Het recht op gegevenswissing geldt niet wanneer de verwerking gebeurt met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden, en verwijdering van de persoonsgegevens het doel van archivering in het algemeen belang bedreigt.[40] Deze uitzondering geldt alleen wanneer bij de archivering passende waarborgen zijn genomen om de verwerking van persoonsgegevens te minimaliseren, bijvoorbeeld pseudonimisering of anonimisering.[41] Het is dus van belang om van alle persoonsgegevens die zich onder de content op sociale media bevinden, voorafgaand aan het bewaren als archiefbescheiden, te inspecteren op informatie die niet noodzakelijk is om te archiveren in het algemeen belang.

4.3 Maatregelen

De AVG is gericht op bescherming van persoonsgegevens. Een verwerking met het oog op archivering in het algemeen belang is daarom onderworpen aan passende waarborgen.[42] Deze waarborgen zijn gericht op dataminimalisatie. Dit betekent dat er zo min mogelijk persoonsgegevens moeten worden verwerkt, maar wel op een manier dat er voldoende persoonsgegevens worden verwerkt om aan het doel van de Archiefwet te voldoen.

De content van bewindspersonen die overheidsinformatie betreft, valt als archiefbescheiden onder de archiefplicht van het ministerie van de bewindspersoon. In het geval van informatieverzoeken van burgers (Wob) of het parlement (bijvoorbeeld in het kader van een parlementaire enquête) dient het ministerie eveneens over de gepubliceerde overheidsinformatie/content te beschikken.

Aangezien het vanuit technisch oogpunt in eerste instantie niet mogelijk is om slechts een selectie veilig te stellen/te archiveren, dient daarvoor eerst alle content te worden veiliggesteld. Vervolgens zal een verwerking moeten plaatsvinden om content die niet onder de archiefplicht valt blijvend te verwijderen. Toestemming van de bewindspersoon voor het veiligstellen is niet noodzakelijk. De noodzaak voor het betreffende ministerie om aan de Archiefwet te voldoen biedt de wettelijke grondslag.

De Rijksorganisatie dient echter wel al bij het veiligstellen van de sociale media-content zoveel mogelijk rekening te houden met het uiteindelijke doel om te archiveren. Op grond van de Archiefwet kunnen er beperkingen worden gesteld aan de openbaarheid, met het oog op de eerbiediging van de persoonlijke levenssfeer.[43] Daarom adviseren wij om reeds bij het veiligstellen van alle sociale media-content een zorgvuldige afweging te maken tussen het doel van archiveren (bewaren van belangrijke informatie) en bescherming van persoonsgegevens, en de volgende passende waarborgen te treffen:

39 Artikel 45 lid 3 Uitvoeringswet Algemene verordening gegevensbescherming.
40 Artikel 17 lid 3 (d) Algemene verordening gegevensbescherming.
41 Artikel 89 lid 1 Algemene verordening gegevensbescherming.
42 Artikel 89 lid 1 Algemene verordening gegevensbescherming. Zie ook artikel 24 Algemene verordening gegevensbescherming voor de algemene norm voor dergelijke waarborgen.
43 Artikel 15 lid 1 (a) Algemene verordening gegevensbescherming.

- Voer een DPIA uit op het project (zoals reeds beoogd wordt), om in kaart te brengen waar de specifieke risico's liggen en aantoonbaar te maken dat deze risico's zijn gemitigeerd, in zoverre dat de restrisico's aanvaardbaar zijn.

- Bewaar de sociale media-content van een persoonlijk of hybride account niet, wanneer de gehele content van dat gehele account niet is ontstaan uit en/of tijdens de uitvoering van een overheidstaak en daarmee als privé kan worden aangemerkt.

Vooruitlopend op het juridisch kader (fase 2 van dit advies), dienen bij voorkeur voorafgaand aan het veiligstellen, maar indien dat niet mogelijk is, daarna, zoveel als redelijkerwijs mogelijk de volgende maatregelen te worden genomen:

- Bewaar, voor zover technisch mogelijk, geen bijzondere persoonsgegevens en/of gevoelige persoonsgegevens, tenzij het bewaren zeer goed te verantwoorden is wegens een algemeen belang. Als de sociale media-content de waarde voor het algemeen belang verliest zonder bijzondere persoonsgegevens en/of gevoelige persoonsgegevens, dan mogen de bijzondere persoonsgegevens en/of gevoelige persoonsgegevens worden bewaard.[44]

- Bewaartermijnen: leg met inachtneming van de hiervoor genoemde passende waarborgen in selectielijsten vast wat blijvend bewaard blijft en wat niet, met in het laatste geval de geldende bewaartermijn.

- Doelbinding: gebruik de sociale media-content alleen voor archiveringsdoeleinden en niet ook voor andere doeleinden, tenzij er een wettelijke verplichting is waaraan de Rijksorganisatie gehoor moet geven.

- Toegang en autorisaties: zorg ervoor dat alleen personen toegang hebben tot de veiliggestelde sociale media-content, voor zover dat noodzakelijk is voor hun werkzaamheden met het oog op archivering in het algemeen belang. Praktisch gezien betekent dat, dat er scherp toezicht dient te worden gehouden op de juiste toegangsrechten, middels vooraf vastgestelde gebruikersprofielen binnen een autorisatiematrix.

- Verantwoordelijkheid: vul het verwerkingsregister aan met betrekking tot de verwerkingen van de sociale media-content.

Het kan voorkomen dat persoonsgegevens binnen de sociale media-content op grond van dit advies niet kunnen worden veiliggesteld, omdat de oorspronkelijke publicatie onrechtmatig was (zie §4.1 onder 'Grondslag'), maar de sociale media-content zelf wel bewaard dient te worden op grond van de Archiefwet. Wanneer de

[44] Bijzondere persoonsgegevens zijn limitatief opgesomd in artikel 9 Algemene verordening gegevensbescherming. Gevoelige persoonsgegevens zijn persoonsgegevens die (mogelijk) een hoog risico kunnen vormen voor de privacy van de betrokkene(n). Gevoelige persoonsgegevens zijn niet in de wet opgenomen. De Rijksorganisatie dient zelf een afweging te maken van (mogelijke) risico waarbij de vraag gesteld dient te worden hoe groot de mogelijke gevolgen zijn voor de betrokkene(n) indien de persoonsgegevens in verkeerde handen vallen en/of er misbruik gemaakt wordt van de persoonsgegevens. Denk bijvoorbeeld aan persoonsgegevens van kinderen op foto's en financiële gegevens.

onrechtmatigheid van de verwerking zwaarder weegt dan het belang van archivering in het algemeen belang van de betreffende informatie, dienen de persoonsgegevens door de archiefvormende organisaties te worden geanonimiseerd, bijvoorbeeld door de persoonsgegevens (tekst of beeldmateriaal) onherkenbaar te maken met een zwart vlak.

Door pas na het veiligstellen passende waarborgen te treffen handelt de Rijksorganisatie niet volledig in lijn met het begrip dataminimalisatie zoals bedoeld in de AVG. Een dergelijke handelswijze vormt daarom een risico. Om in de toekomst te zorgen dat archivering in het algemeen belang in lijn met de AVG plaatsvindt, dienen Rijksorganisaties zich reeds bij de creatie van sociale media-content te houden aan de richtlijnen die in fase 2 en 3 van dit advies zullen worden opgesteld.

5. Voorwaarden sociale media-platforms

Bij het veiligstellen van sociale media-content krijgt een Rijksorganisatie te maken met de voorwaarden van de sociale media-platforms. Om te bepalen of het veiligstellen van sociale media-content is toegestaan – volgens de voorwaarden – hebben wij onderzocht hoe Twitter, Facebook, Instagram en LinkedIn hiermee omgaan. In alle gevallen is het verzamelen van de informatie op de platforms (zoals 'scraping') verboden, tenzij de platforms daarvoor toestemming hebben verleend.

De relevante bepalingen uit de voorwaarden van Twitter, Facebook, Instagram en LinkedIn:

> Twitter
> *…(iii) access or search or attempt to access or search the Services by any means (automated or otherwise) other than through our currently available, published interfaces that are provided by Twitter (and only pursuant to the applicable terms and conditions), unless you have been specifically allowed to do so in a separate agreement with Twitter (NOTE: crawling the Services is permissible if done in accordance with the provisions of the robots.txt file, however, scraping the Services without the prior consent of Twitter is expressly prohibited);*[45]
>
> Facebook
> *3. Je mag geen gegevens verzamelen uit onze Producten of je hiertoe toegang verschaffen met behulp van geautomatiseerde middelen (zonder onze voorafgaande toestemming) of proberen toegang te krijgen tot gegevens waarvoor je geen toestemming hebt.*[46]
>
> Instagram
> *Je mag niet proberen om op ongeautoriseerde manieren accounts te maken of informatie te verzamelen of hier toegang toe te krijgen.*
> *Dit geldt ook voor het automatisch maken van accounts of het automatisch verzamelen van informatie zonder onze uitdrukkelijke toestemming.*[47]
>
> LinkedIn
> *You agree that you will not:*
>
> *2. Develop, support or use software, devices, scripts, robots or any other means or processes (including crawlers, browser plugins and add-ons or any other technology) to scrape the Services or otherwise copy profiles and other data from the Services;*[48]

Als het (technisch) mogelijk is om de sociale media-content veilig te stellen zonder het accepteren van de voorwaarden, dan vormen de voorwaarden geen beletsel om de sociale media-content veilig te stellen. Of dit daadwerkelijk mogelijk is, is echter twijfelachtig. Om toegang te krijgen tot alle benodigde sociale media-content is het

---

45 Twitter Terms of Service, 4. Using the Services, https://twitter.com/en/tos.
46 Facebook Servicevoorwaarden, 3, Je toezeggingen aan Facebook en aan onze community, https://www.facebook.com/terms.php.
47 Instagram Gebruikersvoorwaarden, Je verplichtingen, https://help.instagram.com/581066165581870.
48 LinkedIn User Agreement, 8.2 Dont's, https://www.linkedin.com/legal/user-agreement#rights.

meestal noodzakelijk om een account aan te maken en de voorwaarden te accepteren.

Twitter, Facebook, Instagram en LinkedIn nemen als uitgangspunt dat er geen gegevens mogen worden verzameld. Om niet in strijd met de voorwaarden te handelen, is ons advies aan Rijksorganisaties om gezamenlijk met de sociale media-platforms in contact te treden, om specifieke afspraken te maken (toestemming te verkrijgen) voor het veiligstellen van sociale media-content.

Mocht een Rijksorganisatie niet de benodigde afspraken willen of kunnen maken met de sociale media-platforms, dan stelt een Rijksorganisatie de sociale media-content in strijd met de voorwaarden van de sociale media-platforms veilig (wanprestatie[49]). Het risico bestaat dat de sociale media-platforms in reactie daarop maatregelen nemen. Denk in eerste instantie aan blokkades die kunnen worden opgeworpen door de sociale media-platforms. Daarnaast bestaat het risico dat de sociale media-platforms een Rijksorganisatie aansprakelijk stellen als het veiligstellen van sociale media-content tot aantoonbare schade leidt.

[49] Vergelijk Ryanair Ltd v PR Aviation BV, 15 januari 2015, C-30/14.