

Vergaderjaar 2022–2023

32 761

Verwerking en bescherming persoonsgegevens

26 643

Informatie- en communicatietechnologie (ICT)

Nr. 286

BRIEF VAN DE STAATSSECRETARIS VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES EN MINISTER VAN ECONOMISCHE ZAKEN EN KLIMAAT

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 5 september 2023

Tijdens het Tweede Kamerdebat op 17 mei 2023 (Handelingen II 2022/23, nr. 82, item 11) heeft de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties toegezegd met een brief te komen over de inzet van het kabinet op het onderwerp van cookies.¹ Met deze brief informeren de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties en de Minister van Economische Zaken en Klimaat u mede namens de Minister voor Rechtsbescherming over cookies en online tracking. Onderwerpen waar elke internetgebruiker mee te maken heeft. Gebruikers worden op nagenoeg elke website geconfronteerd met cookiebanners. Daarbij is het vaak moeilijker om cookies te weigeren dan te accepteren, waardoor gebruikers de cookies vaak accepteren ondanks dat ze dat mogelijk niet echt willen. Voor gebruikers is vaak niet duidelijk of en aan wie de gegevens verzameld door cookies worden doorverkocht. Dit is een onwenselijke praktijk waar het kabinet wat aan wil doen.

Het kabinet vindt dat het mogelijk moet zijn om gemakkelijker cookies te kunnen weigeren. Het kabinet spant zich daar op Europees niveau voor in. Op nationaal niveau ziet het kabinet geen betekenisvolle mogelijkheden om met aanvullende wetgeving de huidige praktijk te verbeteren. De huidige wetgeving biedt echter al veel mogelijkheden voor toezicht. Daarnaast wil het kabinet inzetten op voorlichting en het versterken van de privacy op overheidswebsites.

¹ Cookies zijn het bekendste voorbeeld van tracking, maar niet de enige vorm. Waar in deze brief verwezen wordt naar cookies, wordt in het algemeen bedoeld: «via een elektronisch communicatienetwerk opslaan van of toegang verkrijgen tot informatie in de randapparatuur van een gebruiker». Dit betreft ook bijvoorbeeld browser/device fingerprinting, tracking pixels of javascripts. Op deze vormen van tracking is de Telecommunicatiewet ook van toepassing.

Deze brief beschrijft de huidige wetgeving rondom cookies en welke problemen er spelen in de praktijk. Daarna gaat de brief in op de Nederlandse inzet in Europa en wat Nederland op nationaal niveau gaat doen.

1. Huidige wetgeving

Sinds 2002 is de regelgeving omtrent cookies op Europees niveau geregeld in de ePrivacy-richtlijn.² In eerste instantie was voor de plaatsing van cookies geen toestemming nodig. Wel moest de eindgebruiker, degene bij wie de cookies wordt geplaatst, de mogelijkheid worden geboden de plaatsing/het aflezen van cookies te weigeren.

In 2009 is de ePrivacy-richtlijn aangepast³ en in 2012 is deze aanpassing geïmplementeerd in de Telecommunicatiewet (Tw).⁴ Daarin is sindsdien bepaald dat cookies slechts mogen worden geplaatst als de eindgebruiker voorzien is van *duidelijke en volledige informatie* en als deze voorafgaand toestemming heeft verleend. Voor de definitie van *duidelijke en volledige informatie* en de definitie van *toestemming* wordt verwezen naar de Algemene verordening gegevensbescherming (AVG). Er gelden uitzonderingen voor de toestemmings- en informatievereisten. Het doel van deze uitzonderingen is om het aantal cookiebanners te beperken als het gaat om cookies met geen of gering effect op de privacy van de eindgebruiker. Het gaat om de volgende drie uitzonderingen:

- Als een cookie bedoeld is om communicatie over een communicatienetwerk uit te voeren (bijvoorbeeld sessiecookies);
- Als een cookie strikt noodzakelijk is om de door de eindgebruiker gevraagde dienst te leveren (ook wel bekend als functionele cookies);
- Als een cookie bedoeld is om informatie te verkrijgen over de kwaliteit en/of effectiviteit van de geleverde dienst, mits dit geen of geringe gevolgen heeft voor de persoonlijke levenssfeer (ook wel bekend als analytische cookies).

In de praktijk bevatten gegevens verkregen via cookies vaak persoonsgegevens.⁵ Dan is de AVG onverminderd van toepassing. De AVG vereist dat iedere verwerking van persoonsgegevens gebaseerd is op een geldige grondslag, waarvan toestemming er een is. Uit de Tw volgt dat voor de verwerking van de met cookies verkregen gegevens voor het doel dat wordt vermeld door de plaatser van de cookies toestemming vereist is. De toestemming bedoeld in de Tw moet voldoen aan de eisen die aan toestemming gesteld worden in de AVG. Toestemming moet onder andere een vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting zijn. De bepaling in de Tw heeft geen betrekking op de eventuele verdere verwerking van persoonsgegevens die via cookies zijn verkregen. Hiervoor geldt het algemene kader voor gegevensverwerkingen zoals neergelegd.

² Richtlijn 2002/58/EG van het Europees parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie), meer specifiek in artikel 5, derde lid.

³ Richtlijn 2009/136/EG van het Europees parlement en de Raad van 25 november 2009 tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronischecommunicatienetwerken en -diensten, Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie en Verordening (EG) nr. 2006/2004 betreffende samenwerking tussen de nationale instanties die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming.

⁴ Specifiek in artikel 11.7a.

⁵ De Telecommunicatiewet specificeert ook dat de verwerking van persoonsgegevens vermoed wordt als het doel is gegevens over het gebruik van verschillende diensten te verzamelen, combineren of analyseren zodat de gebruiker anders behandeld kan worden.

In het verleden verleenden sommige websites geen toegang tot een website als cookies niet geaccepteerd werden, de zogenoemde cookie-muren. De Tw regelt al sinds 2012 dat overheden geen cookiemuren mogen gebruiken. Met de komst van de AVG heeft de Autoriteit Persoonsgegevens (AP) in 2019 het begrip toestemming zo uitgelegd dat cookie-muren ook buiten de overheid niet zijn toegestaan, omdat het gebruik ervan niet goed verenigbaar is met vrijelijk gegeven toestemming.^{6, 7}

Cookies worden in de praktijk vaak geplaatst om het gedrag van eindgebruikers op het internet te volgen. Met behulp van algoritmes kan uit deze informatie een (interesse)profiel van de eindgebruiker worden opgesteld. Uiteraard geldt het toestemmingvereiste van de Tw ook voor deze cookies. Daarmee geldt voor gepersonaliseerde algoritmes, zoals verzocht in de motie van de leden Bouchallikh en Kathmann⁸, dat toestemming nodig is als de informatie voor het algoritme verkregen is via cookies.

Hoewel het vereiste van toestemming de wens van de eindgebruiker centraal stelt, zien we in de praktijk niet altijd dat dit heeft geleid tot een prettige gebruikerservaring. Eindgebruikers worden immers op elke website geconfronteerd met cookiebanners, waardoor zogenaamd «consentmoetheid» ontstaat: een vermoeidheid die ervoor zorgt dat de eindgebruiker overal akkoord mee gaat. Eindgebruikers accepteren daardoor standaard de cookies, ondanks dat dat mogelijk niet is wat zij echt willen. Een belangrijke rol in deze consentmoetheid spelen zogenoemde dark patterns: websites maken het moeilijker om cookies te weigeren dan te accepteren. Er is dan zeer waarschijnlijk geen sprake van «vrijelijk» gegeven toestemming, zoals de Tw en AVG vereisen. Het is aan de toezichthouder om dit te interpreteren, waar in deze brief later nader op ingegaan wordt.

Veel gegevens verkregen door cookies komen ook terecht bij derde partijen. Dat is voor eindgebruikers niet altijd duidelijk. Een voorbeeld daarvan is het realtime bieden, waarbij reclameruimte wordt verkocht op een veiling op basis van de gegevens verkregen uit cookies. Ook is het voor betrokkene onduidelijk hoe om rectificatie of wissen van de persoonsgegevens of beperking van de betreffende verwerking kan worden verzocht. Net als dat het onduidelijk is hoe om het recht tegen de verwerking bezwaar te maken en het recht op gegevensoverdraagbaarheid kan worden verzocht.

Samengevat is het dus vanaf 2012 zo dat websites geen cookies mogen plaatsen, tenzij er sprake is van toestemming. De huidige wetgeving sluit daarmee aan bij hetgeen dat verzocht is door uw Kamer in de motie van de leden Dekker-Abdulaziz en Kathmann.⁹ De praktijk die hieruit volgt kan echter beter. Het kabinet wil deze praktijk verbeteren met een versterking van het toezicht en aanvullende Europese regels om zo de privacy en gebruikerservaring van eindgebruikers te versterken.

2. Europese wetgeving

Websites en daarmee ook cookies hebben een grensoverschrijdende werking. Regulering is grensoverschrijdend daarom het meest effectief. Het is daarom van belang voor verbetering van de praktijk dat op Europees niveau gewerkt wordt aan wijzigingen. In 2017 is gestart aan de onderhandelingen over de ePrivacyverordening, waar cookiebeleid deel

⁶ Normuitleg ap cookiewalls | autoriteitpersoonsgegevens.nl.

⁷ edpb_guidelines_202005_consent | European data protection board (europa.eu).

⁸ Kamerstukken II. 2022/23, 32 761, nr. 275.

⁹ Kamerstuk 32 761, nr. 267.

van uitmaakt. Gezien dat deze onderhandelingen al jaren vast zitten, kijkt het kabinet naar alternatieve oplossingen, bijvoorbeeld waarbij Europese cookiewetgeving in een apart en hopelijk sneller traject los van de ePrivacyverordening wordt behandeld.

Uw Kamer heeft gevraagd aan het kabinet om te pleiten voor verbeteringen van Europese wetgeving.¹⁰ De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties heeft de wens om te komen tot Europese wetgeving wederom benoemd tijdens de Telecomraad van 2 juni 2023 (Kamerstuk 21 501-33, nr. 1029). Het kabinet is van plan hier de komende tijd in Europa aandacht voor te blijven vragen. Hiervoor werkt het kabinet ook aan een non-paper met de Nederlandse inzet.

Het kabinet streeft er naar, zonder afbreuk te willen doen aan de vereisten voor toestemming, dat in de Europese wetgeving geregeld wordt dat eindgebruikers in één keer aan kunnen geven met welke cookies zij wel of niet akkoord gaan. Bijvoorbeeld door instellingen in de browser. En dat websites gehoor moeten geven aan deze instelling. Zodat eindgebruikers dit niet langer per website en per bezoek hoeven aan te geven. Het in één keer toestemming geven of weigeren blijkt echter tot op heden niet (eenvoudig) realiseerbaar. Generiek toestemming geven voor cookies verhoudt zich bijvoorbeeld lastig ten opzichte van de in de AVG opgenomen eis dat een toestemming voldoende specifiek moet zijn.

Het kabinet blijft zich inzetten voor het in stand houden van het verbod op cookiemuren in Europees verband, zoals uw Kamer al in 2018 vroeg. Het kabinet wil verder de Nederlandse toestemmingsuitzondering voor analytische cookies Europees behouden.

3. Cookie pledge

Vanwege de vertraging in de onderhandelingen over de ePrivacyverordening heeft Eurocommissaris voor Justitie Reynders een initiatief gelanceerd om cookietoestemming voor eindgebruikers te versimpelen.¹¹ Het doel is om bedrijven vrijwillig te binden aan de resultaten van het initiatief. Het initiatief richt zich op drie onderwerpen, die elk behandeld worden in een werkgroep:

1. presentatie van informatie over bedrijfsmodellen en hun gevolgen op het gebied van privacy en toestemming aan consumenten;
2. alternatieven voor op tracking gebaseerde advertenties; en
3. technische oplossingen voor geautomatiseerd beheer van consumentenkeuzes.

Op 1 juni 2023 heeft de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties met Reynders gesproken over dit initiatief. Zij heeft namens het kabinet aangegeven dat Nederland het initiatief steunt en graag wil bijdragen. De Staatssecretaris heeft ook aangegeven dat het kabinet het liefst ziet dat het initiatief omgezet wordt in afdwingbare Europese regels. De Staatssecretaris wil de komende tijd ook spreken met bedrijven in Nederland om te kijken welke stappen zij kunnen zetten, in lijn met het Europese initiatief.

4. Toezicht

De Autoriteit Consument en Markt (ACM) is de toezichthouder op artikel 11.7a van de Telecommunicatiewet. De Autoriteit Persoonsgegevens (AP) is de toezichthouder op de AVG. Vanwege de samenhang tussen beide

¹⁰ Kamerstuk 32 761, nr. 266.

¹¹ Cookie Pledge | European Commission (europa.eu).

wetten, zijn beide toezichthouders in de praktijk bevoegd om te handhaven op cookies. De toezichthouders hebben daarvoor ook een samenwerkingsprotocol.

Het is aan de toezichthouders om te beoordelen of de huidige cookie-banners voldoen aan de eisen voor *duidelijke en volledige informatie* en *toestemming* zoals bedoeld in de AVG. Uiteindelijk is het aan de rechter om hierover te oordelen. Een uitspraak van het Hof van Justitie van de Europese Unie (HvJEU) bevestigde bijvoorbeeld dat vooraf aangevinkte vakjes niet leiden tot geldige toestemming.¹² En toezichthouders in andere Europese lidstaten hebben maatregelen genomen tegen (grote) bedrijven vanwege de inrichting van hun cookiebanner en de informatievoorziening omtrent doorverkoop.

Het kabinet ziet dat op Europees niveau verder gewerkt wordt aan deze normuitleg. Onder het Europees Comité voor gegevensbescherming (EDPB) is een *Cookie Banner Taskforce* opgericht. In hun rapport van januari 2023 bespreken zij hoe verschillende praktijken, zoals dark patterns, zich verhouden tot de ePrivacy-richtlijn en de AVG.¹³ De EDPB heeft ook een richtlijn uitgebracht over deze dark patterns op sociale media, die ook relevant kunnen zijn voor cookies.¹⁴

Een groot deel van de eerder genoemde problemen in de praktijk met cookies, wordt al geadresseerd in de Tw en de AVG. Op basis van de huidige wetgeving hebben de toezichthouders al veel mogelijkheden om te handhaven. Het is van belang dat dit ook gebeurt. De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties is met de AP in overleg hoe het toezicht op cookies versterkt kan worden. Samen met de Minister voor Rechtsbescherming willen we dit gesprek met beide toezichthouders voortzetten om het toezicht te versterken.

5. Mogelijkheden wijzigen nationale wetgeving

In het debat van 17 mei 2023 is de vraag gesteld wat Nederland kan en gaat doen om de wetgeving te verbeteren. Regulering op dit onderwerp wordt ingekaderd door de eerdergenoemde Europese ePrivacy-richtlijn en AVG. Dit maakt dat er slechts zeer beperkte ruimte is voor nationale invulling. Dat is ook niet vreemd, gezien het doel van harmonisatie en het grensoverschrijdende karakter van cookies. Het kabinet heeft daarom moeten concluderen dat het niet mogelijk is om op nationaal niveau betekenisvol af te wijken.

In het eerdergenoemde debat werd verwezen naar een Duitse wetsaanpassing op het gebied van cookies. In deze wetsaanpassing worden *Personal Information Management Systems (PIMS)* wettelijk geïntroduceerd. Deze PIMS kunnen door eindgebruikers gebruikt worden om toestemming voor en weigering van cookies bij te houden. Deze PIMS moeten die voorkeuren vervolgens doorgegeven aan de websites. In de wet wordt ook certificering voor PIMS geïntroduceerd.

De Duitse wetsaanpassing introduceert echter geen verplichting voor websites om de opgegeven voorkeur via PIMS te honoreren, omdat de ePrivacy-richtlijn hiervoor geen ruimte laat voor lidstaten. Ondanks dat de Duitse wet wordt aangepast, is hier nog steeds sprake van een initiatief waaraan bedrijven vrijwillig kunnen deelnemen. Iets wat bedrijven in het

¹² HvJ 1 oktober 2019, C-673/17, ECLI:EU:C:2019:801.

¹³ Report cookie banner taskforce | European Data Protection Board (europa.eu).

¹⁴ Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them | European Data Protection Board (europa.eu).

verleden al vrijwillig konden op basis van bijvoorbeeld het Do Not Track-sigitaal in de browser, en wat vrijwel niet gedaan werd.

6. Voorlichting

Uitgangspunt voor het kabinet is dat er wetgeving is die de privacy van eindgebruikers effectief beschermt en dat deze wetgeving uiteraard nageleefd dient te worden. Zoals eerder beschreven, is er ruimte voor verbetering in zowel de Europese wetgeving als de toepassing in de praktijk. Tegelijkertijd zijn er middelen voor eindgebruikers om hun privacy te beschermen. Het gaat dan bijvoorbeeld om browserplug-ins die cookies opruimen of beperken en cookiebanners verbergen. We willen kijken hoe wij de bekendheid van deze middelen kunnen vergroten.

7. Bij de overheid

Het is vanzelfsprekend van belang dat de Nederlandse (mede)overheden zich houden aan de wetgeving omtrent cookies. Dit bleek in de praktijk niet altijd het geval te zijn. In de beantwoording¹⁵ van Kamervragen heeft de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties daarom toegezegd een brief te sturen naar verschillende koepels over de naleving van de cookiewetgeving. Dat is in januari van dit jaar gedaan. Het toezicht op de naleving daarop is verder belegd bij de bevoegde toezichthouders.

Los van de wettelijke eisen, vinden wij het van belang dat burgers websites van de overheid onbespied door derde partijen kunnen bezoeken. Wij vinden het daarom wenselijk dat er geen third-party cookies of andere tracking gebruikt wordt op overheidswebsites, ongeacht het verkrijgen van toestemming. Maar dat ook breder geen informatie door derde partijen verkregen kan worden die herleidbaar is tot een persoon bij het bezoeken van een overheidswebsite.

Wij zullen daarom in kaart brengen waar third-party cookies en scripts gebruikt worden, en welke. Op basis daarvan willen we onderzoeken of we deze kunnen vervangen door (open source) alternatieven, die door de overheid zelf gehost worden, waardoor die informatie niet naar derden gaat. Dit sluit aan bij de ambities omtrent digital commons.¹⁶

Het artikel van Follow the Money over online tracking,¹⁷ naar aanleiding waarvan het debat op 17 mei gevoerd werd, wees ook op het gevaar van het volgen van ambtenaren. Het kabinet heeft al het beleid om apps uit landen met een offensief cyberprogramma te ontraden. Wij willen verder in gesprek met ICT-leveranciers binnen de overheid om te kijken of we het tracken van ambtenaren kunnen beperken.

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,
A.C. van Huffelen

De Minister van Economische Zaken en Klimaat,
M.A.M. Adriaansens

¹⁵ Aanhangsel Handelingen II 2022/23, nr. 534.

¹⁶ Kamerstuk 26 643, nr. 1057.

¹⁷ Je meest intieme data gaan naar de hoogste bidder, en dat kan een spion zijn – Follow the Money (ftm.nl).