

# Whois-data; domeinnamen, persoonsgegevens en de openbaarheid daarvan

42

## Trefwoorden:

domeinnamen, Whois-register, ICANN, openbaarheid

De kernvraag die in dit artikel wordt onderzocht is in hoeverre de persoonsgegevens van houders van domeinnamen openbaar en voor ieder raadpleegbaar mogen zijn in een Whois-register. Dit is een eis die Internet Corporation for Assigned Names and Numbers (ICANN) uit de VS oplegt aan Europese beheerders.

Achter internetdomeinnamen zitten persoonsgegevens van de domeinnaamhouder, een administratief contactpersoon en een technisch contactpersoon. De beheerders van de domeinnamen in de EU zijn van mening dat de persoonsgegevens die verwerkt worden bij het toekennen en beheer van domeinnamen maar beperkt openbaar mogen zijn in een 'layered access model'. In dit artikel wordt de werking van het beheer van domeinnamen uitgelegd, de eis van ICANN tot openbaarheid van gegevens wordt getoetst aan de vraag of dit in overeenstemming is met de AVG en aan het slot wordt de actuele stand van zaken en een oplossingsrichting gegeven.

## 1 Inleiding

De kernvraag is in hoeverre de persoonsgegevens van houders van domeinnamen openbaar en voor ieder raadpleegbaar mogen zijn in een Whois-register. Deze vraag vormt al 15 jaar een discussiepunt, maar door de komst van de AVG is er een urgentie om hier helderheid in te krijgen.

Achter internetdomeinnamen zitten persoonsgegevens van de domeinnaamhouder, een administratief contactpersoon en een technisch contactpersoon. De beheerders van de domeinnamen in de EU zijn van mening dat de persoonsgegevens die verwerkt worden bij het toekennen en beheer van domeinnamen maar beperkt openbaar mogen zijn. ICANN daarentegen stelt als (contractuele) eis dat die gegevens publiekelijk toegankelijk moeten zijn in een Whois-register.

In dit artikel leggen we de wereld achter het beheer van domeinnamen bloot; wie zijn hierbij de betrokken partijen, welke persoonsgegevens worden verwerkt, wat zijn de belangen en wie heeft hierover zeggenschap. De

eis van ICANN tot openbaarheid van gegevens wordt getoetst aan de vraag of dit in overeenstemming is met de AVG. Aan het slot wordt de actuele stand van zaken en een mogelijke oplossingsrichting gegeven.

Het is een betoog met een mondiaal perspectief en de vraagstelling is voor alle Europese beheerders van domeinnamen van belang, maar we beperken ons voornamelijk tot het Nederlandse perspectief. Er is veel tijd verstreken, er zijn veel partijen betrokken, rapporten verschenen en contracten van toepassing. In dit artikel wordt geprobeerd het verhaal zo veel mogelijk op hoofdlijnen te schetsen.<sup>1</sup>

Voordat de kernvraag wordt behandeld volgt eerst een korte uitleg over de oorsprong van de domeinnamen, de persoonsgegevens en de betrokken partijen die daarbij een rol spelen.

Voor de leesbaarheid is het aan te bevelen eerst kennis te nemen van de begrippen die in het kader zijn opgenomen.

## Definities

DNS: Domain Name System

TLD: top-level domain, bijvoorbeeld .com, .amsterdam, .frl

SLD: second-level domain; domeinnamen binnen een TLD; bijvoorbeeld sidn.nl of icann.org; dit is doorgaans wat men een domeinnaam noemt  
ccTLD's: country code top-level domains, uitsluitend gereserveerd voor landen en bestaat altijd uit twee letters, landcodes zoals .be, .nl, .de  
gTLD's: generic top-level domains, deze top-level domains kunnen door iedereen worden aangevraagd en worden uitgegeven door ICANN  
ICANN: Internet Corporation for Assigned Names and Numbers

Registry: beheerder van een top-level domain, zoals in Nederland SIDN en FRLregistry B.V.

Registrant: de domeinnaamhouder; persoon of organisatie op naam waarvan de domeinnaam is geregistreerd ('eigenaar' van de domeinnaam)

Registrar: partij die namens een domeinnaamhouder het contact met de registry onderhoudt en domeinnamen registreert

Whois: raadpleegbaar register met (persoons)gegevens van domeinnaamhouders

\* Corrie Ebbers is sinds 1997 werkzaam als privacyjurist en is redactiesecretaris van P&I. Jelte Jansen is als senior research engineer werkzaam bij SIDN en was tot 1 januari 2019 redactielid van P&I. De tekst van deze bijdrage is afgesloten op 1 maart 2019.

1 Zie ook het artikel van I.M. Wárlám 'Publiek toegankelijkheid WHOIS-gegevens van particuliere domeinnaamhouders', IR 2018, afl. 1 (<http://warlamlegal.nl/wp-content/uploads/2015/05/2018-01-TvI-ICANN-artikel.pdf>).

## 2 Domeinnamen, partijen en persoonsgegevens

De voorgeschiedenis van de domeinnamen begint in de jaren 80. Het internet was nog jong, maar er was behoefte aan een systeem om domeinnamen toe te wijzen. Op internet gebruiken systemen onderling nummers om elkaar te adresseren, maar om het voor mensen makkelijker te maken werd er al snel gebruikgemaakt van namen om de verschillende systemen aan te duiden. De koppeling tussen namen en IP-adressen werd gemaakt via een bestand ('hosts.txt') dat op elk systeem op het internet aanwezig was. Omdat er steeds meer adressen bijkwamen, werd het lastig om die lijst goed bij te houden en te distribueren. Als oplossing bedacht men het Domain Name System (DNS). Het DNS zorgt er nu voor dat een naam zoals uitgeverijparis.nl wordt omgezet in een IP-adres zoals 192.0.2.112.

Een systeembeheerder, Piet Beertema werkzaam bij het Centrum voor Wiskunde en Informatica (CWI) onderdeel van de Nederlandse organisatie voor Wetenschappelijk Onderzoek, had het idee om het .nl-top-leveldomein aan te vragen voor Nederland.<sup>2</sup> Dat deed hij bij Jon Postel, een Amerikaanse wetenschapper die een belangrijke rol heeft gespeeld in de ontwikkeling van de uitwisselingsstandaarden van het internet. De aanvraag werd goedgekeurd en .nl was een feit. Op 30 april 1986 registreerde het CWI de eerste .nl-domeinnaam: cwi.nl. Vanaf dat moment was .nl het eerste actieve landendomein buiten de VS.

### 2.1 De partijen: de registry's, de registrars en ICANN

Het internet en het aantal gebruikers groeide in de jaren 90 hard. Om te zorgen dat het registreren van domeinnamen goed verloopt, werden in diverse landen beheerders opgericht, registry's genaamd. In Nederland de Stichting Internet Domeinregistratie Nederland (SIDN). Op 31 januari 1996 werden de taken van het CWI door deze beheerder overgenomen.

In de beginjaren was het alleen voor in Nederland gevestigde bedrijven mogelijk om .nl-domeinnamen te registreren, maar sinds 2003 mag iedereen dit. Het maakt voor de registratie niet uit of het een bedrijf of een particulier betreft. En de aanvrager hoeft ook niet uit Nederland afkomstig te zijn want registreren kan in de hele wereld. Op een domeinnaam vestigt de domeinnaamhouder (registrant) een exclusief gebruiksrecht, voor een gering bedrag per jaar.

Vanaf 2003 groeide .nl explosief; in december 2018 zijn er meer dan 5,8 miljoen .nl-domeinnamen. Daarmee is .nl het zesde grootste landendomein ter wereld.<sup>3</sup> In 2014 is ook .frl erkend als top-leveldomain voor Friesland, deze wordt beheerd door FRLregistry B.V.<sup>4</sup>

In het jaar 1998 nam ICANN de taken over van Jon Postel. ICANN (Internet Corporation for Assigned Names and Numbers) is een non-profitorganisatie die een aantal internetgerelateerde taken uitvoert die men de IANA-functies noemt (Internet Assigned Numbers Authority), zoals het toekennen en specificeren van top-leveldomeinen.<sup>5</sup>

Aanvankelijk functioneerde ICANN onder toezicht van het Amerikaanse Ministerie van Handel, meer bepaald de National Telecommunications and Information Administration (NTIA), waarmee ICANN overeenkomsten had afgesloten. Op 1 oktober 2016 is ICANN verzelfstandigd en geprivatiseerd, althans voor het uitvoeren van de IANA-functies. Dit betekent dat de discussie nu met de 'hele' stakeholdergroep gevoerd wordt en niet meer alleen met ICANN.

Het beleid voor generic top-level domains wordt sindsdien bepaald door de generic Names Supporting Organization (gNSO), waarbij de gNSO de internetgemeenschap representeert volgens een multistakeholdermodel. Dit model moet ervoor zorgen dat ICANN verantwoording aflegt aan de globale internetgemeenschap die bestaat uit afgevaardigden van de privésector, technische experts, academici, vertegenwoordigers van de burgermaatschappij, overheden en individuele eindgebruikers.<sup>6</sup>

ICANN beheert zelf geen domeinnamen en persoonsgegevens. Dit laat men over aan andere organisaties, de registry's. De primaire taak van deze beheerders is om de veiligheid en de stabiliteit, flexibiliteit en veerkracht van de hoofd(key)-infrastructuur van internet met betrekking tot het gebruik van domeinnamen te waarborgen.<sup>7</sup>

Het beheer van een country code TLD (ccTLD) kent een grote variatie. Het gebeurt door de overheid of door een door de overheid aangewezen partij of door private partijen en stichtingen. Bij de ccTLD-domeinnamen hebben de beherende partijen doorgaans veel vrijheid en zeggenschap over de technische en organisatorische uitvoering van het domeinnaambeheer, terwijl het beleid voor de gTLD's wordt beheerst door de contractuele afspraken met ICANN.

De beheerders, ook wel registry's genoemd, in Nederland zijn onder andere SIDN (.nl) en de Friese FRLregistry B.V. (.frl). Bekende andere beheerders zijn Verisign (.com en .net) en DNS Belgium (.be).

De discussie die we hier schetsen betreft vooral de generic top-level domains, de gTLD's, en de contractuele eis van openbaarheid die ICANN stelt met betrekking tot het Whois-register. Omdat ccTLD's hun eigen beleid bepalen vormen deze in mindere mate onderwerp van discussie. De werking van de ccTLD's komt hier dan ook

<sup>2</sup> <https://godfatherof.nl>.

<sup>3</sup> [www.verisign.com/assets/domain-name-report-Q22018.pdf](http://www.verisign.com/assets/domain-name-report-Q22018.pdf).

<sup>4</sup> <https://nic.frl>.

<sup>5</sup> [www.icann.org/en/system/files/files/functions-basics-07apr14-en.pdf](http://www.icann.org/en/system/files/files/functions-basics-07apr14-en.pdf).

<sup>6</sup> <https://gnso.icann.org/en/about>.

<sup>7</sup> [www.verisign.com](http://www.verisign.com).

niet aan bod, behalve in de beschrijving van het ontstaan van het Whois-register en de beleidskeuzes daaromtrent.

Het gaat bij de discussie over de openbaarheid van het Whois-register over de persoonsgegevens van de gTLD's zoals .amsterdam en .frl. Deze generic top-level domains (gTLD's) kunnen door iedereen worden aangevraagd. gTLD's worden uitgegeven door ICANN. Hierbij worden door ICANN echter wel technische en organisatorische eisen gesteld waaraan een beheerder moet voldoen. Een van die eisen is de openbaarmaking in het zogenoemde Whois-register van persoonsgegevens van domeinnaamhouders. Een domeinnaamhouder is de persoon op wiens naam een domeinnaam is geregistreerd (de registrant).

Openbaarmaking is geen wens van ICANN zelf. ICANN is een rechtspersoon naar Californisch recht. De organisatie kent een board, maar die kan niet zelfstandig besluiten om het beleid met betrekking tot domeinregistraties te wijzigen. Het beleid wordt vastgesteld door de stakeholders binnen de gNSO. De board is in principe gehouden om het door de gNSO ontwikkelde beleid vast te stellen en uit te voeren. Van belang is vervolgens dat de gNSO alleen beleid kan maken voor de zogenaamde generieke domainnaamextensies (.com, .org, .amsterdam, enz.) en niet voor landencodes als .nl en .be. Die laatste bepalen zoals gezegd in principe hun eigen beleid. ICANN heeft daarin slechts zeer beperkt een rol. Binnen de gNSO worden beperkingen aan de openbaarheid van het Whois-register voornamelijk tegengehouden door partijen zoals de beschermers van intellectuele-eigendomsrechten, de security industrie en de opsporingsinstanties (de law-enforcement-kant) van de overheden.

## 2.2 De persoonsgegevens

Gegevens die noodzakelijk zijn voor het aanvragen en beheer van domeinnamen, bestaan uit contactgegevens van de domeinnaamhouder waaronder de naam, het adres, telefoonnummer en e-mailadres. Daarnaast contactgegevens van de administratieve en technische persoon, technische gegevens, duur van de registratie en contactinformatie in verband met misbruik van de domeinnaam.<sup>8</sup>

Volgens de overeenkomsten die ICANN aangaat met elk van haar geaccrediteerde organisaties, de registry's en registrars, wordt de eis gesteld dat de beheerders de verzamelde gegevens openbaar maken via de Whois-diensten van de betreffende registry.<sup>9</sup> Het gaat daarbij om de volgende domeinnaamdata: uniek identificatienummer van de domeinnaam, naam domeinnaamhouder, organisatie, adres, telefoonnummers, faxnummers,

e-mailadres. Ook worden alle contactgegevens van de administratieve en de technische contactpersonen vereist. De overeenkomst bepaalt verder dat de beheerders het gebruik van de Whois-gegevens toestaan voor 'wettelijke' doeleinden.<sup>10</sup>

## 2.3 Betrokkene en verwerkingsverantwoordelijke

Bij de aanvraag van een domeinnaam is de aanvrager, de domeinnaamhouder, in de contracten met ICANN 'registrant' genoemd, de betrokkene. Een betrokkene is een geïdentificeerde of identificeerbare natuurlijke persoon, degene van wie persoonsgegevens worden verwerkt. Deze persoon is verplicht zijn persoonsgegevens te verstrekken. De aanvrager van een domeinnaam kan ook een rechtspersoon zijn. Naast de aanvrager van de domeinnaam zijn ook de administratieve en technische contactpersonen als betrokkenen aan te merken.<sup>11</sup>

De vraag wie als verwerkingsverantwoordelijk voor de verwerking van de gegevens van domeinnaamhouders moet worden aangemerkt is minder eenvoudig te beantwoorden. Volgens sommigen zijn ICANN, de registry's en de registrar gezamenlijke verwerkingsverantwoordelijken.<sup>12</sup> ICANN stelt namelijk de randvoorwaarden van het beheer van domeinnamen en IP-nummers op en de registry's beheren de persoonsgegevens, beslissen over de verstrekking aan externe partijen en dragen zorg voor de openbaarheid in het Whois-register.<sup>13</sup>

Ook valt te verdedigen dat hier sprake is van afzonderlijke verwerkingsverantwoordelijken; dat er een zelfstandige verantwoordelijkheid bestaat voor elke partij. Er zijn vier actoren te onderscheiden. Voor de onderlinge relatie van deze actoren zie het schema boven aan p. 52.

Als we de rollen hierboven bekijken dan blijkt dat ICANN geen juridische relatie heeft met de betrokkene, niet zelf persoonsgegevens verwerkt en ook geen zeggenschap heeft over de gegevens. ICANN wijst extensies toe, bepaalt het beleid en stelt contractuele eisen, maar het toekennen van een domeinnaam aan een domeinnaamhouder gebeurt door een andere partij, door de registry (zie nummer 3 in het schema). De registry beslist wie toegang krijgt tot de gegevens en ook het openbaar maken van persoonsgegevens in een Whois-register ligt primair bij de registry's. Kan ICANN dan toch verwerkingsverantwoordelijke zijn?

De Autoriteit Persoonsgegevens is van mening dat voor het publiceren van Whois-gegevens, ICANN en de beheerders aan te merken zijn als gezamenlijke verwerkingsverantwoordelijken.<sup>14</sup>

<sup>8</sup> [www.sidn.nl/a/nl-domeinnaam/sidn-en-privacy](http://www.sidn.nl/a/nl-domeinnaam/sidn-en-privacy).

<sup>9</sup> Voor de registrars de 2013 Registrar Accreditation Agreement (de 2013 RAA), en voor de registry's de Registry Agreement, vindplaats: <https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-09jan14-en.htm>.

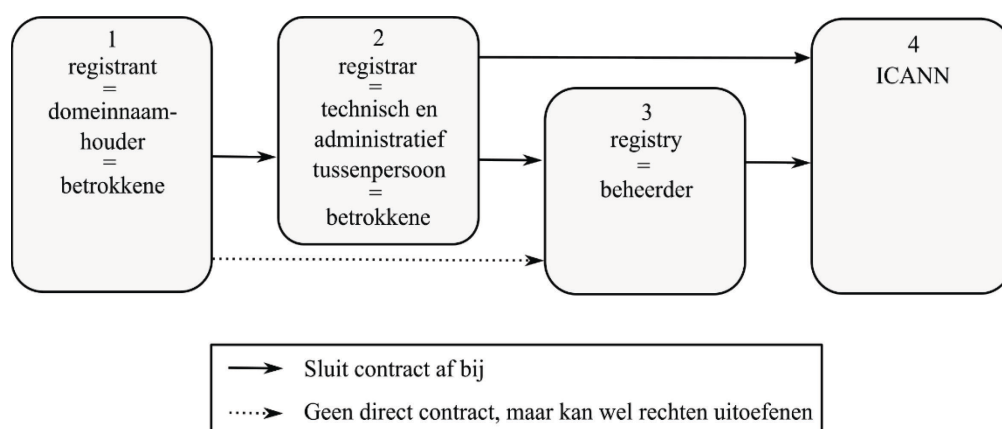
<sup>10</sup> <https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-09jan14-en.htm>.

<sup>11</sup> In een Duitse rechtszaak eist ICANN de gegevens van de administratie en technische contacten, zie [www.natlawreview.com/article/german-court-issues-first-gdpr-ruling](http://www.natlawreview.com/article/german-court-issues-first-gdpr-ruling).

<sup>12</sup> Hamilton Memorandum 16 oktober 2017, p. 20.

<sup>13</sup> Gegevens en ontvangers [www.sidn.nl/a/nl-domeinnaam/sidn-en-privacy](http://www.sidn.nl/a/nl-domeinnaam/sidn-en-privacy).

<sup>14</sup> AP in brief aan FRLregistry B.V. van 26 oktober 2017.



De vraag wie als verwerkingsverantwoordelijke moet worden aangemerkt is een fundamentele vraag die hier niet wordt uitgewerkt maar wel nader onderzoek verdient. De verwerkingsverantwoordelijke heeft immers zeggenschap over de persoonsgegevens, bepaalt het doel en de middelen van de gegevensverwerking en heeft dus ook zeggenschap over de werking van het Whois-register.

Voordat het twistpunt tussen ICANN en de registry's wordt uitgewerkt wordt eerst de werking van het Whois-register toegelicht.

### 3 De werking van Whois

Voor de aanvraag van een domeinnaam, het beheer en de administratie worden dus gegevens van verschillende partijen verwerkt. Dit zijn niet altijd persoonsgegevens waar de AVG op van toepassing is zoals gegevens van de technische uitvoering van de registratie, of de niet-natuurlijke personen zoals rechtspersonen. In par. 6 komt dit onderwerp nog even terug.

Naarmate meer individuen hun eigen domeinnaam gingen registreren namen ook de klachten toe uit diverse landen maar ook bij ICANN was het gaan borrelen.<sup>15</sup> Zo heeft de beheerder (registry) in Nederland, SIDN, in 2010 maatregelen genomen en de toegang die internetters over .nl-domeinen kunnen opvragen ingeperkt. De wens tot beperking van de hoeveelheid beschikbare informatie, was een van de uitkomsten van het Domeinnaamdebat 2008.<sup>16</sup>

#### 3.1 Het beheer van het Whois-register

Het Whois-register is de (semi)publieke kant van de database van domeinregistraties. Het bevat gegevens over degenen die domeinnamen hebben geregistreerd, hoe deze domeinnaam op het internet te vinden is en de contactgegevens van administratieve en technische personen. ICANN eist dat dit register bij gTLD's openbaar is, inclusief namen en contactgegevens zoals telefoonnummers en e-mailadressen.<sup>17</sup>

Hoewel het Whois-beleid van ccTLD's niet het onderwerp van discussie is – omdat ccTLD's doorgaans hun eigen beleid bepalen – schetsen we in deze paragraaf het beleid voor de ccTLD '.nl', dat in de loop der tijd in overleg met de Nederlandse registrars, de Nederlandse internetgemeenschap en op basis van Nederlandse wetgeving (de Wbp) is gevormd. Dit biedt een basis voor de discussie van het beleid bij gTLD's.

De Whois-database van een TLD wordt beheerd door de registry van die TLD. Voor .nl is dat SIDN. De informatie in het Whois-register wordt door SIDN beschikbaar gesteld via haar website en mag gebruikt worden om technische problemen met betrekking tot de werking van het internet te kunnen oplossen en om administratieve zaken af te handelen, zoals het verhuizen van een domeinnaam naar een nieuwe registrar of nieuwe houder. Ook mag de informatie gebruikt worden om intellectuele-eigendomsrechten te beschermen en om illegale en schadelijke inhoud op het internet te voorkomen en te bestrijden.

De toegang tot die informatie is beperkt tot een aantal bevragingen per dag en automatische bulkverwerking is niet toegestaan. Als men voor andere doeleinden de informatie wil gebruiken dan is eerst toestemming van SIDN nodig (dat is een argument om SIDN als verwerkingsverantwoordelijke aan te merken).

Er wordt wat betreft openbaarmaking van contactgegevens onderscheid gemaakt tussen zakelijke en particuliere domeinnaamhouders (individuele natuurlijke personen). Van particuliere domeinnaamhouders is een aantal gegevens niet zichtbaar in het Whois-register, zoals de naam, het adres en het telefoonnummer. Gegevens van zakelijke houders worden wel openbaar gemaakt, tenzij de houder een opt-outverzoek indient.<sup>18</sup>

In Nederland zijn er drie groepen die, buiten de hierboven beschreven publieke Whois om, extra gegevens kunnen opvragen:

- iedereen die er belang bij heeft, een 'belanghebbende'; het opvragen van gegevens als belanghebbende

15 [www.domjur.nl/fileadmin/user\\_upload/publicaties/rapportdomeinnaamdebat2006.pdf](http://www.domjur.nl/fileadmin/user_upload/publicaties/rapportdomeinnaamdebat2006.pdf) en [www.icann.org/news/announcement-2009-09-28-en](http://www.icann.org/news/announcement-2009-09-28-en).

16 [www.opennieuwsbank.nl/bericht/2009/01/14/1077-stichting-internet-domeinregistratie-nederland.html](http://www.opennieuwsbank.nl/bericht/2009/01/14/1077-stichting-internet-domeinregistratie-nederland.html).

17 AP-uitspraak z2017-07686 van 28 augustus 2017 (FRLregistry B.V.).

18 [www.sidn.nl/a/over-sidn/gebruikersvoorwaarden-whois](http://www.sidn.nl/a/over-sidn/gebruikersvoorwaarden-whois).

moet door middel van een in te vullen formulier, waarbij het belang en de reden van de opvraging opgegeven moeten worden;

- opsporings- en handhavingsautoriteiten;
- Certification Authorities (CA's), dat zijn bedrijven die Transport Layer Security-certificaten (TLS) uitgeven aan de houders van domeinnamen. Zij controleren altijd bij de uitgifte van een TLS-certificaat of de gegevens kloppen met de gegevens die zijn geregistreerd bij de registry in Nederland, SIDN of FRL-registry B.V.

Samengevat is er voor .nl dus een gelaagd model: alleen een beperkte set gegevens is volledig openbaar, en, afhankelijk van noodzaak of regelgeving, zijn extra gegevens beschikbaar voor specifieke partijen.

Een volledige beschrijving van het beleid is te vinden op de website van SIDN.<sup>19</sup>

Deze werkwijze is vanuit de praktijk gegroeid. Het is wereldwijd gebruikelijk dat op dergelijke wijze bepaalde gegevens van een domeinnaam opgevraagd kunnen worden.

De houder van de domeinnaam kan bezwaar maken tegen deze openbaarmaking en een opt-outverzoek indienen. Aan dat verzoek wordt voldaan als anonimiteit echt nodig is én als dat niet op een andere manier is te regelen.

Een aantal contactgegevens is niet zichtbaar in de Whois zoals de naam van de particuliere domeinnaamhouder (individuele natuurlijke personen), het adres van domeinnaamhouder, de naam, het adres en telefoonnummer van de administratief contactpersoon voor de domeinnaam en naam, adres en telefoonnummer van de technisch contactpersoon voor de domeinnaam.<sup>20</sup>

#### 4 Wat is het twistpunt tussen partijen?

De discussie over de openbaarmaking van persoonsgegevens in het Whois-register speelt dus met name tussen enerzijds de beheerders, de registry's, die persoonsgegevens verwerken waarbij ze gebonden zijn aan de AVG en anderzijds ICANN die gevestigd is in de VS en waarvan het beleid nu bepaald wordt door de gNSO. Hierbij is de rol van de registry als integer beheerder in het geding en onder de dreiging van zeer hoge boetes die sinds de invoering van de AVG kunnen worden opgelegd, is de weerstand tegen de volledige openbaarmaking van de gegevens zoals ICANN wenst, toegenomen en is de discussie aangescherpt.

Oorspronkelijk was het doel van het ter beschikking stellen van persoonsgegevens, dat technici contact op kunnen nemen met eigenaren van websites om technische storingen op te lossen en voor allerlei administratieve taken zoals bijvoorbeeld het beheren van de domeinnamen. In de loop der tijd, met de groei van het aantal

domeinnamen, is er gaandeweg een systeem ontstaan waarbij een set gegevens publiekelijk gedeeld wordt, zonder dat de doelen daar nu heel helder voor zijn vastgelegd. Men is de data in de loop der jaren voor uiteenlopende doeleinden gaan gebruiken.

Naast de noodzaak om technische storingen op te lossen en een juiste administratie te voeren, worden gegevens verwerkt:

- om voor zakelijke doeleinden de houder van een domein te identificeren, bijvoorbeeld in verband met een aankoop van de domeinnaam of andere transacties;
- voor facturering, ondersteuning en andere administratieve acties met betrekking tot geregistreerde domeinnamen;
- om fraude, misleiding van consumenten, schendingen van intellectuele eigendommen of andere schendingen van de wet te onderzoeken;
- om de identiteit van een aanbieder van goederen of diensten op internet te verifiëren, inclusief voor consumentenbeschermingsdoeleinden.<sup>21</sup>

ICANN eist nu dat registry en registrars een Whois-register beschikbaar stellen, doorzoekbaar op domeinnaam, waarna de bijbehorende gegevens getoond worden: naam registrant, adres, telefoonnummer en e-mailadres.

Voor registrars geldt dat het niet naleven van de ICANN-eis kan leiden tot de intrekking van de accreditatie door ICANN, waardoor de registrar de mogelijkheid, c.q. bevoegdheid, verliest om domeinnamen te registreren. Dit was in 2018 een dreigement van ICANN in een Duitse rechtszaak.<sup>22</sup>

ICANN onderkent het dilemma van volledige openbaarmaking dat de Europese wetgeving oproept en heeft advies ingewonnen bij het Zweedse advocatenkantoor Hamilton. Voordat dit advies en de reactie van ICANN daarop wordt besproken volgt hier eerst de opvatting van de Artikel 29-werkgroep en de Autoriteit Persoonsgegevens.

##### 4.1 De zienswijze van de Artikel 29-werkgroep en de Autoriteit Persoonsgegevens

Zoals gezegd speelt de discussie over de openbaarheid van gegevens van domeinnaamhouders al lang. In 2003 heeft de Artikel 29-werkgroep al een standpunt bepaald met betrekking tot het Whois-register.<sup>23</sup> In dit advies worden aan ICANN richtlijnen aangereikt voor het beheer van het Whois-register en andere openbare registers met domeinnamen en IP-adressen. De Artikel 29-werkgroep constateert dat publicatie van de identiteits- en contactinformatie, zonder toestemming van betrokkene, in strijd is met de wet en daarmee onrechtmatig. Er is namelijk geen rechtmatige grondslag die rechtvaardigt

<sup>19</sup> [www.sidn.nl/a/nl-domeinnaam/sidn-en-privacy/](http://www.sidn.nl/a/nl-domeinnaam/sidn-en-privacy/).

<sup>20</sup> [www.sidn.nl/a/nl-domeinnaam/uitleg-whois](http://www.sidn.nl/a/nl-domeinnaam/uitleg-whois).

<sup>21</sup> Hamilton Memorandum 16 oktober 2017.

<sup>22</sup> [www.natlawreview.com/article/german-court-issues-first-gdpr-ruling](http://www.natlawreview.com/article/german-court-issues-first-gdpr-ruling).

<sup>23</sup> [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp76\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp76_en.pdf).

digd dat openbaarmaking van gegevens verplicht gesteld kan worden. Publicatie van persoonsgegevens van individuen zoals adres en telefoonnummer, is in strijd met het recht van het individu om zelf te bepalen of gegevens worden opgenomen in een openbaar register en in welk register. De Artikel 29-werkgroep voegt daaraan toe dat de verwerking van data in reverse registers of in zoekmachines, die het mogelijk maken te zoeken op meerdere criteria, zonder de ondubbelzinnige toestemming van het individu, ook onrechtmatig is. In het rapport wordt ICANN opgeroepen om privacyvriendelijke manieren te ontwikkelen om de registers te beheren, in lijn met de rechten van de betrokkene en met de oorspronkelijk vastgestelde doeleinden. Het moet te allen tijde mogelijk zijn voor individuen om een domeinnaam te registreren zonder dat persoonlijke gegevens in een publiek register verschijnen.

Dit standpunt wordt herhaald in 2017; de Artikel 29-werkgroep erkent dat verwerking van gegevens gerechtvaardigd is (legitimate purpose) als ze gebruikt worden voor support (onderhouds)doeleinden, maar dat openbaarmaking daarmee onverenigbaar is. Er is dus nog steeds geen rechtmatige grondslag aan te wijzen voor een publiekelijk toegankelijk register (public access).<sup>24</sup>

Ook de Duitse rechter en de Autoriteit Persoonsgegevens stellen zich op het standpunt dat er geen rechtmatige grondslag is voor het openbaar maken van gegevens omdat niet aan de noodzakelijkheidseis wordt voldaan want het doel kan ook op andere wijze worden bereikt en bovendien zou volledige openbaarmaking van alle persoonsgegevens bovenmatig zijn.<sup>25</sup>

#### 4.2 De ICANN-eis

De monopoliepositie van ICANN met betrekking tot de toewijzing van de gTLD's vormt in deze discussie een extra complicatie. ICANN heeft namelijk rechtstreekse controle over de gTLD's zelf, of ze bijvoorbeeld de TLD .gratisgeld uitgeven of niet.<sup>26</sup>

In juli 2017 heeft ICANN de beheerders van de domeinnamen verplicht om voor het openbaar maken van de gegevens toestemming te vragen aan de domeinnaamhouders. Door de overeenkomst tussen ICANN en de beheerders eenzijdig met deze verplichting aan te vullen, zijn de verhoudingen op scherp gezet. Juridisch gezien is dit een onmogelijk eis. Van enige 'in vrijheid gegeven toestemming' is in dit geval natuurlijk geen sprake. Zoals ook de AP in haar advies aangaf; het geven van toestemming is verbonden aan het verwerven van een domeinnaam, hierdoor is geen sprake van een vrije wilsuiting zoals artikel 7 AVG als eis voorschrijft.

Dus toestemming kan geen rechtmatige grondslag vormen voor het openbaar maken van de gegevens. Het navolgen van deze eis van ICANN in het contract zou in

strijd zijn met AVG en tot hoge boetes voor de beheerders kunnen leiden.

Met het oog op de inwerkingtreding van de AVG heeft ICANN aan advocatenkantoor Hamilton (Zweden) gevraagd een advies op te stellen met betrekking tot de vraag wat de gevolgen zijn van de nieuwe regelgeving in relatie tot het ter beschikking stellen van de persoonsgegevens van de generieke top-level domeinnamen (gTLD's) in het Whois-register, als openbaar register (public directories).

In de volgende paragraaf wordt dit advies kort besproken.

#### 4.3 Hamilton-advies

Het Hamilton-advies werkt het openbaar maken van gegevens in het Whois-register uit en komt tot de volgende bevindingen:<sup>27</sup>

'Op basis van het huidige gebruik van de Whois-gegevens worden persoonsgegevens verwerkt binnen de Whois-diensten door de volgende partijen en voor de volgende doeleinden:

(i) door beheerders (registrars) en netwerkexploitanten, voor facturering, ondersteuning en andere administratieve acties met betrekking tot geregistreerde domeinnamen.

(ii) voor het beschermen van de rechten van domeinnaam-eigenaren, bijvoorbeeld door het bewaren van de gegevens in escrow met escrow-agenten, voor herstel in het geval van bijv. een noodlijdende registrar of registry of nalaten van een registrar of registry om zijn verplichtingen na te komen.

(iii) door handhavingsinstanties voor het onderzoeken en bestrijden van ernstige criminaliteit, terrorisme, fraude, misleiding van consumenten, inbreuken op intellectuele eigendommen of andere schendingen van de wet.

(iv) door houders van intellectuele-eigendomsrechten om inbreuken op intellectuele-eigendomsrechten te onderzoeken.

(v) door het grote publiek om de identiteit van een aanbieder van goederen of diensten op internet te verifiëren, ook voor consumentenbescherming.

(vi) om de eigenaar van een domein voor zakelijke doeleinden te identificeren, bijvoorbeeld in verband met een aankoop van de domeinnaam of andere transacties.'

De bovenstaande lijst is niet volledig en ook de rechtmatige grondslagen van de verwerking zijn in dit advies niet uitgewerkt. De Hamilton-advocaten adviseren om naar de Whois-diensten te kijken vanuit het oogpunt van gegevensverwerking:

<sup>24</sup> Artikel 29-werkgroep 6 december 2017.

<sup>25</sup> AP eind 2017: de kwestie werd in Nederland aangeslingerd door FRLregistry B.V. en door hen aan de AP voorgelegd (uitspraak z2017-07686).

<sup>26</sup> Zie ook brief AP 26 oktober 2017, over uitspraak z2017-07686.

<sup>27</sup> Advies Hamilton 21 december 2017, Draft 3.

‘Als een legitiem doel en een rechtsgrond kunnen worden aangewezen, moet de verwerking altijd voldoen aan de algemene beginselen voor verwerking zoals uiteengezet in artikel 5 AVG. Dit betekent dat, onder andere, in aanmerking moet worden genomen het principe van doelbinding, dataminimalisatie en rolbased-access d.w.z. alleen de partijen die de gegevens voor het vastgestelde doel moeten verwerken, hebben toegang tot die gegevens. Daarnaast moet bij het bepalen van de doelstellingen en het beoordelen van de mogelijke juridische grond voor verschillende verwerkingsactiviteiten de volgende vragen nog beantwoord worden:

- Welke Whois-gegevens zijn noodzakelijk om het specifieke doel te bereiken?
- Welke partijen moeten toegang hebben tot de Whois-gegevens voor het specifieke doel?
- Moeten de Whois-gegevens openbaar zijn voor het specifieke doel?

In het licht van het bovenstaande is de inschatting van de adviseurs dat de gegevens die moeten worden verwerkt voor administratieve acties, de eerste doelstelling, waarschijnlijk vrij uitgebreid zijn, waarbij de registrars bijvoorbeeld contactgegevens moeten verwerken en registraties moeten meer technische gegevens verwerken, zoals IP-adressen. Maar de toegang tot de gegevens moet worden beperkt tot de partijen die het echt nodig hebben in het licht van het relevante doel. Diezelfde gegevens kunnen niet worden gebruikt voor publicatie in openbare registers zoals Whois.

In het advies wordt ook een oplossingsrichting voorgesteld die logisch uit het voorgaande voortvloeit; layered access, gelaagde toegang.

‘De beste mogelijkheid om de Whois-diensten te kunnen blijven aanbieden en te blijven voldoet aan de AVG is een interim-oplossing gebaseerd op een gelaagd toegangsmodel dat zorgt voor verdere verwerking van Whois-gegevens voor een beperkt aantal doeleinden. Daarvoor is het nodig om de exacte doelen en mechanismen voor een dergelijk model grondig in beeld te brengen. Een gelaagd toegangsmodel kan het gebruik van Whois-gegevens veiligstellen voor beheer en noodherstel, waardoor de meest elementaire functies van het gTLD-systeem kunnen blijven functioneren. Een extra functie toevoegen zou kunnen voorzien in het voortgezette gebruik van Whois-gegevens voor wetshandavingsdoeleinden (naast de wetshandhaving die al is voorzien in de nationale EU-wetgeving van de EU). Dit is een mogelijke en werkbare tijdelijke oplossing. Een werkbaar langetermijnmodel kan ondertussen worden onderzocht om het gebruik voor andere doeleinden mogelijk te maken.’<sup>28</sup>

Het is niet duidelijk of in het advies bedoeld wordt om de Whois-gegevens rechtstreeks toegankelijk te maken voor opsporingsinstanties. Ook blijft in het midden wat

de adviseurs voor ogen hebben als ze spreken over het gebruik van Whois-gegevens voor ‘andere doeleinden’ in het langetermijnmodel.

#### 4.4 *The Cookbook van ICANN*

Na het Hamilton-rapport kwam ICANN in maart 2018 met een eigen voorstel; het Interim Compliance Model kortweg Cookbook genaamd.<sup>29</sup> Het Interim Compliance Model vertegenwoordigt ICANN’s analyse van wat ICANN zou vereisen voor naleving van het ICANN-beleid en voor de overeenkomsten met registry’s en registrars.

Het model stelt eveneens een gelaagde toegang voor tot Whois-gegevens. Dit is een verschuiving van het huidige Whois-systeem. Deze functie is ingebed in het model op basis van de voorgaande juridische analyses van het Hamilton-advocatenkantoor en de feedback van de Artikel 29-werkgroep.<sup>30</sup>

Maar de uitwerking van het interim-model door ICANN leidt niet tot een beter inzicht in de rechtmatige grondslagen. Integendeel. Er worden wel doelstellingen zoals ‘ter identificatie’ en ‘contact onderhouden’ genoemd en daarbij de rechtmatige grondslagen uit de AVG, zonder dat duidelijk is wie de betrokkene of verantwoordelijke is. Het verwerken van persoonsgegevens om ‘contact te onderhouden’ is echter een weinig concreet doel; het is een middel om een doel te bereiken. In het Cookbook lijkt de eis van ICANN door te klinken dat het *bewaren* van gegevens voor ICANN een hoofddoel van de gegevensverwerking is. Dat de gegevens als een publiek ‘goed’ gezien moeten worden dat voor iedereen toegankelijk moet zijn.

#### 5 **Tijdelijke oplossing: Temporary Specification for gTLD Registration Data**

In navolging van het advies en de discussies met de stakeholders heeft ICANN in mei 2018 een tijdelijk beleid aangenomen in de vorm van de ‘Temporary Specification for gTLD Registration Data’.<sup>31</sup>

In deze specificatie worden (tijdelijke) eisen en maatregelen opgesteld waar registry’s en registrars aan moeten voldoen op het gebied van Whois- en andere registratiegegevens. De basis van deze oplossing is een ‘layered access model’, waarbij het wel mogelijk moet zijn voor partijen om, met een legitiem doel, gegevens te raadplegen zonder dat de gegevens gepubliceerd en daarmee openbaar worden.

De Whois-gegevens moeten nog wel verzameld en opgeslagen worden, maar niet alle gegevens hoeven van ICANN meer publiek beschikbaar gesteld te worden, tenzij er door de betrokkene expliciet toestemming is gegeven. Het gaat hierbij om de volgende gegevens van de domeinnaamhouder:

- identificatiecode;

<sup>28</sup> Hamilton-advies 21 december 2017, § 3.2.

<sup>29</sup> [www.icann.org/en/system/files/files/gdpr-compliance-interim-model-08mar18-en.pdf](http://www.icann.org/en/system/files/files/gdpr-compliance-interim-model-08mar18-en.pdf).

<sup>30</sup> Cookbook § 6.6. en 6.7.

<sup>31</sup> [www.icann.org/resources/pages/gtld-registration-data-specs-en](http://www.icann.org/resources/pages/gtld-registration-data-specs-en).

- naam- en adresgegevens;
- telefoonnummer(s);
- e-mailadressen.

De registrar moet daarbij de mogelijkheid bieden om contact met een domeinnaamhouder op te nemen via bijvoorbeeld een webformulier, zonder dat daarbij de houdergegevens bekend worden gemaakt.

De registry's en registrars moeten daarnaast zorgen voor een 'redelijke toegang' tot gegevens voor derde partijen met een legitiem doel. Daarbij wordt verwezen naar de grondslag 'gerechtvaardigd belang' van artikel 6 lid 1 onderdeel f AVG. Ook moet toegang verleend worden aan derde partijen wanneer de EDPB een bevoegde toezichthoudende autoriteit of een rechtbank in een relevante jurisdictie betreffende de AVG besluit dat deze toegang wettelijk gerechtvaardigd is.<sup>32</sup>

Met het van toepassing worden van de AVG heeft het Europees Comité voor gegevensbescherming tijdens de eerste plenaire vergadering op 25 mei 2018 de verklaring van de Artikel 29-werkgroep over ICANN en het Whois-register bekrachtigd.<sup>33</sup> En op 5 juli 2018 nam de EDPB een brief aan namens de EDPB-voorzitter gericht aan ICANN, die richtlijnen biedt om ICANN in staat te stellen een AVG-compatibel model te ontwikkelen voor toegang tot persoonsgegevens die in de context van Whois worden verwerkt. De brief behandelt de kwesties van doel-specificatie, verzameling van 'volledige Whois-gegevens', registratie van rechtspersonen, logging van toegang tot niet-openbare Whois-gegevens, gegevensbewaring en gedragscodes en accreditatie. De EDPB verwacht van ICANN dat zij een Whois-model ontwikkelt en implementeert dat legitiem gebruik door relevante belanghebbenden, zoals wetshandhavers, in overeenstemming met de AVG mogelijk maakt, zonder dat dit leidt tot een onbeperkte publicatie van die gegevens.<sup>34</sup>

## 6 Oplossingsrichting

Gezien het Hamilton-advies zou een logische vervolgstap zijn om een beschrijving te maken van alle zes door Hamilton vermelde doeleinden. De diverse doeleinden zijn helder:

- facturering met betrekking tot domeinnamen;
- beschermen van de rechten van domeinnaameigenaren;
- verstrekking aan handhavingsinstanties;
- bewaken van intellectuele-eigendomsrechten;
- ter consumentenbescherming de identiteit verifiëren van een aanbieder;
- identificeren van de eigenaar van een domein voor zakelijke doeleinden.

Vervolgens kan bij elk doel getoetst worden of sprake is van het verwerken van persoonsgegevens waar de AVG

op van toepassing is. Daarvoor is het nodig bij elk doel te vermelden wie de betrokkene en wie de verantwoordelijke is. Vervolgens kunnen de categorieën persoonsgegevens beschreven worden die voor elk afzonderlijk doel noodzakelijk zijn en kunnen de bewaartermijnen worden vastgesteld.

Als sprake is van het verwerken van persoonsgegevens waar de AVG op van toepassing is, dan kan de rechtmatige grondslag worden aangewezen, wie toegang mag hebben tot die gegevens en de wijze waarop die gegevens worden verstrekt. Als voorbeeld kan dienen de werkwijze zoals die sinds 2010 door SIDN als staand beleid is opgesteld.

Misschien zijn niet altijd persoonsgegevens noodzakelijk om de gestelde doeleinden te bereiken en is een algemeen contactadres voldoende zoals `admin@naambedrijf.nl` zoals ook het EDPB voorstelt.

En als wel sprake is van persoonsgegevens is mogelijk ook nog een andere wet van toepassing. Zoals bij het bewaken van intellectuele-eigendomsrechten waaronder het Merkenrecht of de Handelsnaamwet.

In enkele gevallen is sprake van het verwerken van gegevens van rechtspersonen zoals bij het onder v en vi genoemde doel. Gegevens van rechtspersonen vallen niet onder de beschermende werking van de AVG. De AVG regelt alleen de verwerking van persoonsgegevens van natuurlijke personen (artikel 4 AVG).

Als gegevens van zzp'ers als domeinnaamhouders of contactpersonen van de rechtspersonen nodig zijn, dan is een mogelijke oplossing om aan te sluiten bij het regime van de openbaarheidsbepalingen zoals we die nu ook al kennen van de openbare registers zoals het Handelsregister. De namen van bestuurders en vertegenwoordigers van rechtspersonen zoals die staan ingeschreven in het handelsregister zijn weliswaar persoonsgegevens maar de verwerking ervan valt in Nederland onder het regime van de Handelsregisterwet. De persoonsgegevens behoren tot de openbare registers welke een openbaar belang dienen. Ook de persoonsgegevens van zzp'ers vallen onder de openbaarheidsbepalingen van het Handelsregister. Daarbij is de openbaarheid wel enigszins beperkt; de informatie is opvraagbaar maar selecties en geautomatiseerde bulkverwerking van persoonsgegevens is niet toegestaan.<sup>35</sup>

Zo kan het Whois-register op dezelfde wijze als het Handelsregister juridisch vormgegeven worden, wellicht op EU-niveau met een instantie die het centraal beheert.

## 7 Conclusie

Zoals de naam al aangeeft is het Temporary Specification-beleid van ICANN van tijdelijke aard; het vervalt in mei 2019. Als er dan geen definitief vervangend beleid is, valt men terug op bestaande contracten met daarin de eisen zoals 'toestemming' voor openbaarmaking van de

<sup>32</sup> [www.icann.org/resources/pages/gtld-registration-data-specs-en](https://www.icann.org/resources/pages/gtld-registration-data-specs-en).

<sup>33</sup> [https://edpb.europa.eu/news/news/2018/european-data-protection-board-endorsed-statement-wp29-icannwhois\\_en](https://edpb.europa.eu/news/news/2018/european-data-protection-board-endorsed-statement-wp29-icannwhois_en).

<sup>34</sup> [https://edpb.europa.eu/news/news/2018/letter-icann\\_en](https://edpb.europa.eu/news/news/2018/letter-icann_en).

<sup>35</sup> Artikel 21 e.v. Handelsregisterwet.

houder van de domeinnaam. Maar dan blijft het dilemma dat de registry's geen geldige toestemming kunnen verkrijgen. Immers, de domeinnaamhouders moeten onder dwang toestemming geven, anders kunnen zij geen domeinnaam registreren. De registry's zitten daarmee klem zowel contractueel tegenover ICANN als op grond van de AVG. ICANN kan de toestemming niet afdwingen.

Het mag opmerkelijk genoemd worden dat niet helder is wie als verwerkingsverantwoordelijke moeten worden aangemerkt. Zelfs op een bijeenkomst die door ICANN zelf is geïnitieerd, kon door ICANN en de aanwezige panelleden geen eenduidig antwoord op die vraag gegeven worden.<sup>36</sup>

Als het noodzakelijk is een openbaar register van domeinhouders in het leven te roepen dan kan het Whois-register wellicht worden vormgegeven op dezelfde wijze als andere openbare registers zoals het Handelsregister, met een gelaagde toegang, met de registry's en registrars als verwerkingsverantwoordelijken en eventueel een centrale verwerker op Europees niveau.

Vanwege de langdurige en omvangrijke discussie en de verschillende belangen van de diverse stakeholders, wordt deze casus wel gezien als de grote testcase van het nieuwe model van ICANN. Als er op korte termijn geen definitieve oplossing gevonden wordt, zullen veel partijen dit zien als het falen van het oorspronkelijke multistakeholdermodel van ICANN.

---

<sup>36</sup> Computers, Privacy en Data Protection conference 1 februari 2019, panel 'Ensuring domain name data is safe: the Whois experience (...)' zie: [www.cpdconferences.org/panels/friday-1-february-grid](http://www.cpdconferences.org/panels/friday-1-february-grid).