CONSULTATIEREACTIE VBNL BIJ VOORSTEL IMPLEMENTATIEWET DAC8

Datum: 20 november 2024

1. Inleiding

De Verenigde Bitcoinbedrijven Nederland (VBNL) is de Nederlandse branchevereniging van aanbieders van cryptoactivadiensten.

De VBNL heeft kennisgenomen van het conceptwetsvoorstel voor de Wet implementatie EU-richtlijn gegevensuitwisseling cryptoactiva. Dit voorstel ziet op implementatie van Richtlijn (EU) 2023/2226 (DAC8). Op basis van het voorstel zullen aanbieders van cryptoactivadiensten vanaf 1 januari 2026 worden verplicht om jaarlijks te rapporteren over hun gebruikers aan de Belastingdienst.

De VBNL maakt graag gebruik van de gelegenheid om een consultatiereactie te geven op het voorstel. Het voorstel zal naar verwachting grote impact hebben op de leden van de VBNL en hun cliënten. De leden van de VBNL zullen worden geconfronteerd met een verstrekkende rapportageverplichting ten aanzien van hun cliënten, hetgeen grote operationele inspanningen zal vergen en tot hoge lasten zal leiden. De cliënten van de leden van de VBNL zullen worden geconfronteerd met een ingrijpende inbreuk op hun privacy. De VBNL trekt zich dit laatste ook specifiek aan: de leden van de VBNL wensen te voldoen aan de relevante fiscale regelgeving, maar tegelijkertijd dienen zij ook de waarborgen in acht te nemen op basis van (onder meer) de Algemene Verordening Gegevensbescherming. Dat plaatst hen in een lastige positie.

2. Algemeen

De VBNL is zich ervan bewust dat de EU-richtlijn (DAC8) reeds – door de Europese regelgever – is aangenomen. De Europese lidstaten dienen de richtlijn uiterlijk 31 december 2025 te implementeren in de nationale regelgeving. Ten aanzien van een aantal verplichtingen geldt een latere implementatietermijn, te weten 1 januari 2028 en 1 januari 2030. Deze verplichtingen zullen in latere wetsvoorstellen worden behandeld.

In de concept Memorie van Toelichting wordt herhaaldelijk verwezen naar DAC8 en de keuzes die in dat verband zijn gemaakt door de Europese wetgever. Dat neemt niet weg dat van de Nederlandse wetgever een kritische en objectieve opstelling mag worden verwacht, met voldoende aandacht voor Nederlandse stakeholders. Het is van groot belang dat binnen de Europese Unie sprake is van een *level playing field* en dat de concurrentiepositie van Nederlandse aanbieders van cryptodiensten niet onnodig wordt benadeeld.

Binnenkort zal de Europese Verordening betreffende de cryptoactivamarkten (MiCAR) van toepassing worden. Deze Verordening beoogt gelijke regelgeving te introduceren voor aanbieders van cryptoactivadiensten binnen de Europese Unie. DAC8 is een richtlijn en niet een verordening. Dat betekent dat nationale divergenties kunnen ontstaan. Voorkomen moet worden dat (i) de Nederlandse wetgever meer verstrekkende verplichtingen introduceert dan andere lidstaten en/of (ii) in Nederland bepaalde verplichtingen onder DAC8 eerder van toepassing worden dan in andere lidstaten.

Cliënten op de markt voor cryptoactivadiensten zijn internationaal georiënteerd en mobiel. Zij stappen gemakkelijk over naar een aanbieder in een ander land indien dat in het voordeel van de gebruiker is. De drempels hiervoor zijn laag, juist gezien de aard en kenmerken van cryptoactiva. Deze mobiliteit maakt dat indien de Nederlandse wetgever verder zou gaan dan de wetgever in andere lidstaten ten aanzien van de implementatie van DAC8, dit naar verwachting zal leiden tot grote schade voor de Nederlandse cryptosector. Het ligt in de rede dat afnemers van cryptoactivadiensten dan op grote schaal zullen overstappen naar aanbieders in een andere Europese lidstaat, waar de rapportageverplichtingen onder DAC8

pas later van toepassing worden en/of waar die verplichtingen minder verstrekkend zullen zijn. Voor de goede orde: de betreffende buitenlandse aanbieder zal gewoon diensten naar Nederland kunnen aanbieden op basis van het zgn. Europees paspoort onder MiCAR. Een risico is ook dat afnemers van cryptoactivadiensten zullen kiezen voor niet-Europese of decentrale aanbieders. Een dergelijke ontwikkeling zou niet alleen de positie van Nederlandse aanbieders van cryptoactivadiensten raken, maar ook de doelstellingen van DAC8 ondermijnen.

Hieronder zal de VBNL opmerkingen maken ten aanzien van een aantal onderwerpen uit het concept wetsvoorstel. Verzocht wordt om deze opmerkingen te betrekken bij het verdere wetgevingsproces. De opmerkingen zijn nadrukkelijk een selectie en deze kunnen niet als uitputtend worden beschouwd.

3. Privacy van gebruikers

Het voorstel heeft grote impact op de privacy van gebruikers. In dat kader vraagt de VBNL aandacht voor de volgende onderwerpen.

Herleidbaarheid transactiehistorie

Met de wetswijziging zijn te rapporteren aanbieders van cryptoactivadiensten vanaf 1 januari 2026 verplicht om inlichtingen op te vragen bij hun gebruikers, en moeten zij de inlichtingen van bepaalde gebruikers delen met de Belastingdienst samen met informatie over de door gebruikers verrichte transacties. Deze informatie wordt vervolgens gedeeld met andere belastingdiensten via een Europese databank.

Het gaat om een verstrekkende verplichting ten aanzien van de privacy van gebruikers. De inhoud van de te rapporteren informatie is uitgebreider dan de informatie die aanbieders van cryptoactivadiensten op basis van de (wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) dienen in te winnen. De rapportageplicht is bovendien zeer ruim: alle transacties van gebruikers moeten worden gerapporteerd.

De feitelijke impact van deze verplichting wordt vergroot door de aard van cryptoactiva: de transactiegeschiedenis van een gebruiker is voor eenieder immers herleidbaar op basis van de openbare blockchain (DLT). Wanneer een adres wordt aangemaakt binnen een wallet, zal dit altijd geldig blijven. Het is voor eenieder zichtbaar welke eerdere transacties hebben plaatsgevonden vanaf of naar hetzelfde adres, zonder limitering in de tijd. Dat betekent dat op basis van de verkregen informatie, ook de transactiehistorie buiten de rapportageperiode herleidbaar is ten aanzien van de gebruikers. De rapportageverplichting werkt hierdoor verder door in relatie tot afnemers van cryptoactivadiensten, vergeleken met de fiscale rapportageverplichtingen die gelden voor overige administratieplichtige ondernemingen, zoals financiële instellingen. Deze laatste verplichtingen zien op de financiële situatie (bijv. banksaldi) van cliënten. Het betreft een momentopname, op basis waarvan de eerdere transactiehistorie van de gebruiker niet kan worden herleid. Dat is anders ten aanzien van cryptoactiva.

Het wetsvoorstel bevat geen mitigerende maatregelen, om te voorkomen dat onder DAC8 feitelijk een verdergaande inbreuk plaatsvindt van de privacy belangen van gebruikers dan onder vergelijkbare fiscale rapportageverplichtingen ten aanzien van andere soorten ondernemingen. De VBNL acht het van groot belang dat dergelijke waarborgen alsnog worden geïntroduceerd. Daarbij is van belang dat de Nederlandse wetgever een eigen verantwoordelijkheid heeft wat betreft naleving van de rechtsbeginselen zoals volgen uit het Handvest van de Grondrechten van de Europese Unie, het Europees Verdrag voor de Rechten van de Mens (EVRM) en de Algemene Verordening Gegevensbescherming (AVG). De Nederlandse wetgever kan in dat verband niet volstaan met een verwijzing naar de Europese wetgever.

Kan worden toegelicht welke specifieke waarborgen zullen worden toegepast met betrekking tot de privacy positie van gebruikers, gezien de specifieke aard van cryptoactiva wat betreft de openbaarheid van transactiehistorie aan de hand van de gebruikte adressen?

Niet-unierechtelijke staten

De Nederlandse wetgever geeft in de Memorie van Toelichting aan dat de richtlijn in overeenstemming is met de Europese wetgever op het gebied van privacy en gegevensbescherming, en dat zij in de implementatiewet niet verder gaat dan wat de richtlijn voorschrijft.[1] Daarbij stelt zij dat het vragen van gegevens en ook het opslaan van deze gegevens door lidstaten in overeenstemming is met de EU-gegevensbeschermingswetgeving. De richtlijn verschaft echter voor lidstaten ook de mogelijkheid om de verkregen inlichtingen te delen met niet-unierechtelijke staten. Deze staten vallen niet onder de Europese wetgeving omtrent gegevensbescherming en bieden niet vanzelfsprekend adequate bescherming voor personen en hun persoonsgegevens – iets waar het Europees Hof in recente rechtspraak (zoals Schrems I en II) veel waarde aan hecht.

Hoe wordt de privacy van gebruikers gewaarborgd in deze staten die niet onder EU-gegevensbeschermingswetgeving vallen?

Cybersecurity

Er zal ontzettend veel data van gebruikers terechtkomen in een centrale databank van de Europese Unie. De verschillende lidstaten zullen toegang hebben tot deze databank, maar deze lidstaten verschillen onderling in het niveau van cybersecurity dat zij hebben.

Welke maatregelen zijn er genomen om ervoor te zorgen dat de informatie van gebruikers wordt beschermd? Waar zal de informatie feitelijk worden opgeslagen? Welke servers zullen hiervoor worden gebruikt en door wie worden deze servers beheerd en/of aangeboden?

Het is niet ondenkbaar dat deze database een doelwit kan worden voor cyberattacks. Hier geldt opnieuw: gezien de aard van cryptoactiva die worden verhandeld op een publieke blockchain, geven de transacties in de database toegang tot een veel grotere set aan achterliggende data met betrekking tot de transactiehistorie van de betreffende gebruikers.

Hoe ziet de Nederlandse wetgever het risico dat lidstaten met een ondermaats niveau van cybersecurity volledige toegang hebben tot alle gegevens van de te rapporteren gebruikers van cryptoactiva binnen de EU? Wie zal er verantwoordelijk zijn voor de vervolgschade indien er een data lek van de gegevens van gebruikers plaatsvindt? Zullen alle lidstaten toegang hebben tot de gehele databank of wordt de toegang voor belastingdiensten beperkt tot informatie over specifieke gebruikers (dat wil zeggen: gebruikers die belastingplichtig zijn in het betreffende land)?

Dezelfde vragen spelen – in nog dringendere mate – ten aanzien van de situatie waarbij inlichtingen gedeeld worden met niet-unierechtelijke staten (zie hiervoor).

4. Data minimalisatie

Uitbreiding doeleinden

[1] Concept MvT par. 3.1.

In artikel 1 lid 7 van de richtlijn (in de implementatie staat het onder art. 1 V) is opgenomen dat de lidstaten de verkregen data ook voor andere doeleinden mogen gebruiken, zoals voor de handhaving van douanerechten en voor de bestrijding van witwassen en terrorismefinanciering. Welke grens is hieraan gesteld? 'Handhaving van douanerechten' en 'bestrijding van witwassen en terrorismefinanciering' zijn ruime doeleinden. Het wordt niet verduidelijkt op welke manier de inlichtingen (mogen) worden gebruikt en wanneer het doel is bereikt. Zijn hier maatstaven voor? Met betrekking tot een verregaande rapportageverplichting als hier aan de orde, dient naar het inzicht van de VBNL glashelder te zijn voor welke – afgebakende – doeleinden de gegevens kunnen worden gebruikt.

Ook wordt de bevoegdheid gegeven om de inlichtingen te delen aan de lidstaat die op grond van art. 215 TFEU (sancties jegens iets/iemand) beperkende maatregelen heeft getroffen.

Kunnen de inlichtingen dus voor meer gebruikt worden dan alleen voor belastingdoeleinden? Hoe ziet de Nederlandse wetgever dit?

Bewaartermijn

Hoe lang verwacht de wetgever dat de informatie wordt bewaard? De richtlijn schrijft voor dat de informatie minimaal voor 5 jaar moet worden bewaard en niet langer dan nodig is om de doelstellingen van de richtlijn te verwezenlijken. De wetgever geeft in de Memorie van Toelichting aan dat dit in de praktijk vaak voor 7 jaar wordt gehouden.

Waarom beperkt de Nederlandse wetgever zich niet tot 5 jaar? Wanneer zijn de doelstellingen verwezenlijkt?

Binnenlandse gebruikers

In de preambule (13) van de richtlijn staat opgenomen:

'*De rapportageverplichting moet betrekking hebben op zowel grensoverschrijdende als binnenlandse transacties, teneinde de doeltreffendheid van de rapportregels, de goede werking van de interne markt, een gelijk speelveld en de naleving van het non-discriminatiebeginsel te waarborgen*'.

In de concept Memorie van Toelichting (par. 2.6) wordt gesuggereerd dat dit in DAC8 wordt "voorgeschreven". DAC8 ziet echter op internationale samenwerking en een considerans bij een richtlijn kan niet op één lijn worden geplaatst met de tekst van de richtlijn zelf. Vereist een minimale of neutrale implementatie van DAC8 dat deze verplichting wordt geïntroduceerd? Is het de bedoeling dat *dezelfde* inlichtingen (in beginsel worden van alle gebruikers inlichtingen verzameld, waarna op basis van deze inlichtingen vervolgens wordt gefilterd op wel/niet te rapporteren), ook worden gebruikt voor deze *binnenlandse* doeleinden?

5. Kosten van naleving

De in de Memorie van Toelichting genoemde extra lasten die de bedrijven zullen ervaren ten gevolge van het beoogde wetsvoorstel, worden te laag voorgesteld.

In par. 5.1.1 van de concept Memorie van Toelichting wordt toegelicht dat de administratieve last gering zal zijn. Vervolgens worden echter op basis van het impact assessment van de Europese Commissie toegelicht, dat het voor in Nederland rapporterende aanbieders zou gaan om incidentele administratieve lasten van tussen € 20,8 miljoen en € 25,4 miljoen. Hierbij wordt uitgegaan van 15 aanbieders, op basis van het aantal AFM vergunningaanvragen onder MiCAR. Dat zou een bedrag betekenen van gemiddeld meer dan € 1 miljoen (!) per aanbieder (waaronder ook kleine partijen moeten worden begrepen).

Begrijpt de wetgever de impact hiervan voor de sector? Hetzelfde geldt voor de structurele administratieve lasten, die tussen de € 1,8 miljoen en de € 2,2 miljoen worden geschat. Het gaat hier derhalve om kosten van gemiddeld meer dan € 100.000 per aanbieder. Deze kosten komen bovenop de jaarlijkse toezichtkosten die moeten worden betaald aan de toezichthouders AFM en DNB. Welke maatregelen worden genomen om de kosten van naleving tot een minimum te beperken?

Onduidelijkheid over aan te leveren data

Op dit moment is sprake van veel onduidelijkheid in de markt over de exacte aard van de data die door aanbieders van cryptoactivadiensten dient te worden gerapporteerd. Dit is onwenselijk. Voor een goede voorbereiding op de naleving van de toekomstige rapportageverplichting is vereist dat duidelijkheid bestaat over de vereiste *single datapoints*. Voorkomen moet worden dat binnen de markt verschillende interpretaties zullen worden gehanteerd.

Kan hier meer aandacht aan worden besteed? De verschillende onderdelen van het voorgestelde artikel 10ob lid 4 WIB laten ruimte voor interpretatie. Nu het hier gaat om de essentie van de rapportageplicht, kan dit onderwerp niet naar een later stadium worden doorgeschoven. De exacte aard en omvang van de aan te leveren informatie bepaalt immers de impact voor aanbieders (alsmede de impact op de privacy van gebruikers, zie hiervoor).

Datum eerste rapportage

DAC8 regelt niets aangaande een bepaalde datum waarop rapporterende aanbieders van cryptoactivadiensten uiterlijk moeten rapporteren. Dat betekent dat lidstaten hierin zelf een keuze moeten maken. Voor rapportage in Nederland is in het voorstel gekozen voor een uiterste rapportagedatum voor 31 januari van het kalenderjaar volgend op het jaar of de periode waarover moet worden gerapporteerd.

Heeft hieronder op Europees niveau afstemming plaatsgevonden? Is door het Nederlandse Ministerie van Financiën aan andere lidstaten verzocht op welke wijze zij hiermee om zullen gaan?

Ontwikkeling nieuwe IT-systemen

De rapporterende aanbieders van cryptoactivadiensten zullen van al hun gebruikers informatie moeten opvragen, hieruit moeten zij vervolgens de te rapporteren gebruikers filteren en hun informatie en ook de gegevens van elke transactie die zij uitvoeren bijhouden en rapporteren aan de bevoegde autoriteit. Naar verwachting zullen de aanbieders nieuwe IT oplossing moeten aanschaffen om dit te kunnen uitvoeren. In dat geval kunnen de kosten flink oplopen.

Hierbij speelt ook het format waarin de informatie moet worden opgeslagen een rol. Bepaalde wijzen van opslaan zijn goedkoper dan andere wijzen. Er is echter nog geen duidelijkheid over in welke specifieke format de gegevens moeten worden aangeleverd. Kan de Nederlandse wetgever specifieker aangeven op welke wijze het rapporteren dient plaats te vinden?

Mocht dit een XML file zijn die enkel via Digipoort kan worden ingediend, dan zullen de kosten voor de rapporterende aanbieders van cryptoactivadiensten oplopen nu blijkt dat het in de praktijk zeer lastig is om zelf een connectie met Digipoort tot stand te brengen.

De rapporterende aanbieders van cryptoactivadiensten hebben de tijd nodig om aan de rapportageverplichtingen te kunnen voldoen. Het kan maanden duren voordat zij geschikte IT systemen hebben dan wel inhuren, die zullen voldoen aan de door de Belastingdienst gestelde vereisten. Hoe wordt hier rekening mee gehouden?

Omvang van aan te leveren data

Het is niet duidelijk in welke vorm de verkregen data zal worden opgeslagen en verwerkt. Het gaat om ontzettend veel gegevens. Denk bijvoorbeeld aan de situatie waarbij (zeer) frequent wordt gehandeld (al dan niet met behulp van een trading bot). Het lijkt technisch niet goed haalbaar om hier op een efficiënte wijze mee om te gaan in lijn met de doelstellingen van DAC8. Kan worden toegelicht hoe dit in de praktijk zal werken? Hierover dient van meet af aan duidelijkheid te bestaan. Voorkomen moet worden dat een meldplicht wordt geïntroduceerd, zonder dat duidelijk is hoe precies met de verkregen informatie zal worden omgegaan. Er worden niet alleen inlichtingen over de gebruikers zelf gevraagd, maar ook wordt er ten aanzien van elke transactie gedetailleerde informatie gevraagd. Ingeval van geautomatiseerde *high-frequency* handel kan het gaat om duizenden (of meer) transacties per dag. Het is niet duidelijk waarom informatie over elke transactie is vereist om te kunnen voldoen aan de doelstelling van DAC8.

In hoeverre zou informatie op geaggregeerde basis kunnen worden aangeleverd? Hoe ziet de wetgever dit? In welke vorm wil de Nederlandse wetgever/Europese wetgever de gegevens hebben? En hebben Nederland en (de overige lidstaten binnen) Europa de digitale capaciteit om zoveel gegevens op te slaan en op efficiënte wijze te kunnen verwerken?

Overleg marktpartijen

De wetgever heeft in de Memorie van Toelichting aangegeven dat de Belastingdienst zal onderzoeken langs welke digitale weg de gegevens en inlichtingen door de rapporterende aanbieders van cryptoactivadiensten op de meest laagdrempelige manier aan de Belastingdienst zullen kunnen worden aangeleverd. Er staat aangegeven dat dit zal gebeuren in overleg met marktpartijen.[2] Wie mogen deelnemen aan dit overleg en wat zal feitelijk gebeuren met de namens de marktpartijen gegeven input? Wordt er rekening gehouden met kleinere cryptoaanbieders, voor wie de relatieve impact mogelijk groter zal zijn dan voor de grotere partijen? Hier geldt opnieuw dat eerst duidelijkheid dient te worden gecreëerd over de wijze waarop aan de rapportageplicht kan worden voldaan, alvorens deze verplichting in werking treedt.

6. Rapportageverplichting

Benadeling Nederlandse aanbieders

Zoals hiervoor genoemd kenmerkt de markt van cryptoactivadiensten zich door een grote mate aan mobiliteit. De drempel voor het overstappen van een Nederlandse aanbieder naar een aanbieder in het buitenland ligt laag voor gebruikers. Wanneer een bepaalde aanbieder zwaardere informatieverplichtingen invoert of deze pas invoert per een latere datum, zal dit voor veel van de gebruikers reden zijn om deze aanbieder te verlaten en over te stappen naar een aanbieder die deze informatieverplichtingen niet heeft. De houders van cryptoactiva zullen naar verwachting op grote schaal overstappen naar aanbieders in een Europese lidstaat waar de minste vergaande verplichtingen van toepassing zijn dan wel overstappen naar een niet-Europese aanbieder. Dit zou zowel de concurrentiepositie van Nederlandse aanbieders ten opzichte van Europese aanbieders aantasten, als de concurrentiepositie van alle Europese aanbieders – waarvan in het bijzonder ook Nederlandse aanbieders – ten opzichte van alle niet-Europese aanbieders.

Heeft de Nederlandse wetgever dit voldoende gerealiseerd? Vindt er op Europees niveau overleg plaats over een uniforme implementatie van DAC8 en de desbetreffende interpretatie van in DAC8 opgenomen definities? Heeft de Nederlandse wetgever hierover overleg met andere lidstaten, zoals Duitsland, Oostenrijk of Frankrijk? Wat is bekend over de verwachte datum van implementatie in andere lidstaten?

[2] Par. 5.1.1. concept MvT.

Bestaande gebruikers

Het zal voor te rapporteren aanbieders van cryptoactivadiensten een grote opgave zijn om de vereiste gegevens te verkrijgen van gebruikers. Ten aanzien van bestaande gebruikers zal dit nog lastiger kunnen zijn, aangezien het gaat om aanvullende informatie ten opzichte van de informatie die eerder door de aanbieder werd verlangd, dat wil zeggen ten tijde van het aangaan van de contractuele relatie. Bovendien zijn er veel gebruikers die niet actief handelen in cryptoactiva. De responsiegraad ten aanzien van deze groep zal mogelijk beperkt zijn. Hoe ziet de wetgever dit?

In de bijlage van de richtlijn is opgenomen dat een aanbieder van cryptoactivadiensten moet verhinderen dat een gebruiker, die na twee aanmaningen volgend op het initiële verzoek van de aanbieder nog niet de vereiste inlichtingen aan hem heeft verschaft, te rapporteren transacties kan verrichten bij de aanbieder.[3] Er moeten minimaal zestig dagen zijn gepasseerd tussen de aanmaningen en de verhindering. Ten aanzien van bancaire cliënten is voor zover bekend geen sprake van een verplichting om de relatie op te zeggen, indien de bank niet kan voldoen aan fiscale rapportageverplichtingen. Hoe ziet de wetgever dit in verhouding tot aanbieders van cryptoactivadiensten?

Diepgang verificatie

Hoe ver moeten de cryptoaanbieders gaan om de juistheid/volledigheid van de door de gebruikers aangeleverde informatie te verifiëren? In de concept Memorie van Toelichting staat:

'*Bij algemene maatregel van bestuur - waarvoor dit wetsvoorstel een grondslag biedt - worden (nadere) regels gesteld met betrekking tot de verzamel- en verificatievereisten waaraan rapporterende aanbieders van cryptoactivadiensten moeten voldoen. Die regels zien ook op de eisen waaraan een eigen verklaring van een gebruiker van cryptoactiva moet voldoen.*'[4]

Kan dit verder worden toegelicht? Het is naar het inzicht van de VBNL onwenselijk dat een dergelijke uitwerking plaatsvindt op het niveau van een AMvB, in plaats van de wet in formele zin.

In de richtlijn is voor een geldige eigen verklaring slechts nodig dat deze is ondertekend door de verklarende en dat de verklaring de naam, woonadres, lidstaat van fiscale woonplaats, fiscaal identificatienummer en geboortedatum bevat. De richtlijn stelt enkel dat een aanbieder de redelijkheid van de aangeleverde eigen verklaring moet kunnen bevestigen op basis van de aangeleverde informatie. Wanneer een aanbieder weet of redenen heeft om te weten dat de aangeleverde eigen verklaring onjuist of onbetrouwbaar is, zal deze voor een nieuwe eigen verklaring moeten vragen en deze vervolgens bevestigen. Hoe diepgaand moet dit onderzoek zijn?

Wanneer verwacht de wetgever dat de algemene maatregel van bestuur wordt gepubliceerd? Het is voor de cryptoaanbieders belangrijk om te weten aan welke verzamel- en verificatievereisten zij moeten voldoen, want daar moeten zij hun IT-systemen wel op aanpassen.

Implementatiedatum

De datum waarop de richtlijn wordt geïmplementeerd is erg belangrijk. Wanneer een lidstaat DAC8 al eerder implementeert dan andere lidstaten, worden de cryptoaanbieders in die

---

[3] Richtlijn 2023/2226, Bijlage IV, Deel V, paragraaf A, punt 2.

[4] MvT p. 9.

lidstaat benadeeld. De gebruikers kunnen en zullen gemakkelijk naar aanbieders in de andere lidstaten overstappen, omdat die nog geen informatie over hen hoeven op te vragen.

De implementatiedatum van de wetswijziging is 1 januari 2026. Dit is de uiterlijke datum waarop de Europese richtlijn geïmplementeerd moet zijn in de nationale wetgeving van de lidstaten. De Nederlandse wetgever wijkt in dit opzicht niet af door het al veel eerder te implementeren.

Als echter de komende periode duidelijk wordt dat in andere lidstaten de implementatie later zal plaatsvinden (zoals in de praktijk regelmatig voorkomt), dan brengt het vereiste van een gelijk speelveld mee dat ook de inwerkingtreding van het Nederlandse voorstel wordt aangehouden. Voorkomen moet worden dat Nederlandse aanbieders van cryptodiensten onnodig worden benadeeld en zij gebruikers zullen verliezen. In de praktijk komt zeer regelmatig voor dat richtlijnen later worden geïmplementeerd, zonder dat dit leidt tot inbreukprocedures door de Europese Commissie. Kan de Nederlandse wetgever dit monitoren?

7. Europese rechtsbeginselen

Ten aanzien van de Europese rechtsbeginselen gaat het volgende.

Spanning met de AVG

Het bovenstaande geef aan dat DAC8 op spanning staat– en waarschijnlijk strijdig is met de AVG en fundamentele rechten op privacy. Zonder af te doen aan eerder genoemde punten van zorg is het belangrijk om duidelijk te maken dat DAC8 niet strookt met de principes van de AVG zoals genoemd in artikel 5 AVG: De grote verzameling gegevens staat onder andere op gespannen voet met artikel 5(1)(c) AVG, dat bepaalt dat gegevens toereikend moeten zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt. De aanzienlijke verzameling data legt daarnaast extra nadruk op de noodzaak om passende technische en organisatorische maatregelen te nemen – iets waar vooralsnog weinig rekenschap van wordt genomen artikel 5(1)(f) AVG. Tot slot zijn er amper maatregelen genomen om verder gebruik van de gegevens adequaat te beperken, iets wat niet overeenkomt met het doelbindingsbeginsel (artikel 5(1)(b) AVG).

Spanning met fundamentele rechten

In 2014 oordeelde het Hof van Justitie van de Europese Unie (**HvJ**) dat de richtlijn Betreffende Gegevensbewaring (inzake verplichte bewaring telecommunicatiegegevens door aanbieders) dat deze in strijd was met het recht op eerbiediging van het privéleven (artikel 7 Handvest) en het recht op bescherming van persoonsgegevens (artikel 8 Handvest).[5] De twee voornaamste bezwaren van het Hof zijn ook bij DAC8 een reden tot voorzichtigheid:

- Volgens het Hof voldeed de richtlijn niet aan het proportionaliteitsbeginsel. Hoewel de richtlijn legitieme doelen nastreefde, zoals de bestrijding van ernstige criminaliteit, was de inbreuk op de fundamentele rechten door de enorme verzameling gegevens te groot en onvoldoende specifiek. DAC8 kenmerkt zich ook door een zeer grote, weinig specifieke, en potentieel disproportionele gegevensverzameling.

- Daarnaast bevatte de richtlijn onvoldoende waarborgen voor de bescherming van de opgeslagen gegevens, zoals duidelijke voorwaarden voor toegang en gebruik door autoriteiten. Zoals hierboven beschreven is ook dit een serieus punt van zorg bij DAC8, waar nog bij komt dat de gegevens ook nog eens in een centrale database

[5] Europees Hof van Justitie, 8 april 2014 gevoegde zaken C-293/12 en C-594/12, ECLI:EU:C:2014:238 (*Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources ea.*)

worden opgeslagen. De noodzaak voor specifieke en verregaande waarborgen is evident, en ligt zeker bij een richtlijn, grotendeels bij de lidstaten zelf.

De jurisprudentie van het HvJ en ook het Europees Hof voor de Rechten van de Mens (**EHRM**)[6] benadrukken consistent het belang van proportionaliteit in het kader van het verzamelen van persoonsgegevens.[7] De implementatie van DAC8 door de Nederlandse overheid dient hier dan ook in het bijzonder rekenschap van te geven.

8. Overige aandachtspunten

Tot slot kunnen de volgende aandachtspunten worden genoemd.

Hoogte van sancties

In artikel 1 deel V van het conceptwetsvoorstel wordt het volgende lid toegevoegd aan artikel 11 WIB:

4. Indien het aan opzet of grove schuld van de rapporterende aanbieder van cryptoactivadiensten, bedoeld in de artikelen 10ob, eerste lid, 10od, eerste en tweede lid, is te wijten dat de verplichtingen, bedoeld in hoofdstuk II, afdeling 4ad, en de daarop berustende bepalingen, niet, niet tijdig, niet volledig of niet juist zijn of worden nagekomen, vormt dit een vergrijp ter zake waarvan Onze Minister hem een bestuurlijke boete van ten hoogste het bedrag van de zesde categorie, bedoeld in artikel 23, vierde lid, van het Wetboek van Strafrecht, kan opleggen.

Deze sanctie op overtreding van de wet kan disproportioneel zijn. Een boete van de zesde categorie 6 kan oplopen tot €1.030.000. De richtlijn stelt slechts dat de sancties '*doeltreffend, evenredig en afschrikkend*'[8] moeten zijn. Het lijkt erop dat Nederland veel hogere sancties stelt op overtreding dan dat andere lidstaten. Hoe is dit in andere lidstaten geregeld? Is daar onderzoek naar gedaan? Zijn er waarborgen om een vergelijkbare aanpak te hanteren, gelet op de concurrentiepositie van Nederlandse cryptoaanbieders?

Zie bijvoorbeeld de Duitse implementatiewet van DAC8, daarin zijn de maximale sancties veel lager, namelijk €50.000 en €10.000.

Een te hoge potentiële sanctie kan ervoor zorgen dat huidige in Nederland gevestigde en potentieel toekomstige aanbieders van cryptoactiva zullen overwegen of Nederland nog wel de beste vestigingslocatie is vergeleken met andere lidstaten.

Verschuiving naar niet-gereguleerd

Zoals hiervoor genoemd is de kans aanwezig dat huidige gebruikers op grote schaal zullen overstappen naar andere cryptoaanbieders binnen of buiten de EU, indien daar minder vereisten van toepassing zijn.

Het kan zich ook voordoen dat houders van cryptoactiva hun cryptoactiva weghalen van aanbieders van bewaarportemonnees (de meeste exchanges bieden deze mogelijkheid) en de cryptoactiva 'cold' (dat wil zeggen middels een eigen *non-custodial* oplossing) zullen opslaan en/of buiten in Europa gereguleerde exchanges om zullen handelen (via bijvoorbeeld een

---

[6] Zie bijvoorbeeld EHRM, 13 september 2018, 58170/13 (*Big Brother Watch and others v United Kingdom*)

[7] Zie in meer algemene zin *European Data Protection Supervisor* (EDPS), 'Guidelines on Proportionality', te raadplegen: https://www.edps.europa.eu/data-protection/our-work/publications/guidelines/edps-guidelines-assessing-proportionality-measures_en.

[8] Art. 25 bis

decentralised exchange of op basis van *reverse sollicitation* via een exchange buiten de EU). In dat geval is de gebruiker de enige die toegang heeft en is geen sprake van een externe partij, zodat de rapportageplicht niet van toepassing is.

In deze gevallen is het gevolg dat er juist minder zicht is op de cryptomarkt en dat ook het heffen van belasting lastiger wordt. De maatregelen van DAC8 zullen derhalve averechts kunnen werken. Ook vanuit het perspectief van de regelgever is daarom van belang dat het middel het doel niet voorbij schiet.

Ondermijning MiCAR

Een van de doelen van de MiCAR verordening is het creëren van veiligheid voor de houders van cryptoactiva door middel van regulering op Europees niveau.

Met de invoering van deze inlichtingenplicht stappen huidige, maar ook toekomstige, gebruikers wellicht over naar cryptoaanbieders buiten de EU, die geen of minder vergaande informatie van hen zal verzoeken. Hoe ziet de wetgever dit? Betekent dit dat een non-EU aanbieder van cryptodiensten, die buiten het bereik van MiCAR valt (bijv. doordat activiteiten op basis van *reverse sollicitation* worden verricht) en geen aanwezigheid heeft in een van de lidstaten (zoals bedoeld in artikel 10ab lid 1 onderdeel b van het voorstel), niet aan enige rapportageplicht onderhavig is? Artikel 61, lid 1, MiCAR beschrijft de situatie waarin een gebruiker die in de Europese Unie is gevestigd of gesitueerd, uit eigen beweging het initiatief neemt tot het afnemen van een cryptoactivadienst door een onderneming gevestigd in een derde land. In een dergelijk geval is deze onderneming uit het derde land niet onderworpen aan de vergunningsvereiste voor het aanbieden van crypto-activadiensten onder MiCAR.

Kan de wetgever in de Memorie van Toelichting aandacht besteden aan deze situatie?

Wordt met het voorstel een goede werking van MiCAR verordening ondermijnd? MiCAR heeft onder meer tot doel om veiligheid te verschaffen aan houders van cryptoactiva, maar de DAC8 richtlijn duwt diezelfde houders mogelijk naar non-EU cryptoaanbieders of *decentralised exchanges* waarbij er geen waarborgen voor de veiligheid van hun cryptoactiva zijn.

In de ter consultatie voorgelegde concept Memorie van Toelichting is hier geen of onvoldoende aandacht voor. Heeft de wetgever in voldoende mate afstemming gezocht met specialisten (waaronder wetgevingsjuristen) met voldoende expertise op het gebied van de werking – niet alleen in theorie, maar ook in de praktijk, van de markt voor cryptoactivadiensten en marktpartijen?

9. Tot slot

De VBNL hoopt dat het bovenstaande een constructieve bijdrage levert aan het wetgevingsproces. De VBNL is graag bereid tot het geven van een andere mondelinge of schriftelijke toelichting op het bovengenoemde.

Hoogachtend,

Bert de Groot

Voorzitter VBNL