

Onderwerp **Re: TMNL - Your Letter to Amazon Web Services**
Afzender Human Rights in Finance.EU (legal) <legal@hrif.eu>
Ontvanger [REDACTED]
Antwoord-aan <legal@hrif.eu>
Datum 2024-06-28 10:31



Dear Mr [REDACTED]

We forgot to send the name server info, but this would be helpful as well, we assume.

with kind regards

Simon

tmnl.nl



Domain Information

Domain:	tmnl.nl
Registrar:	Gandi
Registered On:	2007-07-17
Updated On:	2024-02-16
Status:	active
Name Servers:	ns-64.awsdns-08.com ns-1216.awsdns-24.org ns-743.awsdns-28.net ns-1978.awsdns-55.co.uk

Simon Lelieveldt

Bestuurslid / Board Member
Human Rights in Finance.EU
<https://hrif.eu>
legal@hrif.eu

KvK - 91170974

Human Rights in Finance.EU (legal) schreef op 28-06-2024 12:11:

Dear [REDACTED]

Thank you kindly for your communication and confirmation of receipt of the letter by Amazon Web Services.

To be honest, the exact Amazon corporate structure is a mystery to us and we apologize if our communications are sent to the wrong part of the company. If so we would highly appreciate you forwarding our communications to the relevant corporate bodies or legal entities within the Amazon business.

A brief explanation on TMNL as a customer and its operations (including a link to the AWS document in which AWS refers to them as part of their commercial proposition for cloud based monitoring work) is found below. We have also listed an outline of the main legal angles via which its processing is unlawful.

We trust Amazon to draw the appropriate conclusions and stop servicing TMNL immediately as well as deleting all data and algorithms/outcomes of data processing (and thereby stop transgressing the Dutch Penal Code itself).

Then again, as we have 30+ years background in financial legislation and an active working background within supervisors, central banks, banks and fintechs, we do fully understand that this intersection of GDPR, AML-law and Dutch specificities is complex to grasp in first instance. Do also note that from open government information it has become clear that TMNL has misinformed our Ministry of Finance on the exact nature of its operations (as it may have misinformed you).

What you have received so far from us is the main legal opinion that matters most, but we stand ready to further elaborate in an online-call on our explanation and highlight the range of legal details which will allow AWS to draw its own further conclusions.

We propose to hold an online meeting by Monday 0930 focused on further mutual understanding of the legalities and investigations of constructive ways forward so that no further harm is being done in terms of human rights infringements by TMNL (including arrangements on possible joint publicity and action).

In this respect do also note that our request is the logical follow up to the [petition](#) that we presented to Dutch parliament in february (supported by 15000 Dutch customers and 9 NGO among which Bits of Freedom and Privacy First).

With kind regards

Simon Lelieveldt

Chair HRIF.EU

Brief outline of TMNL - and its illegal/criminal operations

TMNL stands for Transaction Monitoring Netherlands (Transactie Monitoring Nederland BV) and their services requested from Amazon pertain (possibly) to webservice for the domain www.tmn.nl as well as back office cloud computing for their transaction monitoring operations.

They are registered under Chamber of Commerce number (78554454) and we have attached a copy of their Chamber of Commerce Registration as well as their bylaws. As you can read in the bylaws, their core business is doing transaction monitoring for banks.

A further description of the situation with respect to TMNL and our priority to ensure its immediate and full stop of unlawful data processing can be found the following English pages our website: <https://hrif.eu/en/2024/04/tmnlstopuk/>. You will also see that an administrative action is pending in the court of Rotterdam (this Summer) as a follow up to the enforcement request that we made to the Dutch central bank: <https://hrif.eu/en/2024/04/dnbstopmnlnow/>

It is clear from notifications on LinkedIn (a.o. https://www.linkedin.com/posts/webstar_soc2t2-teamwork-aws-activity-7196848718430568448-soWU?utm_source=share&utm_medium=member_desktop) and on the web (<https://customers.xebia.com/dutch-banks-assemble-to-fight-financial-crime>) that AWS is providing back office-services to TMNL. This is more specifically confirmed by the document on Amazon's own website: <https://pages.awscloud.com/rs/112-TZM-766/images/Banking-on-the-Cloud-ebook.pdf> which proudly lists TMNL as an example and customer.

How AWS transforms the fight against financial crimes

Monitoring financial crimes requires access to large and diverse sets of data and the ability to run on-demand or real-time analytics. Financial crimes and compliance departments at banks are using cloud-based technology to meet these demands and manage emerging fraud patterns.

Some of these cloud-based solutions include:

Real-time data analytics

Most banks are enabling end-to-end digital onboarding of customers, thus helping them achieve higher customer conversion rates as they deploy real-time analytics in the cloud, giving them the ability to use unstructured data such as biometrics, facial images, and documents and structured data. making authentication and customer

ML deployment at scale

Banks are relying on rules-based transaction monitoring patterns, but with modern fraudsters relying on sophisticated technology, rules rapidly become stale and might not successfully prevent fraud. To counter this, banks are using cloud-based ML that can scale to accommodate and detect unknown spikes or trends in financial transactions and generate alerts for review. As these models are compute intensive, banks are using the cloud to deploy ML features such as Deep Graph Library (DGL) to train neural network models to detect malicious transaction patterns. For instance, Transaction Monitoring Netherlands (TMNL)—a joint venture among five large banks in the Netherlands—is building a scalable transaction analytics platform to analyze a significantly large number of business payments for seemingly unusual transactions.

Fact of the matter is that a legal basis for monitoring those transactions is missing. Also, when setting up the bylaws of TMNL, errors were made. The bylaws are missing an activity constraints condition that states: until such time a legal basis has been promulgated in the Netherlands, which allows the outsourcing of transaction monitoring to third parties, the activities of TMNL will only be limited to setting up operations and will not involve any operational transaction monitoring, testing or use of personal and

transaction data received from banks. TMNL is well aware of this constraint but chose to process data of Dutch citizens and companies regardless and is receiving those personal data on a regular/daily basis.

If you read/translate the history of setting up the legislation (<https://open.overheid.nl/documenten/ronl-e333903480c1fbc1cf4f9b529d34f6030f405a42/pdf>) you will read particularly on page 29-31 that TMNL has started operations without respecting the GDPR. It has not done a prior data protection impact assesment and its chosen legal title: justified interests is insufficient under the GDPR as there is a prohibition on outsourcing of transaction monitoring by bank to third parties. More important (and by itself sufficient to immediately stop AWS-service) TMNL is processing sensitive personal data without explicit legal title.

Late last year, TMNL itself asked the central bank to get a different appreciation of the law that would allow their outsourced processing. By May 2024, DNB specifically turned repeated its stance that outsourcing of transaction monitoring is not allowed under the current AML-law. The DNB [feedback statement](#) briefly rejects the suggestion.

Uitbesteding			
Paragraaf 2.2 (consultatieversie)		Paragraaf 3.4 (finale versie)	
1	Reikwijdte uitbesteding	a) EMA, TMNL en VBIN vragen naar de reikwijdte van uitbesteding: valt het gebruik van software van een derde partij hier ook onder?	a) DNB heeft deze suggestie meegenomen en verwijst naar de Q&A 'Is het gebruik van software van een derde ter ondersteuning van het cliëntenonderzoek uitbesteding?' in paragraaf 3.4. a) Ja b) Nee

15

	b) TMNL vraagt om toe te voegen dat het voortdurend monitoren een dynamisch proces is met vier belangrijke elementen. Als enkele specifieke elementen door een derde partij worden uitgevoerd, dan is er geen sprake van uitbesteding.	b) DNB heeft (vooralsnog) geen beleidsuiting over dit onderwerp opgenomen in de Q&A/GP Wwft.	
2	Verantwoordelijkheid Het Verbond ziet graag meer nadruk op de	DNB heeft deze suggestie meegenomen en verwijst naar	la

Simon Lelieveldt

Bestuurslid / Board Member
Human Rights in Finance.EU
<https://hrif.eu>
legal@hrif.eu

KvK - 91170974

schreef op 28-06-2024 10:57:

Dear Mr. Lelieveldt,

We refer to your letter dated June 20, 2024, concerning a request to Amazon Web Services (AWS) to suspend services to "Transaction Monitoring Systems Netherlands" or "TMNL" based on alleged infringements of Dutch anti money laundering laws and alleged violations of the EU's General Data Protection Regulation.

AWS asked us to confirm receipt of that letter and to respond to you as follows:

1. AWS kindly requests that you provide further information that allows AWS to determine the specific company identified in your letter and the specific websites, resources, or other information relating to its relevant activities. Based on the information currently available, AWS cannot precisely determine whether any and, if so,

which, AWS account(s) are associated with the activity you are reporting and what specific resources may be concerned. Preferably, you could provide this information by stating the IP address(es) paired with timestamp(s) of the activity in question. This would allow AWS to proceed with the assessment of this matter in a diligent and accurate manner.

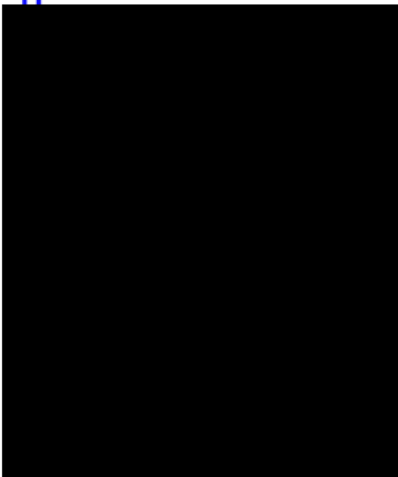
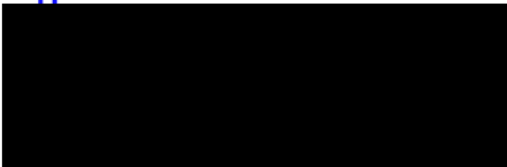
1. To expedite the further process, AWS also asks for your consent to forward your letter to the AWS customer in question in a non-anonymized form – provided, of course, that AWS can, based on further information provided by you, identify a specific AWS account that the reported activities are connected to.

We look forward to hearing back from you.

Kind regards,



Rechtsanwalt | Counsel



=====

This message may be confidential and privileged. Use or disclosure by anyone other than an intended addressee is prohibited. If you received this message in error, please delete it and advise the sender by reply email. Learn about

