

To Mishcon de Reya LLP
Att. Filippo Noseda
Partner
70 Kingsway
London WC2B 6AH
United Kingdom
Via email: filippo.noseda@mishcon.com

Date 1 October 2024, Amsterdam

Re RBE – Register of Beneficial Ownership
Procedures before the Tribunal d'Arrondissement de Luxembourg

Dear Mr Noseda,

We understand that:

- (a) you are involved in several cases before the district court of Luxembourg in relation to the mechanisms of accessing the local UBO-register (*Registre des Bénéficiaires Effectifs* or "RBE"), which is maintained by the Luxembourg Business Registers (LBR);
- (b) those cases were first initiated on 23 October 2020 and were suspended while *Sovim v LBR* was being decided by the Court of Justice of the EU (CJEU);
- (c) Following the CJEU judgment¹, which struck down the provisions of AMLD5² that established public registers of beneficial ownership (thus resuming the concept of "legitimate interest" under Art. 30 of AMLD4³), on 31 May 2024 the European Parliament adopted a new Anti-Money Laundering Directive⁴ ('AMLD6') that *de facto*

¹ *WM and Sovim SA v Luxembourg Business Registers* (C-601/20)

² Directive (EU) 2018/843

³ Directive (EU) 2015/849

⁴ Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024 on the mechanisms to be put in place by Member States for the prevention of the use of the financial

maintains public access to UBO-registers through expansive access provisions.

- (d) You are now seeking to continue the existing cases with the assistance of a local law firm, NautaDutilh, to address shortcomings to the rules concerning the concept of "legitimate interest".

Privacy First welcomes the work of the Luxembourg court assessing whether openness of the UBO-register complies with European law and, given the relevance for the entire EU, would welcome a reference of your cases to the CJEU to ensure compliance with the principles established in *Sovim*.

About Privacy First

Privacy First is a foundation (*stichting*) established under Dutch law that has financial privacy as one of its focus areas.⁵ We have found that in recent years, citizens' financial privacy is slowly but surely being eroded and the risks of identity fraud, misuse of financial personal data and discrimination are increasing as a result of the violation of basic data protection principles. The European legislator has good intentions to tackle crime and combat criminal financial flows, but deploys methods that are disproportionate and that expose compliant citizens to unnecessary risks for their data, as well as their safety. This is an area where Privacy First has been very active. For instance, we sent a letter to the Dutch Parliament drawing attention to the risks associated with European open finance plans⁶, we commented on credit registration proposals by the Dutch government⁷ and we warned that compliance with financial sanctions should not lead to violation of civil rights.⁸ Recently, we asked the Dutch central bank and the Ministry of Finance to adjust identification practices of financial institutions.⁹

system for the purposes of money laundering or terrorist financing, amending Directive (EU) 2019/1937, and amending and repealing Directive (EU) 2015/849 (Text with EEA relevance), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024L1640>

⁵ <https://privacyfirst.nl/en/theme/financial/>

⁶ <https://privacyfirst.nl/en/articles/privacy-first-advocates-restraint-in-dissemination-of-financial-personal-data/>

⁷ <https://privacyfirst.nl/en/articles/kredietregistratie-in-nederland-bkr-in-current-form-must-vanish/>

⁸ <https://privacyfirst.nl/en/articles/compliance-with-financial-sanctions-must-not-lead-to-violation-of-civil-rights/>

⁹ <https://privacyfirst.nl/en/articles/privacy-first-calls-for-adjustment-of-identification-practices-of-financial-institutions/>

Privacy First work on EU beneficial ownership registers

The beneficial owner ('UBO') phenomenon and the registration of beneficial owners (UBO-register) is a topic that Privacy First has been working on for a long time. An important issue is that we consider it undesirable that the general public should have access to UBO data.

In 2020 we started the preparations of a lawsuit against the Dutch government regarding the Dutch UBO-register. The summons was issued on 5 January 2021 and resulted in a court decision of 18 March 2021¹⁰ and a decision in appeal of 16 November 2021.¹¹ The Dutch court ruled that there were no grounds for provisions by the court in anticipation of the CJEU ruling, which was handed down on 22 November 2022.¹²

In 2023, we participated in a legislative consultation on the new UBO register regulations and called for measures to protect citizens from misuse of personal data in the register.¹³

Privacy First's position on the new AML Directive

Under the new Anti-Money Laundering Directive, AMLD6, the UBO-register is effectively publicly accessible. According to Article 12(2) AMLD6, the following private parties will have access to all UBO data for three years:

"2. The following natural or legal persons shall be deemed to have a legitimate interest to access the information listed in paragraph 1:

(a) persons acting for the purpose of journalism, reporting or any other form of expression in the media, that are connected with the prevention or combating of money laundering, its predicate offences or terrorist financing;

(b) civil society organisations, including non-governmental organisations and academia, that are connected with the prevention or combating of money laundering, its predicate offences or terrorist financing;

¹⁰ <https://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBDHA:2021:2457>, article Privacy First: <https://privacyfirst.nl/en/articles/judge-doubt-about-ubo-register-is-right/>

¹¹ <https://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:GHDHA:2021:2176>, article Privacy First: <https://privacyfirst.nl/en/articles/courts-ubos-can-ask-self-for-fencing/>

¹² Press release: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-11/cp220188en.pdf>; article Privacy First <https://privacyfirst.nl/en/articles/eu-hof-takes-dash-through-public-ubo-register/>

¹³ <https://privacyfirst.nl/en/articles/critical-comments-privacy-first-at-consultation-ubo-register/>

- (c) *natural or legal persons likely to enter into a transaction with a legal entity or legal arrangement and who wish to prevent any link between such a transaction and money laundering, its predicate offences or terrorist financing;*
- (d) *entities subject to AML/CFT requirements in third countries, provided they can demonstrate the need to access the information referred to in paragraph 1 in relation to a legal entity or legal arrangement to perform customer due diligence in respect of a customer or prospective customer pursuant to AML/CFT requirements in those third countries; (...)*
- (j) *providers of AML/CFT products, to the strict extent that products developed on the basis of the information referred to in paragraph 1 or containing that information are provided only to customers that are obliged entities or competent authorities provided that those providers can demonstrate the need to access the information referred to in paragraph 1 in the context of a contract with an obliged entity or a competent authority.*

In addition to the categories identified under the first subparagraph, Member States shall also ensure that other persons who are able to demonstrate a legitimate interest with respect to the purpose of preventing and combating money laundering, its predicate offences and terrorist financing, are granted access to beneficial ownership information on a case-by-case basis."

AMLD6 does not contain any safeguards to protect individuals identified as 'UBOs' (which is a very large group of individuals, not just shareholders).

These new European rules will be implemented in the Netherlands through a bill currently under consideration by the Dutch Parliament.

On 20 September 2024 Privacy First wrote a letter¹⁴ to the financial committee of the Dutch Parliament raising concerns about the new *de facto* public UBO-register.¹⁵ In that letter, Privacy First advised members of the House of Representatives to raise questions about the public accessibility of the UBO register and the lack of safeguards. Privacy First proposed that members of parliament include the following questions (non-official translation):

¹⁴ Letter in Dutch: https://privacyfirst.nl/wp-content/uploads/UBO_PrivacyFirst_TK_20september2024.pdf.

¹⁵ Article Privacy First: <https://privacyfirst.nl/en/articles/privacy-first-asks-second-chamber-not-to-approve-public-ubo-register/>

"What is the reason the Dutch government has agreed to allow access to such a large group of private parties?"

Article 13(6) AMLD states that the private party will get immediate access for the duration of three years. Why has such a long duration of access been chosen? Will this long duration be included in the order in council and, if so, why?

Is it correct that access for private parties under Articles 12 and 13 AMLD means that they can obtain UBO-data in bulk? We infer that from the text (there is no specific provision for those mentioned in Article 12(2)(j) AMLD, but for everyone who gets access).

Article 12(2)(j) AMLD allows data brokers to access the UBO-register. They will enrich the UBO data with personal data obtained from their customers, thus posing a major risk to citizens' data protection. Isn't it about time these parties became subject to licensing, testing for integrity and competence, and checking their systems for security and accuracy?

Has there been a thorough legal assessment of the legal sustainability of access for such a large group of private parties to the UBO register, in the light of European data protection and fundamental rights regulations? If so, please submit that assessment.

What is the reason that, in the case of Article 12(2)(c) (the person seeking to enter into a transaction), a UBO-statement requested by the entity itself is not sufficient? After all, this automatically establishes the legitimate interest and fulfills the requirement of data minimisation in the GDPR.

What is the reason that the private parties mentioned in Article 12(2) AMLD do not have to meet integrity requirements?

Is it correct that the Dutch regulations on detective agencies apply to private parties as referred to in Article 12(2)(a) and (b) AMLD if they conduct targeted research on a particular UBO (person-oriented research), while they are mostly unlicensed? Why is no action taken against such parties?

What is the reason for the inclusion in Article 12(1) AMLD that the legal entity or legal arrangement may not be warned that a private party's access is taking place?

Does it follow from the text of Article 12(1) AMLD that the prohibition on warning only relates to the legal entity or legal arrangement, so that the obligation of Article 14 GDPR has remained, and the UBO register authority and the viewing private party ('the viewer') are obliged to inform the UBO of the inspection taken, whereby the obligations of the GDPR must also be complied with in other respects?

Assuming that the UBO would not need to be informed about the consultation by a private party, what is the reason for deviating from one of the main basic principles of the GDPR, as set out in Articles 13 and 14, namely that every data subject must be informed of the acquisition of his/her personal data by a third party, so that the data subject can verify that processing is taking place on proper grounds and that the data is accurate?

Why is there no provision in the proposal that the UBO has the right to receive the data from the viewer, if it is found that his/her personal data has been misused?

In the future, access to the UBO-register can be obtained through the European system BORIS. Can you indicate what measures will be taken to prevent criminals, trolls and other unsavoury types from obtaining personal data of targets directly or through BORIS?

What is the reason that the government has made it appear that the European anti-money laundering package will only provide harmonisation, when in reality there are very far-reaching changes, which may entail high costs and also pose risks for citizens? Why was Parliament not informed about this earlier?

What is the reason that there are no provisions in the proposed amending law that make it a criminal offence if the UBO data is misused or passed on to third parties?

If private parties are going to have widespread access to UBO data, part of this is that the Dutch Data Protection Authority (AP) is going to exercise more intensive supervision. Will the AP receive extra budget to better monitor compliance with the GDPR by those who gain access to the UBO-register?"

From the above, you can see that our concerns about Europe's new anti-money laundering ('AML') rules are very substantial (and not the only concerns).

Privacy First recognises the importance of fighting crime but believes that the measures being taken should not result in criminals and other persons with bad intentions having free and indiscriminate access to people's personal data held in central UBO-registers. An example of abuse can be found in the recent report on Turkey's use of anti-money laundering rules to silence opponents in the EU, as reported by the Institute for Diplomacy and Economy (instituteDE): *Weaponizing Financial Systems – Erdoğan's Transnational Repression to Muzzle Dissidents Abroad*.¹⁶

¹⁶ See <https://www.institute.org/report/weaponizing-financial-systems-erdogans-transnational-repression-to-muzzle-dissidents-abroad> and the report: https://institute.ams3.cdn.digitaloceanspaces.com/Weaponizing_Financial_Systems_Version_1.2.pdf



We therefore support the request of the parties assisted by you to ask the Luxembourg court to review the new UBO-register rules and have the cases referred before the CJEU.

Yours sincerely,
on behalf of Privacy First,

Vincent Böhre
director