PER REGISTERED MAIL

Meta Platforms Inc.
1 Meta Way
Menlo Park, CA 94025
USA

Meta Platforms Ireland Ltd.
Merrion Road
Dublin 4
D04 X2K5
Ireland

Facebook Netherlands B.V.
Jollemanhof 15
Pakhuis Amsterdam, 2nd floor
1019 GW Amsterdam

In advance by e-mail: privacy@facebook.com

Draft: July 22, 2023
Our ref.: SOMI/Meta
Your ref.: -

Dear Sir/Madam,

On behalf of the Foundation for Market Information Research (`**SOMI**'), we kindly request your immediate attention for the following.

Introduction

SOMI is a non-profit organisation that represents the interests of natural persons, especially consumers and minors, that use online services and whose rights are violated in that regard, including fundamental rights such as the right to non-discrimination, the right to privacy and data protection, consumer rights and rights that protect minors. SOMI is committed to act against parties that violate such rights.

SOMI believes that Meta Platforms Inc. (formerly known as Facebook Inc.), Meta Platforms Ireland Ltd. (formerly known as Facebook Ireland Ltd.) and Facebook Netherlands B.V. ("**Meta**") have acted unlawfully and continue to act unlawfully towards users of the Facebook platform in the Netherlands ("**Dutch Users**"). Meta violates data protection laws on a massive scale, inter alia by permitting unauthorized persons to access the personal data of Dutch Users, by transferring their personal data to countries that do not offer an adequate level of data protection and by processing personal data for personalized advertising purposes without the required consent. SOMI will outline its complaints against Meta in this letter.

This complaint letter also refers to, and hence is accordingly directed at, the business practices of other Meta-related entities and other applications than the Facebook platform, or entities or applications with which Meta exchanges information or shares data, code or facilities, including data platforms or activities under names such as WhatsApp, Instagram and Oculus.

About SOMI

SOMI is a foundation in conformity with article 3:305a of the Dutch Civil Code. It meets all the admissibility requirements for bringing a collective action against Meta in the Netherlands on behalf of all Dutch Users, including a mass damages claim under the Dutch WAMCA. Currently, SOMI is conducting a mass damages case against TikTok.

More than 200,000 people have registered with SOMI to be informed of their GDPR rights and to benefit from SOMI's activities to protect and improve their rights under the GDPR.

In September 2021, SOMI launched a campaign in which participants can check whether their data have been subjected to a data breach that occurred on the Facebook platform in or around April 2021 ("**Facebook Data Breach**"). As part of that campaign, SOMI offers services for users who want to further collect their data from Facebook. In total, 169 data subjects have given SOMI authorization to retrieve all of their personal data stored by Facebook.

Meta's history of privacy violations

A pattern of repeated privacy breaches and unlawful processing of personal data has been visible since Meta's beginnings, starting in 2006 with the introduction of the news feed feature on the Facebook platform. This showed friends' profile updates of all Facebook users directly on its main page. Approximately one million users (at the time, Facebook had around 8 million users) joined the "Facebook News Feed protest group", arguing that the feature was too intrusive, showing every little personal detail such as two users befriending each other, or that a couple had broken up.[1]

In 2007 Facebook tracked purchases of its users and then without consent notified their Facebook friends of what they had bought. Later, Mark Zuckerberg had to issue an apology regarding this "Beacon" feature and had to give users an option to opt-out.[2]

Facebook also started sharing users' data with third parties for advertising purposes despite the lack of consent. In December 2011, Facebook agreed to settle Federal Trade Commission charges that it deceived consumers by telling them they could keep their information on Facebook private, and then repeatedly allowing it to be shared and made public. In total, eight privacy charges had been made against Facebook by the FTC.[3]

---

[1] NBC News, Sep 2nd, 2016, available at: https://www.nbcnews.com/tech/social-media/can-you-even-remember-how-you-coped-facebook-s-news-n641676 (last accessed: July 21st, 2023).

[2] Facebook, Dec 6th, 2007, available at: https://about.fb.com/news/2007/12/announcement-facebook-users-can-now-opt-out-of-beacon-feature/ (last accessed: July 21st, 2023).

[3] FTC, Nov 29th, 2011, available at: https://www.ftc.gov/news-events/news/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep-privacy-promises (last accessed: July 21st, 2023).

In 2014, Facebook performed an ethically highly questionable mood-manipulation experiment in which it altered news feed to test how emotions spread on social media.[4] Neither Facebook nor the company involved notified users that Facebook collected their personal data via cookies and Facebook unlawfully processed personal data for purposes of measuring the results of the experiments.[5]

In the same manner, in 2015 Facebook invaded the privacy of Belgian Facebook users by collecting information on the online behaviour of millions of them by placing cookies on their browsers to track the websites these individuals visited.[6] In February 2018, a Belgian court ordered Facebook to stop collecting private information about Belgian users and to delete all data it collected illegally.[7]

Also, NBC News revealed that Facebook was giving extended access to personal data of its users to partner companies like *Amazon* who advertised on Facebook, while cutting off access to user data for companies that it viewed as competitors.[8]

In 2018, the Bavarian Data Protection Supervisory Authority ruled that transmitting personal data to Facebook's Custom Audience service was unlawful because consent was not obtained from the users and since there is no legal ground to process this data. The Higher Administrative Court in Munich (*Verwaltungsgerichtshof*) confirmed the ruling on September 26th, 2018.[9]

In the updated WhatsApp Terms and Conditions of 2021, Meta enabled WhatsApp to share user data including the mobile phone number used to register with the platform and users' last seen time within the app with Facebook and other Meta-owned companies for marketing and targeting purposes. Again, consent was not freely given because it was conditioned by continuance of using its services in future. This practice resulted in a €225 million fine from the Data Protection Commission in Ireland in September 2021.[10]

A privacy researcher, Felix Krause, found that the Instagram and Facebook app on iOS used tracking codes on users who click on links, thereby opening the in-app browser, which was controlled by the

---

[4] NBC News, Alyssa Newcomb, Mar 24th, 2018, 12.02 PM, available at: https://www.nbcnews.com/tech/social-media/timeline-facebook-s-privacy-issues-its-responses-n859651 (last accessed: July 21st, 2023).

[5] ECJ, Jun 5th, 2018, C-210/16, available at: https://curia.europa.eu/juris/document/document.jsf?text=&docid=204508&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=1367796 (last accessed: July 21st, 2023).

[6] ECJ, Jun 15th, 2021, C645/19, available at: https://curia.europa.eu/juris/document/document.jsf?text=&docid=242821&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=3204053 (last accessed: July 21st, 2023).

[7] Reuters, Feb 16th, 2018, available at: https://www.reuters.com/article/us-facebook-belgium/facebook-loses-belgian-privacy-case-faces-fine-of-up-to-125-million-idUSKCN1G01LG (last accessed: July 21st, 2023).

[8] NBC News, Olivia Solon and Cyrus Farivar, Apr 16th, 2019, available at: https://www.nbcnews.com/tech/social-media/mark-zuckerberg-leveraged-facebook-user-data-fight-rivals-help-friends-n994706 (last accessed: July 21st, 2023).

[9] Lexology, Oct 29th, 2018, available at: https://www.lexology.com/library/detail.aspx?g=f09a96e7-a338-4fde-b017-5ed6f42d75ce (last accessed: July 21st, 2023).

[10] TechCrunch, Sep 2nd, 2021, available at: https://techcrunch.com/2021/09/02/whatsapp-faces-267m-fine-for-breaching-europes-gdpr/ (last accessed: July 21st, 2023).

platform, rather than opening the links on users' web browser of choice. This means that Meta can monitor all user interactions, such as buttons and links clicked, text selections, screenshots, etc., through the in-app browser. Meta failed to disclose to users that it was tracking them this way.[11]

Over the years, there have been several incidents that compromised the personal data of millions of people. In June 2013, news broke of a bug that exposed the sensitive personal data of approximately 6 million Facebook users. The bug, which was related to the contact information archive, allowed the users' email addresses and phone numbers to be viewed by unauthorized individuals.[12]

Between 2013 and 2015, Facebook exposed data on 87 million users to the political consulting firm Cambridge Analytica. The company exploited a loophole in Facebook's API that enabled it to compile profile data not just from users who downloaded the app, but also from their friends' networks. Facebook knew Cambridge Analytica was misusing user data as far back as 2015, but refused to acknowledge any issues and did not take action until the media raised the heat in 2018.[13] In December 2022, Facebook agreed to pay €682 million as settlement in a lawsuit seeking damages.[14]

In September 2018, attackers breached Facebook's security, thereby accessing the entire contents of 50 to 90 million user profiles. A vulnerability in the 'View as' feature code allowed the attackers to view profile information that was private. According to Facebook, the issue went unnoticed for more than a year.[15] In March 2022, the DPC imposed a €17 million fine on Facebook for a string of data breaches from June until December 2018.[16]

In September 2019, hundreds of millions of phone numbers linked to Facebook accounts have been found on the dark web. The exposed server contained more than 419 million records of Facebook users.[17] Again, in December 2019, Facebook user data from approximately 267 million accounts was found on the dark web. The data included names, phone numbers, and Facebook IDs. Then, in March

---

[11] The Guardian, Aug 11th, 2022, available at: https://www.theguardian.com/technology/2022/aug/11/meta-injecting-code-into-websites-visited-by-its-users-to-track-them-research-says (last accessed: July 21st, 2023).

[12] Reuters, Jun 22nd, 2013, available at: https://www.reuters.com/article/net-us-facebook-security/facebook-admits-year-long-data-breach-exposed-6-million-users-idUSBRE95K18Y20130621 (last accessed: July 21st, 2023).

[13] The New York Times, Mar 17th, 2018, available at: https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html (last accessed: July 21st, 2023).

[14] DW, Dec 23rd, 2022, available at: https://www.dw.com/en/facebook-agrees-to-pay-725-million-settlement-for-security-breach/a-64201763 (last accessed: July 21st, 2023).

[15] TechCrunch, Apr 9th, 2019, available at https://techcrunch.com/2019/09/04/facebook-phone-numbers-exposed/ (last accessed: July 21st, 2023).

[16] Data Protection Commission, Mar 15th, 2022, available at https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-meta-facebook-inquiry (last accessed: July 21st, 2023).

[17] TechCrunch, Sep 4th, 2019, available at https://techcrunch.com/2019/09/04/facebook-phone-numbers-exposed/ (last accessed: July 21st, 2023).

2020, a second server was discovered that contained data on 42 million more users, bringing the total up to 309 million. Both servers were associated with the same criminal group.[18]

In 2020, Facebook mistakenly shared users' personal data with outside developers for a longer period of time than promised. The issue applied to apps from some 5,000 developers, but Facebook didn't disclose how many users have been affected.[19]

It is clear from the above examples that Meta does not respect its users' privacy at all.

The Facebook Data Breach

In April 2021, personal data of over 500 million Facebook users were leaked on a hacking forum,[20] including data of around 96.7 million EU/EEA citizens. The leaked data included full names, Facebook IDs, birthdays, phone numbers, locations, relationship statuses, account creation dates, other biographical information, and in some cases users' email addresses.[21]

Lack of appropriate security measures

Under the GDPR, personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organizational measures.

The data exposed by the Facebook Data Breach was allegedly obtained by exploiting a vulnerability that Meta purported it had rectified in August 2019. Despite being warned early in 2017 about "scraping" issues on the Facebook platform, Meta waited two years before taking action.[22] It is clear that Meta has - in violation of article 32 GDPR - implemented insufficient technical and organizational measures to prevent its platform and user data from being scraped. If Meta had fixed the vulnerabilities in its systems at the time, the Facebook Data Breach would not have occurred.

---

[18] Firewall Times, Michael X. Heiligenstein, Jan 18th, 2022, available at https://firewalltimes.com/facebook-data-breach-timeline/ (last accessed: July 21st, 2023).

[19] Fortune, Jul 2nd, 2020, available at https://fortune.com/2020/07/01/facebook-user-data-apps-blunder/ (last accessed: July 21st, 2023).

[20] Business Insider, Aaron Holmes, Apr 3rd, 2021, available at: https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4?international=true&r=US&IR=T (last accessed: July 21st, 2023).

[21] Risk & Compliance Platform Europe, Sep 8th, 2021, available at: https://www.riskcompliance.biz/news/foundation-somi-starts-collective-investigation-into-533-million-leaked-facebook-accounts/ (last accessed: July 21st, 2023).

[22] DataNews, Apr 20th, 2021, available at: https://datanews.knack.be/ict/nieuws/interne-mail-toont-hoe-facebook-veiligheidsproblemen-wil-normaliseren/article-news-1724927.html?cookie_check=1618912845 (last accessed: July 21st, 2023).

Scraping occurs more often, but Meta gave malicious actors a lot more personal data than other platforms. This was due to the Friends Lookup feature that could be exploited by searching random phone numbers and then showing whose name or profile they belong to.[23]

The Facebook Data Breach has left the victims very vulnerable. This matter is especially serious as the leak contains about 500 million phone numbers. Datasets containing names and phone numbers plus social media profile information offer a "treasure trove" for malicious actors to target people such as via phishing and social engineering techniques.[24] For this reason, SOMI has initiated a campaign to warn and protect the victims.

Data protection by design and default

Due to the flaws in Facebook's design, malicious actors were able to obtain data on Facebook users by using a contact importer feature. The design of this feature was insecure in that it allowed large sets of phone numbers to be uploaded, enabling malicious actors to find phone numbers that matched Facebook profiles and collate a massive dataset on individuals that was later found exposed online.

The Irish Data Protection Commission found that the design of the Contact Importer feature did not incorporate data protection principles embedded in Article 25(1) of GDPR requiring controllers to "implement appropriate technical and organizational measures... designed to implement data-protection principles" and Article 25(2) which further requires controllers to ensure that the data protection principles minimizing use, accessibility and the period of storage are in place by default. For this reason, the DPC announced a €265 million fine to Meta in November 2022.[25]

Failure to notify supervisory authority

In case of a personal data breach, the data controller is required to, without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

After publication of the stolen data of millions of users in April 2021, Meta chose not to notify this data breach to the supervisory authority, apparently because Meta believed the data had been stolen before the GDPR came into effect.

The Irish Data Protection Commission stated that it did not receive any proactive communication from Meta on the issue at the time of the leak in April 2021. Rather, the DPC had to approach Meta using a number of channels to try to obtain answers from the company.[26]

---

[23] DataNews, Jan 11th, 2017, available at: https://datanews.knack.be/ict/nieuws/facebook-lekt-telefoonnummer-jan-jambon/article-normal-800275.html (last accessed: July 21st, 2023).

[24] TechCrunch, Natasha Lomas, Jan 10th, 2023, available at: https://techcrunch.com/2023/01/10/digital-rights-ireland-gdpr-lawsuit-facebook-data-scraping-breach/ (last accessed: July 21st, 2023).

[25] Data Protection Commission, Nov 28th, 2022, available at: https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-in-facebook-data-scraping-inquiry (last accessed: July 21st, 2023).

[26] TechCrunch, Apr 6th, 2021, available at: https://techcrunch.com/2021/04/06/answers-being-sought-from-facebook-over-latest-data-breach/ (last accessed: July 21st, 2023).

Failure to communicate data subjects on personal data breach

When a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller is required to communicate the personal data breach to the data subjects without undue delay. This is clearly applicable to the Facebook Data Breach, in light of the potential for targeting people via phishing and social engineering using the data in the Facebook Data Breach.

Meta decided not to inform data subjects about the Facebook Data Breach in a timely and adequate manner and up until today, it does not have plans to do, as their spokesperson said to many news outlets.[27]

We note that the conduct of Meta regarding the Facebook Data Breach also constitutes unfair trade practices in the sense of the EU Unfair Trade Practices Directive.

Lawfulness of data processing

Article 6 of the GDPR requires a lawful ground for processing personal data. Meta processes personal data in order to serve personalized advertisements to its users.

When the GDPR became applicable on May 25th, 2018, Meta attempted to bypass the GDPR's stricter consent requirements by switching from consent to an alleged contract in the Terms of Service for Facebook as the legal ground for processing personal data for personalized advertisement purposes. By doing so, Meta implied that ads are a necessary part of the service that it contractually owes the users. The platforms' services would not be accessible if users declined to accept the updated Terms of Service.

By making the accessibility of its services conditional on users receiving personalized advertisements, Meta was in fact "forcing" the users to consent to the processing of their personal data for targeted advertising and other personalized services, which is in breach of the GDPR.[28]

The use of a contract as the basis for the lawfulness of processing personal data in this case violates GDPR Art. 6(1)(b), recital (40), EDPB Guidelines 2/2019[29], as well as earlier WP29 guidance on the subject. Recently, the European Court of Justice ruled that personalised content does not appear to be necessary for the performance of a contract between the user and Meta, nor does it appear to be necessary for the seamless use of Meta's group services.[30] The district court of Amsterdam came to the same conclusion when it ruled that processing personal data for personalized advertisements is

---

[27] Reuters, Apr 7th,2021, available at: https://www.reuters.com/article/us-facebook-data-leak-idUSKBN2BU2ZY (last accessed: July 21st, 2023).

[28] Data Protection Commission Ireland, Jan 4th, 2023, available at: https://www.dataprotection.ie/en/news-media/data-protection-commission-announces-conclusion-two-inquiries-meta-ireland (last accessed: July 21st, 2023).

[29] EDPB, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Adopted on Apr 9th, 2019, available at : https://edpb.europa.eu/sites/default/files/consultation/edpb_draft_guidelines-art_6-1-b-final_public_consultation_version_en.pdf.

[30] ECJ, July 4th, 2023, C-252/21, available at https://curia.europa.eu/juris/document/document.jsf?text=&docid=275125&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=3204576 (last accessed: July 21st, 2023).

not necessary for the performance of the contract between a user and Meta.[31] It is clearly possible to provide social media services without tracking and profiling of data subjects. Therefore, tracking or profiling is not necessary for the performance of that contract.[32]

The ECL also considered that, where Meta is currently relying on a legitimate interest (art. 6(1)(f) GDPR), as a legal ground for processing personal data for the purpose of personalized advertising, Facebook users cannot reasonably expect that their personal data are being processed for this purpose, and thus that such processing is not necessary and Meta can therefore not rely on this legal ground.[33]

As a result, Meta does not comply with the requirement of lawful processing of article 6 GDPR. Where Meta relies on consent as a ground for the purpose of, inter alia, serving personalised advertisements, Meta fails to meet the requirements of specific and informed consent. Additionally, the information provided in the app is insufficient for the users to provide informed consent. Again, the district court in Amsterdam recently came to the same conclusion.[34]

We note that the unlawfulness of Meta's data processing also constitutes unfair trade practices in the sense of the EU Unfair Trade Practices Directive.

In conclusion, Meta's processing of personal data for targeted advertising purposes has been unlawful since at least May 25th, 2018.

Lack of appropriate safeguards for data transfers

Data controllers that intend to transfer personal data to countries outside the EEA must ensure that the data subject is granted a level of protection essentially equivalent to that guaranteed by the GDPR. Failure to meet this requirement means that operators must suspend the transfer of personal data outside the EEA.

On October 6th, the Court of Justice of the European Union ('**ECJ**') declared the Safe Harbour between the EU and the US invalid. Transfers of personal data on the basis of that Safe Harbour agreement were then in principle invalid. The Safe Harbour agreement was subsequently replaced by the EU-US Privacy Shield.

In its July 2020 Schrems II judgment, the ECJ also declared the Privacy Shield Decision invalid on account of invasive US surveillance programs, thereby making transfers of personal data on the basis of the Privacy Shield Decision unlawful. Furthermore, the ECJ stipulated stricter requirements for the

---

[31] District Court of Amsterdam, Mar 15th, 2023, ECLI:NL:RBAMS:2023:1407, available at https://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBAMS:2023:1407 (last accessed: July 21st, 2023).

[32] Noyb, Nov 23rd, 2021, available at: https://noyb.eu/en/irish-dpc-removes-noyb-gdpr-procedure-criminal-report-filed (last accessed: July 21st, 2023).

[33] ECJ, July 4th, 2023, C-252/21, available at https://curia.europa.eu/juris/document/document.jsf?text=&docid=275125&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=3204576 (last accessed: July 21st, 2023).

[34] District Court of Amsterdam, Mar 15th, 2023, ECLI:NL:RBAMS:2023:1407, available at https://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBAMS:2023:1407 (last accessed: July 21st, 2023).

transfer of personal data based on standard contractual clauses ('**SCC's**'). The ECJ held that SCC's do not, per se, present lawful or unlawful grounds for data transfer. The ECJ also stipulated that data controllers or operators that seek to transfer data based on SCC's, must ensure that the data subject is offered a level of protection essentially equivalent to that guaranteed by the GDPR.

Meta has in the past relied on a combination of the Safe Harbour Agreement, the EU-US Privacy Shield and SCC's. Currently, Meta relies only on SCC's for data transfers outside of the EEA.

However, it is unclear to what extent Meta has provided the necessary 'additional safeguards' in line with EDPB recommendations 01/2020[35] on measures that supplement transfer tools. It remains unclear how Meta would be able to provide essential equivalence to the levels of protection provided within the EU. This is especially true for Facebook, since the company's own data transfers were at the heart of the ECJ cases.[36] SOMI takes the position that in light of the sweeping US surveillance programs, no adequate additional safeguards as required under the GDPR have been taken by Meta.

Claims and damages

In view of all of the above, there have been and still are ongoing serious and large-scale violations of data subject privacy rights and corresponding breaches of the GDPR and the EU Unfair Trade Practices Directive and the Dutch implementation thereof. These practices prompt SOMI and its participants to file this complaint, which may be amended or extended depending on the outcome of our discussions with Meta.

Considering the above, SOMI intends to initiate collective proceedings on behalf of all persons in the Netherlands that have used Meta's services after 25 May 2018, in which it will claim, inter alia:

a) Declaratory judgements that Meta has violated and continues to violate the above-mentioned provisions of law;

b) Orders for Meta to cease and desist its violations of the above-mentioned provisions of law and its unlawful conduct, inter alia by (i) informing all Dutch Users affected by the Facebook Data Breach of the existence and the potential impact of the Facebook Data Breach, (ii) implementing measures to better safeguard the privacy of its users, (iii) making sure that it obtains valid consent from each and every Dutch User for processing their personal data for purposes of personalized advertising, (iv) reorganising and rewriting its legal and data protection documentation, and (v) by ceasing the transfer of personal data to third countries without appropriate measures in place;

c) Immaterial damages to the amount of €500 for each Dutch User. The total amount in damages is estimated at € 5,000,000,000, based on 10 million Dutch Facebook users in 2022.

---

[35] EDPB, recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0, Adopted on 18 June 2021, available at : https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf (last accessed: July 21st, 2023).

[36] Politico, Despite EU court rulings, Facebook says US is safe to receive Europeans' data, available at : https://www.politico.eu/article/despite-eu-court-ruling-facebook-says-us-is-safe-to-receive-europeans-data/ (last accessed: July 21st, 2023).

b) Orders for Meta to cease and desist its violations of the above-mentioned provisions of law and its unlawful conduct, inter alia by (i) informing all Dutch Users affected by the Facebook Data Breach of the existence and the potential impact of the Facebook Data Breach, (ii) implementing measures to better safeguard the privacy of its users, (iii) making sure that it obtains valid consent from each and every Dutch User for processing their personal data for purposes of personalized advertising, (iv) reorganising and rewriting its legal and data protection documentation, and (v) by ceasing the transfer of personal data to third countries without appropriate measures in place;

c) Immaterial damages to the amount of €500 for each Dutch User. The total amount in damages is estimated at € 5,000,000,000, based on 10 million Dutch Facebook users in 2022.

d) In addition, immaterial damages to the amount of €1,000 for each Dutch User affected by the Data Breach.

We note that we explicitly reserve the right to file additional claims, including claims for material damages of the Dutch Users.

Invitation to discuss an amicable solution

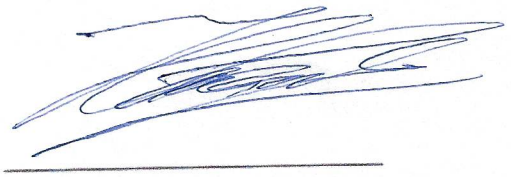
We are aware that not all claims and legal grounds have been fully substantiated in the above. This letter should however provide Meta with sufficient information to assess whether it is willing to enter discussions with SOMI on a possible amicable solution.

We kindly request you to inform us, **within fourteen days of receiving this letter**, whether Meta is prepared to enter good faith and meaningful discussions on the matters indicated above, including on its willingness to compensate the immaterial damage suffered by Dutch Users. Please note that this invitation is made in the context of article 3:305a(3)(c) DCC.

In the absence of a timely and sufficiently affirmative response to this letter by Meta, SOMI reserves the right to take legal action without further notice.

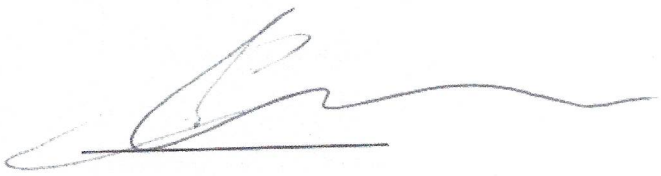
SOMI is looking forward to your response.

Yours sincerely,



Mr. Drs. H.J.M.G. Franke

SOMI



Dr. C.A.M. Wijtvliet

SOMI