noyb
Goldschlagstraße 172/4/3/2
1140 Vienna
AUSTRIA

FORBRUKERRÅDET

To:
Datatilsynet
P.O. Box 458 Sentrum
NO-0105 Oslo
NORWAY

Vienna, 06.06.2024

noyb case number:	**C081-01**
Complainant:	[redacted] [redacted] Norway
Represented under Article 80(1) GDPR by:	***noyb* – European Center for Digital Rights** Goldschlagstraße 172/4/3/2, 1140 Vienna, Austria
Respondent:	**Meta Platforms Ireland Limited** Merrion Road, Dublin 4, D04 X2K5, Dublin, Ireland
Regarding:	The use of personal data for undefined forms of "artificial intelligence technology" and the consequent violation of Articles 5(1) and (2), 6(1), 9(1), 12(1) and (2), 13(1) and (2), 17(1)(c), 18(1)(d), 19, 21(1) and 25 GDPR

COMPLAINT

This complaint is filed by *noyb* - in cooperation with Forbrukerrådet (Norwegian Consumer Council).

OVERVIEW

Given the short time since Meta has introduced its changes to irreversibly ingest the entire data sets of more than 400 million EU/EEA data subjects for undefined "artificial intelligence" technologies, without any indication as to the purposes of such systems, we see the urgent need to file this complaint.

Meta appears to violate at least Articles 5(1) and (2), 6(1) 6(4), 9(1), 12, 13, 17(1)(c), 18, 19, 21(1) and 25 GDPR. At its core this complaint relies on the following elements:

- *First*, Meta has **no legitimate interest** under Article 6(1)(f) GDPR that would override the interest of the complainant (or any data subject) and no other legal basis to process such vast amounts of personal data for totally undefined purposes.

- *Second*, Meta actually attempts to get permission to process personal data for **undefined, broad technical means** ("*artificial intelligence technology*") **without ever specifying the purpose** of the processing under Article 5(1)(b) GDPR.

- *Third*, Meta has taken every step to **deter data subjects from exercising their right to choose** by pretending that data subjects would only enjoy a right to object ("*opt-out*") instead of relying on consent ("*opt-in*") and by entertaining **extensive dark patterns** to deter users from objecting under Article 21 GDPR.

- *Fourth*, Meta **fails to provide the necessary** "*concise, transparent, intelligible and easily accessible*" **information**, "*using clear and plain language*".

- *Fifth*, Meta says itself that it is **not able to properly differentiate** (i.) between data subjects where it can rely on a legal basis to process personal data and other data subjects where such a legal basis does not exist and (ii.) between personal data that falls under Article 9 GDPR and other data that does not.

- *Sixth*, Meta says itself that the **processing of personal data is irreversible** and it is unable to comply with the "right to be forgotten" once personal data of the complainant is ingested into (unspecified) "artificial intelligence technology".

As a consequence, and given that Meta itself claims that the processing of the complainant's personal data **cannot be reversed after 26.06.2024**, we apply (see chapter 3. below) that you take (among others) the following urgent action:

- *First*, issue an **urgency decision under Article 66 GDPR** to prevent the immanent processing of the personal data of the complainant – and 300 million EU/EEA residents without consent by these data subjects.

- *Second,* **fully investigate the matter** under Article 58(1) GDPR.

- *Third*, **prohibit the use of personal data for undefined "artificial intelligence technology"** without the opt-in consent from the complainant – and indeed other data subjects.

TABLE OF CONTENTS

1. FACTS OF THE CASE

The following is a short summary of facts at the time of the filing of this case. These facts may be supplemented by additional information that may arise during the next weeks and the course of the investigation:

1.1. Likely agreement with the Irish Data Protection Commission

Meta has publicly stated that the following violations of the GDPR arise from an agreement with the Irish Data Protection Commission (DPC) as their lead supervisory authority:

> *"Meta delayed the launch following a number of enquiries from the DPC which have been addressed. Meta is now giving users a jewel notification, additional transparency measures (AI privacy centre articles), a dedicated objection mechanism, 4 weeks from notification to users to date of initial training so there is now a time between notification and training.*
>
> *Meta has advised the DPC that only that personal data (posts not comments) shared by users based in the EU to a public audience on Instagram and Facebook at the time of training will be used and that this will not include personal data from accounts belonging to users under 18."*[1]

We note that Article 57(1)(d) GDPR foresees the promotion of general awareness, but does not foresee such upfront "*agreements*" with the regulator that is later likely also the decision maker. Meta's conduct also does not appear to be based on any such agreements with other CSAs or the EDPB.

We also note that Meta's processing operations seems to be in breach of the previously issued **EDPB Decisions 3/2022** (on Facebook) and **EDPB Decision 4/2022** (on Instagram), both of which the DPC remains resistant to implementing (see the DPC's lawsuit against the EDPB before the General Court).[2]

1.2. Meta's changes by 26.06.2024

1.2.1. Changes to the privacy policy

Meta has updated its privacy policy, available at https://www.facebook.com/privacy/policy where users have to click on a link to the new policy.

The new policy is planned to go into effect on 26.06.2024. Meta has not provided a "redline" or other comparison document that allows any data subject to quickly understand the changes.

As far as we were able to see, the term "artificial" or "AI" is mentioned only under three headings in the privacy policy that amounts to 127 pages A4 if printed,[3] namely:

- **In the intro section:**
  - The intro now reads: "*We're updating our Privacy Policy, including how we use your information for AI at Meta.*"

[1] One of many press releases at https://www.thejournal.ie/facebook-data-ai-6391876-May2024/

[2] General Court, Case T-70/23.

[3] Based on the new version, if the "printable version" is chosen and printed via a Firefox browser.

- **Under the heading "*How do we use your information*?" (defining the <u>purpose</u>):**
  - Where under the subheading "*Researching and innovating for social good*", the policy now says: "*We support research in areas like artificial intelligence and machine learning.*"
- **Once in a table headed "Performance of a contract" (defining the <u>legal basis</u>):**
  - Where the policy now reads: *"Provide and curate artificial intelligence technology in our Products, enabling the creation of content like text, audio, images and videos, including by understanding and recognising your use of content in the features."*
- **Six times, in a table headed "Legitimate Interests" (defining the <u>legal basis</u>):**
  - Here the policy now reads: "*To develop and improve artificial intelligence technology (also called AI at Meta) we provide, on our Products and to Third Parties*."
  - Further down, the policy now reads: *"We support research in areas like artificial intelligence and machine learning."*

➔ *The updated privacy policy (of 124 printed pages) does not allow a normal data subject to understand the actual use of his or her personal data. We note that this description seems to be extremely vague and even conflicting.*

➔ *In particular, the added wording on the purposes ("innovating for the social good") and the adjusted wording on the legal basis (indicating the use of personal data for undefined "artificial intelligence technology" in the interest of the Meta and third parties) are conflicting.*

1.2.2. Use for undefined "artificial intelligence technology"

Meta informs data subjects that their data will be used by undefined "*artificial intelligence technology*" - an extremely broad term describing an <u>undefined set of vaguely connected long-established, current and future technologies</u>.

The English Wikipedia alone lists <u>countless different techniques</u> that can be considered an "*artificial intelligence technology*" with vastly different applications and implications for data subjects. They include: Search and optimization, various forms of logic, probabilistic methods, classifiers and statistical learning, artificial neural networks, deep learning, generative pre-trained transformers (GPT), large language models (LLMs), machine learning, neural networks, Generative AI, face recognition, translation of texts, predictive technologies and many more.[4] Wikipedia defines "Artificial Intelligence" as *"in its broadest sense,* [the] *intelligence exhibited by machines, particularly computer systems*."[5]

> **Example:** While it may be less of an interference if a system is trained to understand speech (speech recognition) a data subjects may not be happy if their voice is used to generate a computer voice that resembles them ("voice clone") or if his or her data is used for credit ranking, ads, health predictions or to calculate insurance premiums.

Meta <u>does not disclose which type</u> of "*artificial intelligence technology*" it is intending to use personal data with – <u>let alone for which purpose</u>.

[4] See as an example: https://en.wikipedia.org/wiki/Artificial_intelligence. This random list in intended to show that there is no common understanding for what would constitute "*artificial intelligence technology*" and what does not.

[5] See https://en.wikipedia.org/wiki/Artificial_intelligence

1.3. Scope of processing

Meta's intended processing of personal data is exceptionally broad. It is also highly questionable whether Meta is able to properly separate personal data that (i.) falls under Article 6(1)(f) GDPR, (ii.) falls under the application of the GDPR and (iii.) falls under successful objection under Article 21 GDPR.

The exact processing is a matter for further investigation by the authorities under Article 58(1) GDPR and the information below is naturally a preliminary summary:

1.3.1. No limitation based on the type of personal data

Meta does not currently limit the amount or the type of personal data that may be used to train AI systems. Under "*Where does Meta get training information?*", Meta says:

> *"Since it takes such a large amount of data to teach effective models, a combination of sources are used for training. We use information that is publicly available online and licensed information. We also use information shared on Meta's Products and services. This information could be things like posts or photos and their captions. We do not use the content of your private messages with friends and family to train our AIs. There are more details on how we use information from Meta's Products and services in our Privacy Policy.*
>
> *When we collect public information from the internet or license data from other providers to train our models, it may include personal information. For example, if we collect a public blog post it may include the author's name and contact information. When we do get personal information as part of this public and licensed data that we use to train our models, we don't specifically link this data to any Meta account."*[6]

There is only one (tiny) exemption to the sweeping claims by Meta, namely "private messages" between two individual users. It is worth noting that any other form of private communication, like chats with a business, a Facebook page or within a closed Facebook group does not seem to be covered by this exception.

➔ *In other words,* ***any data on Meta platforms*** *and* ***any data off-Meta platforms*** *(other than individual-to-individual chats)* ***may be used*** *for the processing operations.*

1.3.2. No limitation for "specific purposes" as required by Article 5

Meta also does not limit the purpose for which these AI systems may be used in the future, as it simply declares the development of AI systems itself as the purpose of the processing operation. There is no differentiation between the following examples:

- An AI system to detect bots, illegal behaviour and the like (*security*)
- An AI system that allows users to interact and answer questions ("*assistant*")
- An AI system to help improve uploaded pictures by users ("*photo filters*")
- An AI system to help find more relevant information in the newsfeed (*personalization*)
- An AI system for external credit ranking companies ("*credit ranking*")

[6] See https://www.facebook.com/privacy/genai/

- An AI system for companies to make hiring decisions ("*automated decision making*")
- An AI system to allow advertisers to exploit users' weaknesses ("*psychological ads*")
- An AI system to allow political parties to influence elections ("*political influence*")
- An AI system to allow the government to find potential future criminals
- An AI system can be used for self-driving cars, but also military drones
- An AI system tasked with the creation of as many paper clips as possible[7]

➔ *Obviously, this list is just a random example, but it shows that* ***Meta is trying to make an entire group of data processing technologies itself the alleged "purpose"*** *under Article 5(1)(b) GDPR. Usually technologies are not a purpose, but "means" in GDPR.*

1.3.3. No time limit, allowing use of very old personal data

We note that Meta has not proposed any limitation on the age of the training data. Meta seems to try to use its many "dormant" accounts as a source for personal data, when the user may not even be aware of or reacting to messages concerning Meta. This allows Meta to generate revenue even from data subjects that have not substantially used the service in years ("data recycling"). Such data should usually have been subject to deletion routines under Article 5(1)(e) GDPR, which Meta has never implemented.

1.3.4. No anonymisation or pseudonymisation of personal data

We note that Meta does not even claim to foresee that personal data is minimised or limited in any way, shape or form.

Most notably, the GDPR usually foresees processes like anonymisation or (at least) pseudonymisation as approaches to implement requirements under Article 5 GDPR or to comply with the duty to have "*data protection by design and by default*".

None of the documents that Meta provided to the complainant contain any hint, let alone clear legal undertaking, in that direction.

1.3.5. Forwarding of personal data to any "third party"

Meta also does not limit the use of personal data (that will be contained in any AI model) to internal use by Meta or within the Meta products, but explicitly foresees that any "*artificial intelligence technology*" may also be provided to "*third parties*":

> *"To develop and improve artificial intelligence technology (also called AI at Meta) we provide, on our Products and to Third Parties."*[8]

[7] See https://en.wikipedia.org/wiki/Instrumental_convergence#Paperclip_maximizer

[8] See https://www.facebook.com/privacy/policy/version/25238980265745528

Meta's wording also explicitly foresees that third parties may "*discover … information*" via its artificial intelligence technology:

> *"To create, provide, support and maintain artificial intelligence technology that enables people, businesses, and others to express themselves, communicate, and discover and engage with information relevant to their interests."*[9]

While Meta has some information pages, that e.g. name specific third parties for "Generative AI models",[10] this is not reflected in the (legally relevant) privacy policy.

➔ *Overall, the setup makes it clear that Meta anticipates that **personal data of** the complainant and all other **4 billion Meta users may be provided to any "third parties"** via Meta's AI systems.*

➔ *Obviously "third parties" is a euphemism for **"anyone in the world".***

1.3.6. Summary: No limitation on the processing operations

In summary, Meta's description of the processing operation foresees none of the typical limitations for the processing of personal data. It seems that Meta is trying to use the current hype around AI technology and the lack of understanding about it to "slip through" processing operations that would otherwise never be tolerated.

➔ *Meta foresees the use of any personal data (on Meta or from a third party), for any purpose (by just declaring "AI" to be the "specific purpose"), with no time limit, with no form anonymisation or pseudonymisation and potentially with anyone in the world as the recipient of information from these systems.*

1.4. Foreseeable technical problems in Meta's implementation

Based on Meta's own submissions in other GDPR related cases, it is obvious that the proposed approach by Meta to have a proper and clear legal basis for any individual piece of information is not achievable in the way Meta is currently conducting the processing.

1.4.1. Lack of separation between data subjects that agree and/or object

The functioning of a social network, where data is often shared or mixed, would usually mean that any objection would (technically) not apply to data that is not directly linked to an account. Meta itself explains that it cannot separate personal data of (non-)users from users of its services:

> *"Even if you don't use our Products and services or have an account, we may still process information about you to develop and improve AI at Meta. For example, this could happen if you appear anywhere in an image shared on our Products or services by someone who does use them*

[9] See https://www.facebook.com/privacy/policy/version/25238980265745528

[10] See https://www.facebook.com/privacy/dialog/ai-partners/

> *or if someone mentions information about you in posts or captions that they share on our Products and services."*[11]

Equally, Meta admits in the opt-out form that it cannot really separate the personal data from people that opted out from the personal data of other users:

> *"We may still process information about you to develop and improve AI at Meta, even if you object or don't use our Products and services. For example, this could happen if you or your information:*
> *- Appear anywhere in an image shared on our Products or services by someone who uses them*
> *- Are mentioned in posts or captions that someone else shares on our Products and services"*[12]

The same technical limitation obviously applies to the use of personal data of various users of the service, such as when a user that objected is in a picture that was uploaded by a user that did not object.

1.4.2. Lack of separation between personal data under Article 6 and 9

Even when it comes to the personal data of a specific data subject, Meta has long maintained that it is technically unable to differentiate between personal data falling under Article 6 GDPR and so-called "sensitive" data, that is protected by Article 9 GDPR.

In fact, Meta is currently facing litigation before the CJEU in C-446/21 *Schrems*, where Meta has submitted that it "*does not separate*" between special categories of data in accordance with Article 9 GDPR and other categories of data and would therefore be unable to comply with Article 9 GDPR.

Given that Meta is repeatedly on record stating that it does not separate between data falling under Article 9 GDPR and other personal data – even before the CJEU – it seems probable that such differentiation would also be lacking when user data is used to train an AI model. The same problem also applies to personal data covered by Article 10 GDPR.

As explained in more detail below, Article 9 GDPR does not foresee the use of special categories of personal data for "*legitimate interests*", but such personal data would nevertheless be used to train Meta's AI systems under the same legal basis too.

1.4.3. Lack of separation between EU/EEA personal data and other data

Furthermore, Meta has repeatedly argued that its data processing is a unified global system and cannot be "*separated*". In litigation on EU-US data transfers (see EDPB Decision 1/2023), Meta has, for instance, argued the following:

- [redacted] ("Confidential" Report of [redacted] on behalf of Facebook Ireland Ltd of 24.09.2021) or
- [redacted] (see paragraph 8 [redacted] 12

[11] See https://www.facebook.com/privacy/genai/

[12] See https://help.instagram.com/contact/233964459562201 (for Instagram) and https://www.facebook.com/help/contact/6359191084165019 (for Facebook).

of the "confidential" Annex I '[redacted], not dated)

Based on Meta's own submissions, we therefore certain that Meta is technically unable to have a "clean cut" between personal data that falls under the scope in Article 3 GDPR and personal data of users that may not be subject to the GDPR (e.g. non-EU/EEA users).

For the complainant, this means that no matter if an objection is filed and approved, it is highly likely that personal data is still processed.

➔ *Meta itself says that it cannot properly separate EU/EEA personal data from other personal data. It seems highly questionable that Meta can properly apply limitations to all EU/EEA data subjects on globally interconnected social networks.*

1.5. Personal data cannot be "forgotten" from an AI system

As already apparent from other artificial intelligence systems like Large Language Models that are based on artificial neural networks (see, e.g., the *noyb* complaint on OpenAI),[13] personal data that is once entered into an AI system cannot (according to the controllers) be "unlearned", "forgotten", deleted or rectified.

Meta itself says that any future objection would not influence the use of personal data that the system was already trained on:

> *"We'll review objection requests in accordance with relevant data protection laws. If your request is honored, it will be applied going forward."*[14]

It therefore seems likely that an "objection" after 26.06.2024 will not have the effect that personal data is not processed within the LLM anymore – contrary to the obligations under Article 17 GDPR ("*right to be forgotten*"). This irreversible approach by controllers is not just a violation of the GDPR, but an additional factor that gravely undermines the rights and freedoms of data subjects.

➔ *Meta itself says that GDPR rights cannot be complied with after 26.6.2024 and any exercise of rights may not stop the further processing of personal data that was already used as training data.*

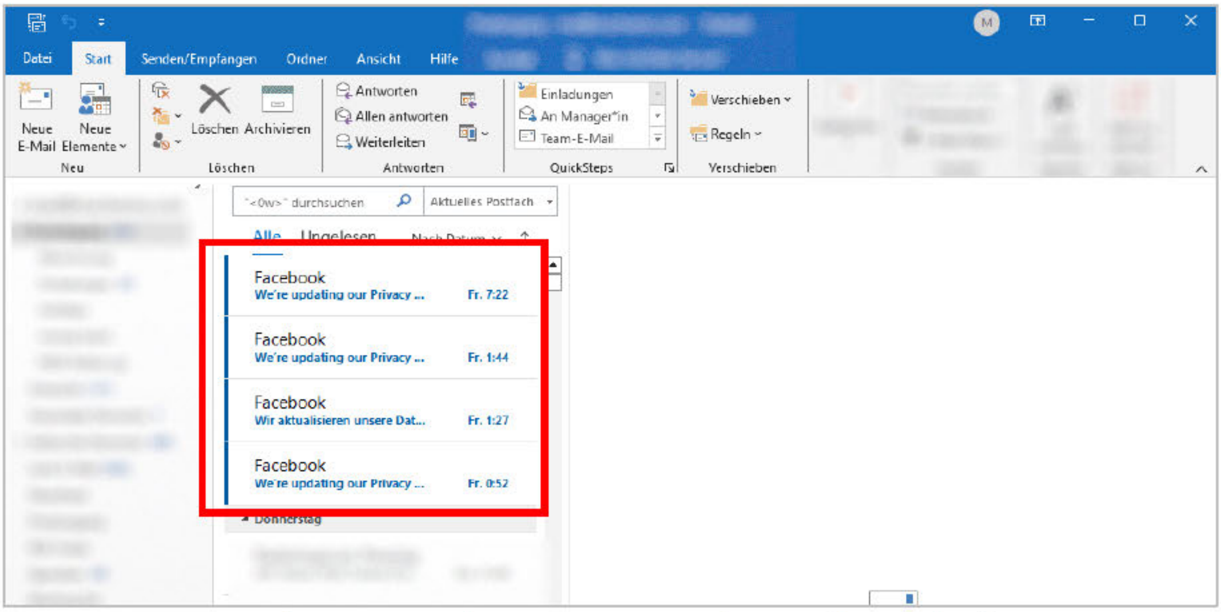
[13] See e.g. https://noyb.eu/sites/default/files/2024-04/OpenAI%20Complaint_EN_redacted.pdf
[14] See objection form at https://www.facebook.com/help/contact/6359191084165019

1.6. Information to the complainant via email

Article 12 GDPR requires information in "*concise, transparent, intelligible and easily accessible form, using clear and plain language*" and requires controllers to "*facilitate the exercise of data subject rights under Articles 15 to 22*". Meta has done exactly the opposite:

1.6.1. Deceptive subject line with no hint on AI or the right to object (CTA)

The complainant was notified about changes via an email with the subject "*We're updating our Privacy Policy as we expand AI at Meta*".



Facebook
We're updating our Privacy ... Fr. 7:22

Facebook
We're updating our Privacy ... Fr. 1:44

Facebook
Wir aktualisieren unsere Dat... Fr. 1:27

Facebook
We're updating our Privacy ... Fr. 0:52

Screenshot: Meta emails as seen in a normal Microsoft Outlook inbox

In most email programs only "*We are updating our Privacy…*" would be visible. It is basic knowledge in email marketing that the first 2-3 words of an email subject line are the principal factors determining whether emails are opened. As a result, the relevant "*call to action*" (CTA) should always be apparent from the first 2-3 words.[15]

Meta's subject line alone indicates that this email is not worth reading, as privacy policies are updated all the time – especially if a user has not visited the page within the last week and is therefore likely a rather inactive user.

➔ *The first 2-3 words and a clear "call to action" in a subject line is known to be the main factor why emails are even opened by users.*

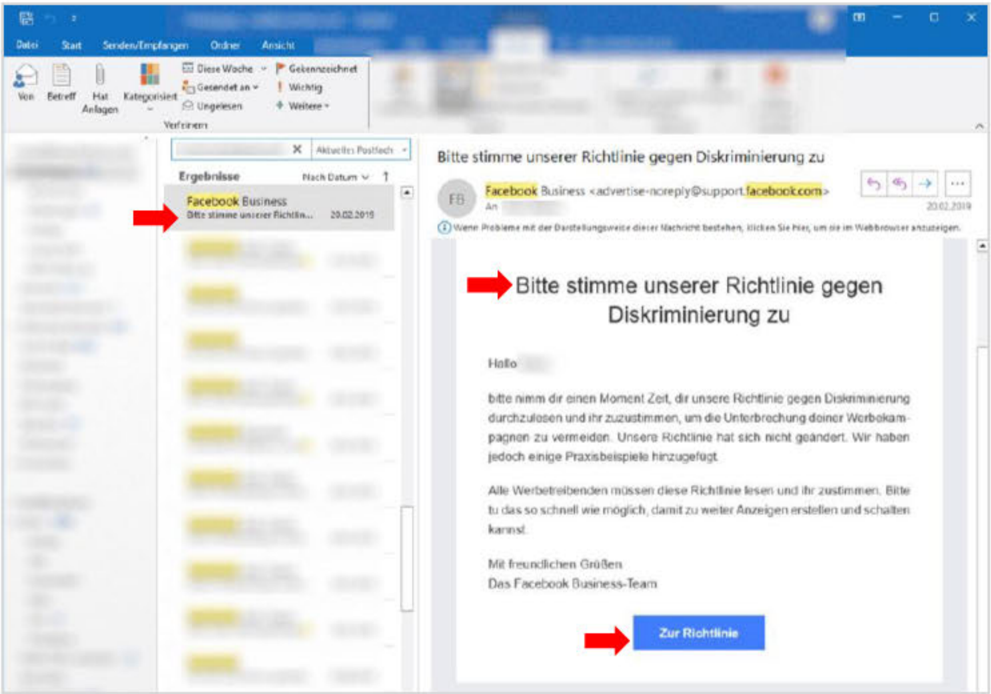
➔ *Meta has not included any relevant elements into the first words of the subject line.*

➔ *Meta is fully aware of this factor, given that all other communication by Meta follows these basic design principles.*

[15] As one of many examples: https://mailchimp.com/de/help/best-practices-for-email-subject-lines/

1.6.2. *No "call to action" (CTA) in the email – contrary to other Meta emails*

Usually, Meta sends emails with a clear graphical "*call to action*" (CTA), usually in the form of a big blue button, highlighting the option for a user to interact or choose something:



Bitte stimme unserer Richtlinie gegen Diskriminierung zu

Facebook Business <advertise-noreply@support.facebook.com>
An [redacted]
20.02.2019

Wenn Probleme mit der Darstellungsweise dieser Nachricht bestehen, klicken Sie hier, um sie im Webbrowser anzuzeigen.

Bitte stimme unserer Richtlinie gegen Diskriminierung zu

Hallo [redacted]

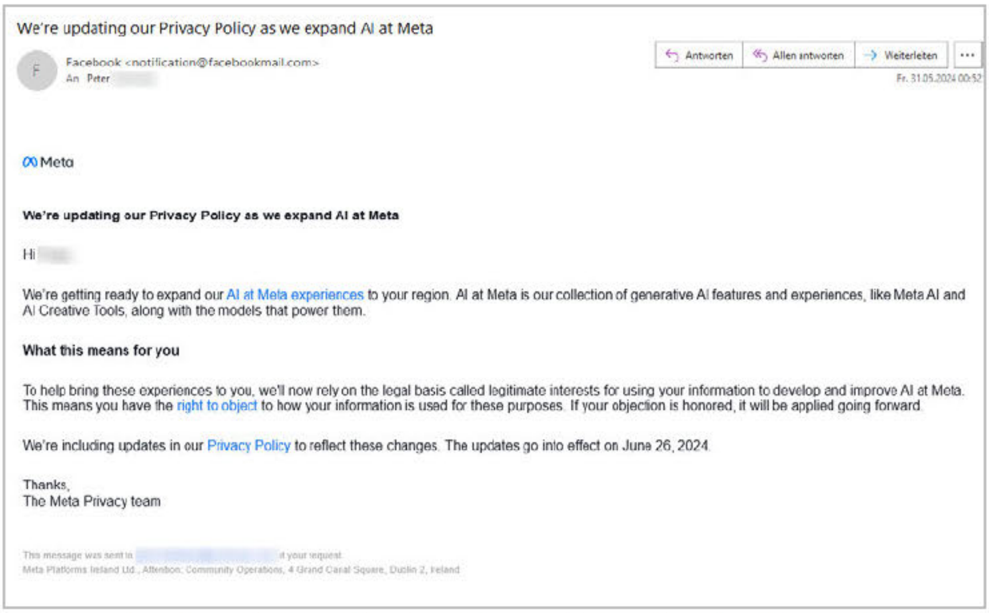
bitte nimm dir einen Moment Zeit, dir unsere Richtlinie gegen Diskriminierung durchzulesen und ihr zuzustimmen, um die Unterbrechung deiner Werbekampagnen zu vermeiden. Unsere Richtlinie hat sich nicht geändert. Wir haben jedoch einige Praxisbeispiele hinzugefügt.

Alle Werbetreibenden müssen diese Richtlinie lesen und ihr zustimmen. Bitte tu das so schnell wie möglich, damit zu weiter Anzeigen erstellen und schalten kannst.

Mit freundlichen Grüßen
Das Facebook Business-Team

Screenshot: Meta marketing email with clear CTAs in subject (German for "Please agree to our guidelines against discrimination"), headline and with blue button.

The email sent to exercise the right to object under Article 21 GDPR did not have any such common CTA, but instead an in-line text link, usually used for further information — not for a user action or choice, which is commonly communicated via a button (see above).



We're updating our Privacy Policy as we expand AI at Meta

Facebook <notification@facebookmail.com>
An Peter [redacted]
Fr. 31.05.2024 00:52

We're updating our Privacy Policy as we expand AI at Meta

Hi [redacted]

We're getting ready to expand our AI at Meta experiences to your region. AI at Meta is our collection of generative AI features and experiences, like Meta AI and AI Creative Tools, along with the models that power them.

What this means for you

To help bring these experiences to you, we'll now rely on the legal basis called legitimate interests for using your information to develop and improve AI at Meta. This means you have the right to object to how your information is used for these purposes. If your objection is honored, it will be applied going forward.

We're including updates in our Privacy Policy to reflect these changes. The updates go into effect on June 26, 2024.

Thanks,
The Meta Privacy team

This message was sent to [redacted] at your request.
Meta Platforms Ireland Ltd., Attention: Community Operations, 4 Grand Canal Square, Dublin 2, Ireland

Screenshot: Meta GDPR notification with no CTAs in subject, headline or a button.

➔ *The lack of a "call to action" is known to be another major reason why users "drop off" in a user engagement flow. Meta therefore (otherwise) always communicates clearly.*

1.6.3. Meta's email links are aimed to block access to information and the right to object

Even though the information about the opt-out was delivered to the email address with which the user can even get a new password (so the most "secure" channel Meta entertains) and the link in the email contained a "token" that identified the data subject, these tokens were not used to allow the data subject to identify itself.

Instead, the tokens were actually used to demand unnecessary extra login steps, even when visiting an otherwise publicly available website.

Information links used in Meta's emails had the following structure:

> https://www.facebook.com/n/?privacy%2Fgenai%2F&entry_point=notification&aref=1717109508947928&medium=email&mid=619b36cbc3d06G5af49c00df46G619b3b6523fd8G8151&n_m=[email_address]&rms=v2&irms=true

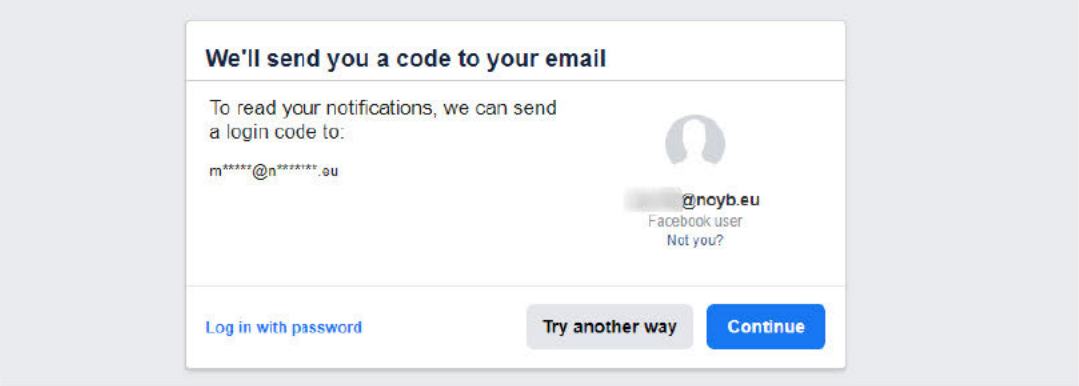
Objection links used in Meta's emails had the following structure:

> https://www.facebook.com/n/?help%2Fcontact%2F6359191084165019&aref=1717137977463652&medium=email&mid=619ba0d975092G5af4aca38af4G619ba572d5364G8151&n_m=[email address]&rms=v2&irms=true

The email links had the following elements:

Value Name	Value	Description
http://...&	URL of objection form	The text until the first "&" is the link to the objection form, the rest refer to tokens/values
entry_point	notification	Likely a tracking token on where a user entered the page
aref	1717137977463652	Likely a link reference ("a" as in <a>")
medium	email	Type of contact (here, via email)
mid	619ba0d975092G5af4aca38af4G619ba572d5364G8151	Unknown, likely a user ID or ID of the email that was sent to the user ("M*ID*")
n_m	[email address]	The email address of the user account
rms	v2	Unknown
irms	boolean (true / false)	Unknown

If a user clicked on the link in the email without being logged in, Meta was able to know the user's email address, given that the personalized link above was actually transferring all necessary data to link an objection with the user account:



We'll send you a code to your email

To read your notifications, we can send a login code to:

m*****@n*******.eu

[redacted]@noyb.eu

Facebook user

Not you?

Screenshot: Personalized login request, showing the email of a noyb staffer when clicking the objection link in a "clean" browser. Login and entry of email still required in next steps.

While these tokens show that Meta was actually personalizing links and had the technical options, it did not use them to make the objection easier - via a single click (like “unsubscribe” links in all newsletters which are an equivalent objection under Article 21(2) GDPR, which have the user ID, email address or a unique token encoded in the link).

➔ *Meta did not provide a single click opt-out (similar to “unsubscribe” links).*

In more detail on the “information link”:

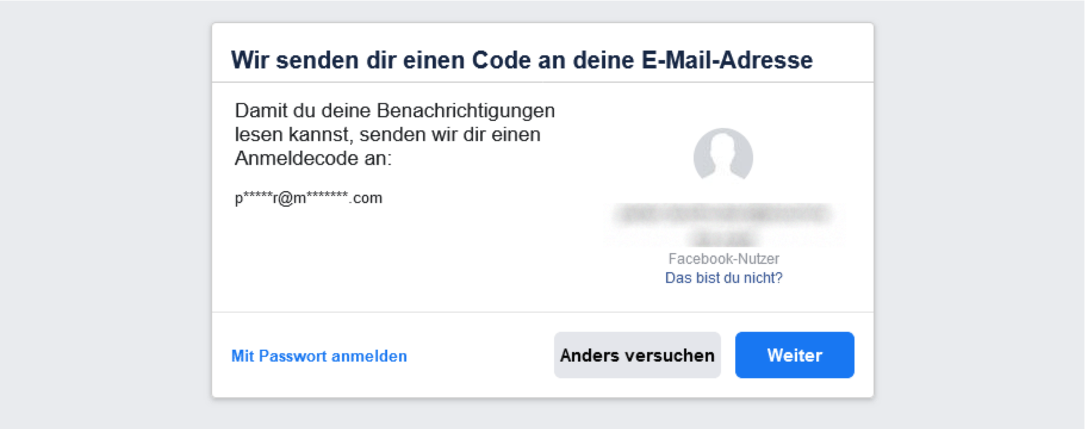
The information email had a link to the general information about Meta’s new AI systems at https://www.facebook.com/privacy/genai/.

However, if the link from the email is used, the additional tokens (see above at 1.6.3) lead to the system showing a “login page” (same as in the screenshot above) – requiring another login to even see privacy information, which is otherwise publicly available.

Data subjects were forwarded to a URL like the following instead of the information page:

> https://www.facebook.com/recover/initiate/?privacy_mutation_token=eyJ0eXBlIjo1LCJjcmVhdGlvbl90aW1***&cuid=[encryped email or phone number of user]&ars=bypass_login_deny_smart_recommendation&ram=email&lara_product=lara_bypass_login_fail_loop

The page seen by the user was equivalent to the page screenshot under 1.6.3 above:



Wir senden dir einen Code an deine E-Mail-Adresse

Damit du deine Benachrichtigungen lesen kannst, senden wir dir einen Anmeldecode an:

p*****r@m*******.com

[redacted]

Facebook-Nutzer

Das bist du nicht?

Screenshot: Login request when the information page was visited via the link sent to a noyb test account.

➔ *Meta required an additional login just to read the basic information about the changes to the privacy policy on an otherwise public page.*

In more detail on the “objection link”: No “one click” option

Usually controllers implement “one click” option e.g. to give consent, but also to unsubscribe from a newsletter. This is done via exactly such tokens as in the Meta link above, by providing a “token” that codes for the specific data subject and allows the server to know (with one click) that a specific user has unsubscribed or consented. There is then no need to log in to exercise GDPR rights.

Despite the technical possibility to have a "one click" objection, Meta has also asked users to log in (see screenshot at 1.6.3 above) when they wanted to submit an objection.

Especially as users may get the email on a device (desktop versus phone) or medium (browser versus app) that is different from their normal use of the Meta services, many users would likely have to find the password to login, which they never need after setup when just opening the app. This need to login thus further disincentivised the objection.

➔ *Despite having the technical means to have a "one click" objection (like a newsletter "unsubscribe"), Meta has instead used these technical means to require another login.*

➔ *Logins are known to be another major reason why users "drop off" in a flow.*

1.6.4. Requirement to go back and click on the link in the email again

After they logged in, as Meta required to access the objection form, data subjects were not shown the form but were instead forwarded to the "newsfeed".

Data subjects therefore had to go back to the email and click the link a second time (while now being logged in) to even reach the form.

➔ *The flow dropped the data subject to a page other than the objection form.*

1.7. Deceptive online form to exercise a right to object

Meta's excessive use of "dark patterns" to minimize the number of data subjects that would exercise their right to object also continued on the online form:

1.7.1. Requirement to provide wholly irrelevant personal data

While Article 12(2) GDPR requires that controllers "*facilitate*" the exercise of rights — including the right to object under Article 21 GDPR — and Article 5(1)(c) GDPR requires data minimisation, Meta seems to have designed the objection form with the intent of discouraging data subjects by requiring totally irrelevant information:

Re-entry of known & irrelevant country details

In order to object, the user needed to be logged in to allegedly confirm that he or she resides in a country that has a right to object – from the login Meta already knows that a data subject has the right to object.[16]

Meta also says it is allocating a jurisdiction to each user account (as it maintains that EU/EEA users are controlled by Meta Platforms Ireland Limited while other users are controlled by Meta USA)[17] and Article 3 GDPR makes clear that any data subject whose data is processed by an EU/EEA entity falls under the GDPR. Therefore, Meta knows from each user account if they fall under the GDPR or not.

[16] If users are not logged in they saw a screen saying "*This form is only available to people in certain regions who have an active Instagram account. Make sure you log into your Instagram account and then try again*".

[17] See Meta Privacy Policy https://www.facebook.com/privacy/policy/?section_id=13-HowToContactMeta, section 'How to contact Meta with questions'.

For both reason, Meta did not need to know the exact country that a data subject resides in to process to the objection.

➔ *The mandatory selection of a country seems to have the sole purpose of discouraging data subjects from filling out the form.*

Re-entry of known and irrelevant email details

As shown above (see description of link tokens under 1.6.3 above), Meta already shares the email address with its systems when a data subject clicks on the link. In addition, Meta has an email address of every user on file (indeed the complainant got an email by Meta in the first place) and users have to log in to even reach the form. Thus, there is also no reason to have users type in the email address another time.

➔ *The mandatory entry of an email address seems to have the sole purpose of discouraging data subjects from filling out the form.*

Need to give reasons for the objection

While Article 21(1) GDPR allows controllers to demand "*grounds relating to his or her particular situation*" to process an objection, most data subjects will not know which grounds they have to argue here, as they are not lawyers and are unfamiliar with the concept of legitimate interests and the interplay of Article 6(1)(f) and 21 GDPR.

In addition, Meta has not disclosed their "legitimate interest" analysis under Article 6(1)(f) GDPR, which makes it (even for well-trained lawyers) impossible to know if a certain factor was indeed already taken into account or not and is therefore a "*ground relating to his or her particular situation*".

As described under 1.7.2. below, it seems wholly irrelevant what a data subject entered in this field – further showing that Meta only used this field as a deterrent.

➔ *The mandatory entry to give "reasons" seems to have the sole purpose of discouraging data subjects from filling out the form.*

1.7.2. Fake "review" process

Persons that did opt-out consistently reported that the objection were "approved" instantly – usually within a minute. In a test by *noyb,* objections with a specific ground under Article 21(1) GDPR like "*no reasons given*" were approved within 50 seconds. There are no public reports about objections that were not approved by Meta.

Overall, this indicates that the complicated form and the need to argue the objection was not required for a material review by Meta, but instead only served as a "dark pattern" to discourage data subjects from submitting an objection.

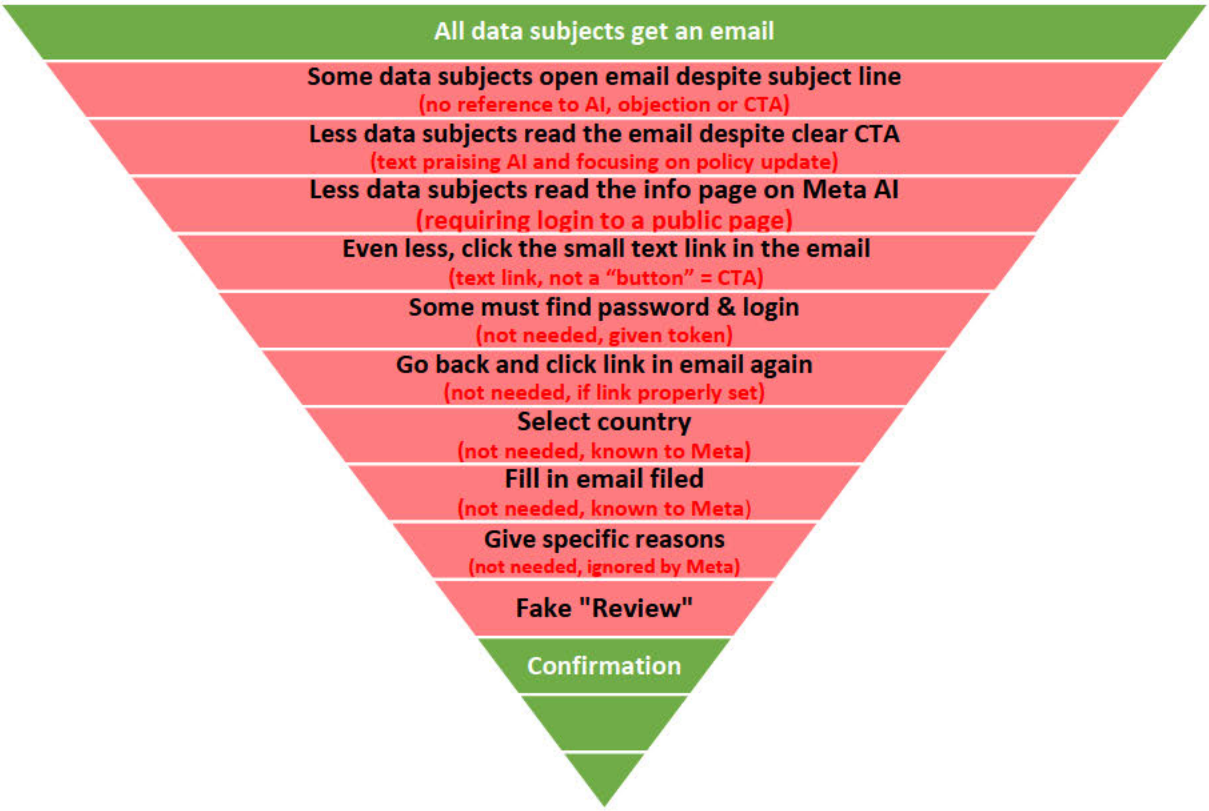
➔ *The alleged review seems to be a mere automatic approval, meaning that a simple click of a button would have been sufficient to "object" under Article 21 GDPR.*

1.7.3. Overview of opt-out process as a "*conversion funnel*" via email

When user engagement flows are designed, they are usually mapped as a "funnel" where each click and step is analysed. UI/UX designers generally do everything they can to avoid any steps that may not be crucially necessary, as each step means "losing" users.

Overall, Meta has introduced 11 steps (!) to file an objection under Article 21(1) GDPR, when this could have been done with a single opt-out button in the email or app.

When the Meta objection flow is mapped as such a "conversion funnel", it becomes evident that Meta has done everything to add more (useless, boring or deceptive) steps (in red below) in an attempt to have data subjects not exercise their right to object:


All data subjects get an email
Some data subjects open email despite subject line
(no reference to AI, objection or CTA)
Less data subjects read the email despite clear CTA
(text praising AI and focusing on policy update)
Less data subjects read the info page on Meta AI
(requiring login to a public page)
Even less, click the small text link in the email
(text link, not a "button" = CTA)
Some must find password & login
(not needed, given token)
Go back and click link in email again
(not needed, if link properly set)
Select country
(not needed, known to Meta)
Fill in email filed
(not needed, known to Meta)
Give specific reasons
(not needed, ignored by Meta)
Fake "Review"
Confirmation

Overview: Meta's objection "funnel" is designed to disengage data subjects.

It is painfully obvious that Meta has taken every step to ensure that it receives a minimal number of objections by using non-engaging language, bad UI/UX design and useless additional steps – the opposite of "*facilitating the exercise of the data subjects' rights*".

1.7.4. Simple way to seek objections in a user-friendly way

Overall, the objection could have been done with the push of a single button in the email itself (like e.g. most "unsubscribe" links in email newsletters under Article 21(3) GDPR). As shown under 1.6.2 above, Meta often uses such clear big blue buttons as CTA in its marketing emails.

➔ *Meta has deliberately made the access to the form substantially more complicated than necessary.*

1.8. Hidden and hideous second objection to the use of third-party data

We finally want to highlight that Meta only linked to a form allowing users to object against the use of personal data collected directly on Meta systems.

Only the third paragraph from the end of the lengthy information disclosure under https://www.facebook.com/privacy/genai/ provided a **second link to a second form** available at https://www.facebook.com/help/contact/510058597920541, which allowed users to object to the use of personal data from external sources. Given that this second form was introduced only at the end of the privacy policy, it seems that the vast majority of data subjects has never realized that there were two forms.

Even when this form would be found by data subjects, it is basically useless, as it requires:

- the data subject to find personal data in an AI system,
- proof that it found such a result and upload a screenshot of such a result and
- an explanation of the "concern" and "what you are requesting".

There seems to be **no option to object to the use of "third party" personal data in training datasets**, when such training data sets are based on web scraping or any form of external data sources or "third party" data.

➔ *Meta has not informed users about the second form on third-party data. Even when users could find the "third party data set objection" form, Meta would not allow them to object to the use of their personal data for training purposes; it would only allow them to protest results that contain personal data.*

2. VIOLATIONS OF THE GDPR

2.1. The lack of a legal basis under Article 6(1) GDPR

The use of any personal data to train an AI model is clearly "processing" of personal data under Article 4(2) GDPR, which requires a "legal basis" under Article 6(1) GDPR, as processing of personal data is by default illegal under the GDPR.

Meta seems to rely on an alleged overriding "*legitimate interests*" under Article 6(1)(f) GDPR to justify the use of personal data (including postings, pictures, friendships, likes, following of pages, visits on third party pages, third party data or messages exchanged with businesses) of about 400 million EU/EEA data subjects.

2.2. Existing case law in C-252/21 *Bundeskartellamt* is crystal clear

We are surprised that Meta is seriously arguing that it has a "legitimate interest" in using all the personal data of roughly 400 million EU/EEA users when the CJEU has recently, explicitly and clearly held in C-252/21 *Bundeskartellamt* that Meta does not even have a "legitimate interest" to use personal data for advertisement.

It seems clear that the bar set by the CJEU would not allow for the irreversible ingestion of their personal data into undefined "artificial intelligence technology" without any purpose limitation and with an undisclosed number of recipients that will be able to access personal data ingested into such a system.

➔ *Given that the CJEU has clearly taken the view that the use for personalized advertisement is not a "legitimate interest", it is painfully obvious that the processing of personal data via new means for any purpose (in all likelihood including "personalized advertisement") cannot be legal under Article 6(1)(f) GDPR.*

For the avoidance of doubt, we nevertheless want to briefly highlight each element of the typical 3-step test under Article 6(1)(f) GDPR that Meta fails:

2.3. Lack of a "legitimate interest" under Article 6(1)(f) GDPR (Step 1)

According to the established 3-step test,[18] Meta must claim and prove to have a "legitimate interest". In the current case, the analysis is already failing in the first step, as Meta neither claims – let alone proves – such a legitimate interest:

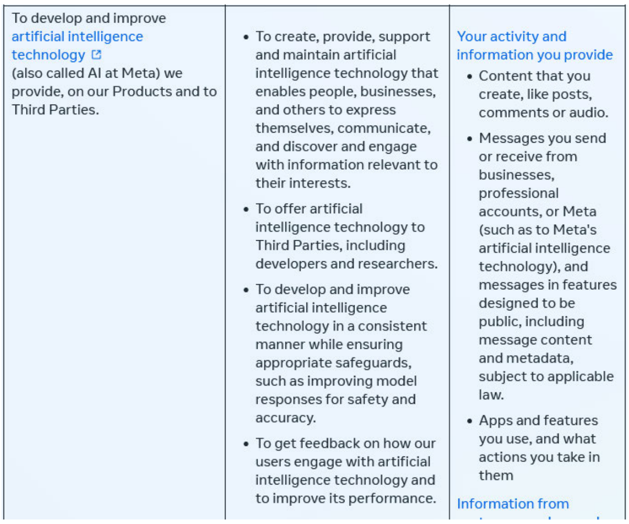
[18] CJEU 4 May 2017, C-13/16 (*Rigas*), para. 28.

2.3.1. *Meta relies on "technical means" – not a "legitimate interest"*

Usually any "legitimate interest" analysis starts with the <u>interest or the aim</u> of the processing activity – in other words the "purpose" of the processing operation.

> **Analogue Example:** If the <u>aim is to "*go to Paris*"</u>, then an "<u>*airplane*" may be a means</u> to reach that aim. However, <u>"airplane" is not an aim in itself</u>, let alone a legitimate interest.
>
> **GDPR Example:** The processing of personal data <u>cannot be justified by the wish to use a database system, a hard drive or an analytics software</u>. It must be justified by the need to achieve an <u>aim, purpose or interest</u>. Meta is not even arguing an aim.

As further detailed under 1.3.2 above, Meta is not naming any purpose that it tries to achieve via AI systems, but is instead trying to bypass the normal analysis of a legitimate interest by simply declaring <u>an entire type of processing ("AI") itself to be a purpose</u>:



To develop and improve artificial intelligence technology ↗ (also called AI at Meta) we provide, on our Products and to Third Parties.	• To create, provide, support and maintain artificial intelligence technology that enables people, businesses, and others to express themselves, communicate, and discover and engage with information relevant to their interests. • To offer artificial intelligence technology to Third Parties, including developers and researchers. • To develop and improve artificial intelligence technology in a consistent manner while ensuring appropriate safeguards, such as improving model responses for safety and accuracy. • To get feedback on how our users engage with artificial intelligence technology and to improve its performance.	Your activity and information you provide • Content that you create, like posts, comments or audio. • Messages you send or receive from businesses, professional accounts, or Meta (such as to Meta's artificial intelligence technology), and messages in features designed to be public, including message content and metadata, subject to applicable law. • Apps and features you use, and what actions you take in them Information from

Screenshot: Relevant disclosure of the "legitimate interests" by Meta in the new privacy policy.

The alleged purpose ("*To develop and improve artificial intelligence technology"*) is just as much of a purpose or a legitimate interest as any other means to process personal data (like "*store all data in a database*", "*run a social network*", "*find correlations in your data*" or "*to do Big Data analysis*"). What Meta is <u>describing is not a purpose, but means</u> (see e.g. Article 4(7) GDPR "*purposes and means*") to achieve various purposes.

Even if "*develop and improve artificial intelligence technology"* were a purpose, it would <u>not constitute a "specific" purpose</u>, as required under Article 5(1)(b) GDPR. For example, Wikipedia defines "artificial intelligence" as:

> *"Artificial intelligence (AI), in its broadest sense, is intelligence exhibited by machines, particularly computer systems."*[19]

➔ *Overall, the mere use of a technology (the use of certain "means" in the wording of GDPR) is not a "legitimate interest".*

➔ *<u>Meta tries to make the processing of personal data itself a "legitimate interest".</u>*

[19] See https://en.wikipedia.org/wiki/Artificial_intelligence

2.3.2. "Legitimate interests" recognised by the GDPR are usually defensive

The examples in Recital 47 to 49 of the GDPR are predominantly defensive legitimate interests (like network security, information security or preventing fraud). In such cases, the legislator has indicated an openness to recognise the processing of personal data as a "legitimate interest", given that the controller is merely acting in a defensive way.

Instead, Meta seems to want to offensively use the personal data of roughly 400 million EU/EEA data subjects to extract profits from (often long abandoned) social media profiles. The GDPR and its recitals do not provide or hint that such processing of personal data could be seen as a legitimate interest.

2.3.3. Making money itself is not a "legitimate interest"

Despite claims to the opposite by controllers, the mere interest in making money is itself not a "legitimate interest", as can be seen from the countless decisions on the sale of personal data, the use for personalized advertisement and the like.[20]

2.3.4. Mere data extraction is itself not a "legitimate interest"

Equally, it is not a legitimate interest to simply buy and collect personal data from third parties ("*data brokerage*") and use internal data for totally unrelated new business ideas.

If the mere extraction of personal data from various systems to support any type of new processing for any undefined purpose were a "legitimate interest", this would literally mean that any controller could use any personal data from any source for any new purpose. This narrative entertained by Meta is therefore totally outside of the common understanding under the GDPR.

2.3.5. Violation of Articles 5, 12, 13, 17(1)(c), 18, 19, 21(1) and 25 GDPR

As demonstrated below (see 2.6. to 2.10.) the proposed AI system of Meta and the way it was introduced clearly violates at least Articles 5(1), 5(2) 12, 13, 17(1)(c), 19, 21(1) and 25 GDPR. The violation of other provisions of the GDPR is another major factor, and why any balancing of interests under Article 6(1)(f) GDPR must fail.

An artificial intelligence system that is based on the violation of eight (!) Articles of the GDPR in one go cannot ever be seen as "legitimate".

2.3.6. Inclusion of "sensitive data" under Article 9 GDPR

The EDPB has dealt with this matter in Binding Decisions 03/2022 and 04/2023, where they asked the Irish DPC to investigate the use of data that falls under Article 9 GDPR by Meta. As you are surely aware, Meta and the DPC continue to resist this decision and filed

[20] See e.g. https://autoriteitpersoonsgegevens.nl/documenten/ap-normuitleg-grondslag-gerechtvaardigd-belang

annulment procedures before the General Court against the EDPB (see T-70/23 and T-129/23).

Already in its request for a preliminary ruling in C-446/21, Margin Number 16, the Oberster Gerichtshof (Austria) states that Meta's "*data processing does not distinguish between 'simple' personal data and 'sensitive' data".*

The same must be true for personal data used by Meta for AI systems. We therefore note that Meta also lacks the option to rely on a "legitimate interest" as it clearly tries to process personal data that does not fall under Article 6(1)(f) GDPR and were relying on a "legitimate interest" is simply not available under the GDPR.

2.3.7. Lack of separation between data subjects' personal data

As already explained in section 1.4.1, Meta admits that it is not in a position to separate personal data of (i.) data subjects that objected and (ii.) personal data relating to data subjects that did not object (and that potentially are not even Meta's users).

This leads to the inevitable conclusion that Meta's users that objected could still have some of their data processed when it was uploaded or published by other users. It is thus reasonable to assume that the right to object under Article 21(1) GDPR cannot be fully complied with.

Reliance on legitimate interest as a legal basis always requires compliance with the law, including that the data subject has the right to object. As this is not always possible, or at least not for all data, Meta cannot use Article 6(1)(f) GDPR for this processing activity.

2.3.8. Summary on the existence of a "legitimate interest"

The first step of the 3-step test already fails and can be summarized as follows:

➔ *Overall, it seems obvious that Meta neither claims – let alone proves – that it pursues any legitimate interest recognizable under Article 6(1)(f) GDPR.*

➔ *The mere use of a broad category of various technologies constitutes co-called "means" not a legitimate interest in itself.*

➔ *Compared to the legitimate interests named in the GDPR or accepted in case-law, the mere extraction of personal data to use for commercial gain is not a "legitimate interest".*

➔ *Finally, Meta tries to process an enormous pool of personal data, which (at least partly) contains personal data that cannot be processed based on a "legitimate interest".*

2.4. All data for any purpose is not strictly necessary processing (Step 2)

Very much overlapping with the principle of data minimisation in Article 5(1)(c) GDPR and the duty to engage in data protection by design and by default in Article 25 GDPR (see below), the second element of the CJEU's legitimate interest test requires that personal data be "*strictly necessary*".

In C-252/21 *Bundeskartellamt* the CJEU held at paragraph 108 that:

> *"…that condition requires the referring court to ascertain that the legitimate data processing interests pursued cannot reasonably be achieved just as effectively by other means less restrictive of the fundamental rights and freedoms of data subjects, in particular the rights to respect for private life and to the protection of personal data guaranteed by Articles 7 and 8 of the Charter…"*

The question is not if the processing would be better, easier or more convenient for the controller, but if it is "strictly necessary" to reach an aim or purpose. It is clear that the "strictly necessary" test must fail for Meta:

- It should be stressed that assessing the necessity of a certain processing operation is very difficult when the specific purposes are not even disclosed. As stated above, "*artificial intelligence technology*" is not a purpose but rather a broad group of means of processing. Processing can never be "necessary" to entertain technological "means".
- That being said, whatever the purposes may be, it is highly unlikely that they strictly require the use of *all* personal data of *all* EU/EEA users (excluding the content of private chats), without any anonymisation or pseudonymisation measures in place and with no time limit.
- This can also be demonstrated by the fact that many controllers have already developed "artificial intelligence technologies" without the use of such vast data sources.
- In addition, it must be noted that the fact that only some types of "artificial intelligence technologies" require a large amount of data to be trained does not authorise Meta to process any data potentially available to them. For example, "Reactive Machines" fall under the definition of "artificial intelligence" and are not based on past experiences to take decisions. It can therefore not logically be "strictly necessary" to use all personal data for any "artificial intelligence technology".

➔ *Overall, it seems obvious that Meta attempts to process personal data far beyond anything that is "strictly necessary" for the (undisclosed) potential purposes.*

➔ *This can also be demonstrated by the many existing AI systems that were trained and run on much smaller dataset.*

2.5. Meta can also not overcome the balancing test (Step 3)

Even if Meta would pursue a "legitimate interest" and the processing of (all) personal data it holds on data subjects would be "strictly necessary", the third level of Article 6(1)(f) – the overall "balancing" test – would also clearly fail for Meta:

2.5.1. Interpretation in light of Articles 7, 8 and 52(1) of the Charter

Obviously, Article 6(1)(f) GDPR must be interpreted in the light of the Charter, especially as Article 6(1)(f) GDPR has a similar function as the proportionality test in Article 52(1) of the Charter.

- If under C-293/12 *Digital Rights Ireland* (and many following judgements by the CJEU) the "mere" storage of communication meta data for the rather important purpose of national security is not "proportionate", how can the use of (almost) all personal data of a social network on about 400 million users be "proportionate" to train an AI model with unclear future use?
- If in C-311/18 *Schrems II* the "mere" scanning of traffic data and the access to stored data for national security purposes violates Article 7 and 8 of the Charter, how can the use of all of this data be "proportionate" when training an AI model?
- If in joined cases C-203/15 and C-698/15 *Tele2* the "mere" retention of traffic data and location data for the purpose of fighting crime violates Articles 7 and 8 of the Charter, how can the use of all this data be "proportionate" when training an AI model?

Already in comparison with CJEU case law on Article 7 and 8 of the Charter, it seems apparent that the use of much vaster amounts of personal data, for much more trivial purposes (like generating an AI picture or improving a chat bot) cannot be proportionate under Article 7 and 8 of the Charter and consequently also not be proportionate under Article 6(1)(f) GDPR.

2.5.2. Unlawful initial collection of personal data

Any balancing of interests must already fail, because Meta had largely no legal basis for the initial collection of large amounts of personal data that it has apparently used to train an AI model. In detail:

- Before the coming into force of the GDPR on 25.5.2018 Meta relied on consent under Article 7(a) of Directive 95/46. However, this consent was bundled, based on the mere use of the website (no "opt-in") and was clearly far from compliant with Article 4(11) GDPR. Meta can therefore not rely on consent obtained from data subjects up until 25.5.2018 for the processing of personal data.
- Given the EDPB Decisions 03/2022 and 04/2022, as well as the CJEU judgement in C-252/21 *Bundeskartellamt*, it is clear that Meta did not have a proper legal basis to collect large parts of the personal data that it obtained between 25.5.2018 and at least until 01.11.2023 when Meta switched to "pay or okay".
- Meta is now relying on a "pay or okay" model, which seems to be equally unlawful in the light of the EDPB Opinion 08/2024 of 17.04.2024.

We therefore note that large quantities of the personal data that are now being used to train Meta's AI model were never obtained legally and may therefore not be processed further. This factor alone would usually be a reason why an overriding legitimate interest (in further processing illegally obtained data) cannot be found.

2.5.3. Exceptionally large and unlimited amount of personal data

Furthermore, the personal data that is meant to be processed by Meta goes far beyond any "data pool" that was ever used for similar purposes:

- The processing concerns all personal data since the complainant signed up to the service – spanning a long time and including deleted personal data,[21] archived data and personal data of other users. The personal data stored with Meta can amount to thousands of A4 pages per single user in just a couple of years.[22]
- Such information can contain sensitive information revealing political leaning, financial background, sexual orientation or health problems, criminal offences, events that people attended or children's data.
- The processing also concerns online tracking data that Meta collects on third pages, personal data uploaded by others (individuals and businesses) and the like.
- Already in 2014, Meta reported to keep 300 Petabytes of data and add another 4 Petabyte per day.[23] Now, ten years later, these numbers have massively increased.

Compared to typical examples of an overriding "legitimate interest" (e.g. the mere storage of CCTV pictures for a limited space and time or the keeping of an IP address for security reasons), Meta engages in processing of totally unheard-of dimensions for undefined future purposes.

2.5.4. Largely non-public personal data

The personal data processed by Meta is largely data from private postings, privately shared pictures, private events or the "liking" or "following" of topics and pages that are not visible to the general public and often not even to "friends" on social networks.

In C-252/21 *Bundeskartellamt* the CJEU has held at paragraphs 84 and 85 that even rather public information, is not "fair game" and is generally protected by the GDPR:

> " [...] *Article 9(2)(e) of the GDPR must be interpreted as meaning that, where the user of an online social network visits websites or apps to which one or more of the categories set out in Article 9(1) of the GDPR relate, the user does not manifestly make public, within the meaning of the first of those provisions, the data relating to those visits collected by the operator of that online social network via cookies or similar storage technologies.*
>
> *85. Where he or she enters information into such websites or apps or where he or she clicks or taps on buttons integrated into those sites and apps, such as the 'Like' or 'Share' buttons or*

[21] See e.g. http://europe-v-facebook.org/removed_content.pdf

[22] See e.g. the blackened (shorter) version of the 1.220 pages provided to Max Schrems in 2011: http://europe-v-facebook.org/msb2.pdf

[23] https://research.facebook.com/blog/2014/10/facebook-s-top-open-data-problems/

> *buttons enabling the user to identify himself or herself on those sites or apps using login credentials linked to his or her social network user account, his or her telephone number or email address, that user manifestly makes public, within the meaning of Article 9(2)(e), the data thus entered or resulting from the clicking or tapping on those buttons only in the circumstance where he or she has explicitly made the choice beforehand, as the case may be on the basis of individual settings selected with full knowledge of the facts, to make the data relating to him or her publicly accessible to an unlimited number of persons."*

Similar statements can be found in C-362/14 *Schrems I*, C-311/18 *Schrems II* or C-468/10 Asnef, where the CJEU has consistently held that non-public data is protected, especially communication data and content data. It is obvious that Meta (operating a "social network") is predominantly using "communication data" and/or "content data" for the relevant processing activities.

2.5.5. High-risk technology with regular problems

In their current state, AI systems are still an unproven and speculative technology. This increases the risks for data subjects in an enormous way. Given that Meta also does not explain what the AI system will be used for, any product may be used against the interest of a data subject or may produce errors that lead to real-life consequences for the data subject.

This is not just theoretical, but very much the headlines of the past year(s). To name just some (of many) examples:

- Microsoft had to turn off an AI chatbot after it "*turned into a Nazi*".[24]
- Google rolled back its AI Search function given countless errors.[25]
- Facebook had to shut down AI bots after they spoke to each other in their own language, not understandable to humans anymore.[26]
- OpenAI had its systems used for phishing and scams.[27]
- California has banned "self-driving" cars, following regular problems.[28]

The lack of accurate results (see Article 5(1)(d) GDPR) and the overall unclear power and use of such systems makes the complainant fearful of having its own personal data ingested into such a system that may later also be used against the complainant.

The processing of personal data contrary to the interests of the data subject is another major factor that leads to a negative outcome in any balancing test.

[24] https://www.cbsnews.com/news/microsoft-shuts-down-ai-chatbot-after-it-turned-into-racist-nazi/

[25] https://www.nytimes.com/2024/06/01/technology/google-ai-overviews-rollback.html

[26] https://www.firstpost.com/tech/news-analysis/facebook-researchers-shut-down-ai-bots-that-started-speaking-in-a-language-unintelligible-to-humans-3876197.html

[27] https://tech.co/news/chatgpt-ai-scams-watch-out-avoid#phishing

[28] https://slate.com/business/2023/10/cruise-suspended-california-robotaxis-self-driving-cars-san-francisco.html

2.5.6. No right to object once personal data is used ("No way back")

As outlined above at 1.5. Meta itself says that any objection can only concern the use of personal data "*going forward*". Contrary to Articles 17(1)(c), 19 and 21(1) GDPR, this means that while no new personal data may be ingested into an AI system, Meta foresees no way to delete personal data that its "artificial intelligence technology" was already trained on. This is the clear opposite of a "*right to be forgotten*", which by definition also requires deletion of previously obtained personal data.

The fact that the use of personal data seems to be (technically) irreversible violates the right to object to any future processing under Article 21 GDPR.

In the Joined Cases C-26/22 and C-64/22 *SCHUFA*, the CJEU has already decided that any processing of (public) personal data must end as soon as the published data is deleted (in this case, within 6 months). The system of Meta does not allow to remove such data once any personal data is ingested into the system.

The fact that the processing is allegedly irreversible is another huge factor that would usually tip any balancing test towards a negative outcome.

2.5.7. Monopolistic role of Meta

As already highlighted in the EDPB Opinion 08/2024 on "pay or consent", Meta also has a large market dominance, profits from massive network effects and has an overall market penetration (400 million European users). This power makes the use of such vast amounts of personal data about a large percentage of the EU/EEA residents an especially grave interference with the rights of data subjects and limits their options to abandon such a network in the future, which is another factor in the balancing test.

2.5.8. Typical case of unlimited "secondary processing"

Sometimes the use of personal data for a closely related purpose (e.g. the option to apply an AI filter to an uploaded picture) may be in line with the expectations of a data subject and purposes of the processing.

However, the use of all personal data (no matter the purpose for which it was shared or generated) for an undisclosed future purpose contemplated by Meta via any form of current or future "artificial intelligence technology" is a typical case of unrelated "secondary processing", which the GDPR explicitly tries to prevent.

2.5.9. Expectation of data subjects

Data subjects have entered into agreement to share posting, watch cat pictures or chat with friends. There was no expectation of a data subject (that may have signed up years ago) that personal data entered into a social network would be used in 2024 to train AI systems with an undefined future purpose.[29]

As the CJEU has held in C-252/21 *Bundeskartellamt* has held at paragraph 117:

> *"In this regard, it is important to note that, despite the fact that the services of an online social network such as Facebook are free of charge, the user of that network cannot reasonably expect that the operator of the social network will process that user's personal data, without his or her consent, for the purposes of personalised advertising. In those circumstances, it must be held that the interests and fundamental rights of such a user override the interest of that operator in such personalised advertising by which it finances its activity, with the result that the processing by that operator for such purposes cannot fall within the scope of point (f) of the first subparagraph of Article 6(1) of the GDPR."*

If data subjects already had no "reasonable expectation" that their personal data would be processed for advertisement on Facebook (which was at least generally known to be a business that Meta was engaging with and more clearly disclosed in the privacy policy than the use of undefined "artificial intelligence technology"), it is absolutely incomprehensible how data subjects would have a "reasonable expectation" that any personal data entered in Meta systems since 2007 (!) would be used to train AI system.

This can also not be overcome by the information email (with deceptive subject lines, engagement flow and like, see above at 1.6) or pop-up messages on the page. Meta has provided similar information when it has previously updated privacy policies that introduced the reliance on Article 6(1)(b) GDPR or the gradual further use of personal data for advertisement – none of which have led to a different conclusion by the CJEU in the above-mentioned case law.

2.5.10. Industry standards

While industry standards under the GDPR are often a "low bar" given that many controllers do not comply with the law, we want to note that we are not aware of any consumer-facing controller that suggested that all personal data that was ever entered into its systems would be used to train "artificial intelligence technology".

Most currently known systems (that can already be highly problematic in relation to the GDPR) are trained with dedicated data that was obtained by the controller (e.g. scans of streets for self-driving cars), publicly available information (e.g. web scraping) or otherwise limited in scope. Meta has unique access to the private posts and pictures consumers have uploaded to Meta's services since 2007. This makes Meta's move to use all the data exceptionally intrusive.

Overall, this move by Meta (just like before the reliance on Article 6(1)(b) or the charging for not giving consent via "pay or okay") is again extremely exceptional.

[29] cf. Recital 47 GDPR: "[...] *At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing.* [...]"

2.5.11.Meta fails the overall balancing test

Given the initial unlawful collection of personal data, the exceptionally large and unlimited amount of personal data (including non-public data), the highly risky nature of the technology involved, the impossibility to object once one's data is has already been used, the disproportionate market power that Meta exercises over its users, the existence of a further processing clearly unrelated to the original one, a scope of processing well beyond the expectations of the data subject and even a lack of compliance with the (minimum) industry standards, Meta fails the balancing test and consequently cannot rely on legitimate interest under Article 6(1)(f) GDPR.

2.6. Violations of Article 5 GDPR

In addition to the lack of a legal basis under Article 6(1) GDPR, the approach by Meta also violates Article 5 GDPR. Given the "multifactor" approach taken under Article 6(1)(f) GDPR, these violations also reflect back on the lack of a "legitimate interest":

2.6.1. Fairness and transparency under Article 5(1)(a)

The extensive use of "dark patterns" when informing data subjects and allegedly allowing an objection (see in detail above at 1.6.1 to 1.7), such as requiring logins to see public links or the filling out of complicated forms (when any objection is actually approved in 50 seconds), were clearly not "*fair*".

The lack of proper information under Article 12 and 13 GDPR (see below) also leads to a violation of the transparency requirement in Article 5(1)(a) GDPR.

2.6.2. Purpose limitation under Article 5(1)(b) and 6(4)

As already highlighted under 2.3.1. above, Meta does not name any "specific purpose" for the processing of personal data via "artificial intelligence technology" but instead tries to make a specific means of processing itself the "purpose".

Even if a technology for data processing were a "specific purpose", it could never be a compatible purpose under Article 6(4) GDPR, as it may be used for wholly unrelated other purposes (see examples above under 1.3.2). The use for "any purpose" can by definition not be limited to only "compatible" purposes. Furthermore, the processing for such other purposes was also not foreseeable for the data subject.

Under the criteria listed in Article 6(4) GDPR, it is clear that the processing of personal data shared by Meta's users for the purpose of "*artificial intelligence technology*" is not compatible with the initial purposes, which is the provision a social network:

- There is no link between this initial purpose and the purpose of the intended further processing. Meta's envisioned use of personal data for the training of AI-models is not due to any link with the initial purpose, but rather arises from the fact that such training needs large amounts of data and Meta happens to possess large quantities of data that it wants to bring it to use.

- The context in which the personal data was collected contradicts the use for the intended further processing. Information was initially shared on Meta's platforms in order to participate in the social network provided by Meta and share information with certain people. The complainant and certainly also other Meta users did not anticipate that this information would be used to train AI models for all kind of undetermined future applications.
- The nature of the personal data, in particular the fact that special categories of personal data are processed, also contradicts the compatibility with the processing for training purposes of AI-models.
- The complainant can only speculate on the existence of any appropriate safeguards. It will be up to Meta to demonstrate in the ongoing proceedings whether such safeguards are in place. But even the existence of such safeguards does not change the fact that overall the further processing is incompatible with the initial processing.

Since a compatibility test in accordance with Article 6(4) GDPR shows an incompatibility between the initial purpose and the further processing for the training of unspecified future "*artificial intelligence technology*", Meta could not base the further processing on a legitimate interest (even if there was a legitimate interest which is challenged in this complaint). Instead, Meta would have to obtain the data subject's consent if it wants to use the data for intended further processing.

Overall, Meta clearly violates the purpose limitation principle in Article 5(1)(b) GDPR.

2.6.3. Data minimisation under Article 5(1)(c)

As already highlighted under 1.3.1 to 1.3.3, Meta does not limit the processing of personal data in any way (scope, sources, types of data or time limits). Other than private messages with other individuals, all personal data will be ingested in the AI systems. There is also no limitation via anonymisation, pseudonymisation or other privacy enhancing technologies.

Thereby, Meta also violates the data minimisation principle in Article 5(1)(c) GDPR.

2.6.4. Accuracy under Article 5(1)(d)

We further note that AI systems still have a very low accuracy rate.[30] While AI generated pictures of people with four fingers may be tolerable, inaccurate information on an individual can lead to serious harm. It is likely that any results that relate to a data subject will regularly produce false results, which will likely violate Article 5(1)(d) GDPR.

2.6.5. Storage limitation under Article 5(1)(e)

[30] https://noyb.eu/en/chatgpt-provides-false-information-about-people-and-openai-cant-correct-it

As far as the information by Meta goes, it plans to process personal data ingested into its artificial intelligence systems indefinitely. This would likely constitute an additional breach of Article 5(1)(e) GDPR.

2.6.6. Accountability under Article 5(2)

As demonstrated under 1.4.2 to 1.4.3 above, Meta says itself that it is (i.) unable to separate between personal data that falls under the GDPR and personal data that is not covered by the geographic application of the law and (ii.) unable to have a "clear cut" between personal data where Meta claims to have a legal basis under Article 6(1)(f) and personal data where users objected under Article 21(1) GDPR.

Reliance on a legal basis (like the claimed "legitimate interest") requires that the management of the legal basis be operationally possible. By not even being able to demonstrate the (already otherwise erroneous) reliance on Article 6(1)(f) GDPR, Meta is also clearly violating Article 5(2) GDPR.

2.7. Violation of Article 12 GDPR

As shown in 1.2 to 1.7, Meta does not provide "*concise, transparent, intelligible and easily accessible*" information according to Article 12 GDPR, nor does it inform the complainant in "*clear and plain language*". On the contrary, Meta attempts to conceal information by using "dark patterns" as highlighted in sections 1.6.1 to 1.6.6 of this complaint.

Furthermore, as discussed in 1.7, Meta is seeking to deter data subjects from exercising their rights by adopting a complex procedure instead of a "one click" objection. Thereby, Meta acts in violation of Article 12 (2), which requires the controllers to "*facilitate the exercise of data subject* rights".

2.8. Violation of Article 13 GDPR

As is already apparent under 1.2, Meta's new privacy policy violates Article 13 GDPR by failing to include several elements of this Article, as follows:

- Meta fails to inform the complainant of the exact purpose of processing, but simply names technical means ("*artificial intelligence technology*"). However, the disclosure of the specific purposes is obligatory under Article 13(1)(c) GDPR.
- Meta should have informed about legitimate interest it pursued in the processing, according to Article 13(1)(d) GDPR. Instead, the new privacy policy informs again only about the technical means ("*artificial intelligence technology*").
- In relation to the duties under Article 13(1)(e) GDPR to name the recipients of any processing operations, Meta merely refers to any "*third parties*". Given that this term includes everyone in the entire world, Meta does in fact not provide any information.
- Meta's new privacy policy does not provide any information on the duration of the processing nor on the criteria used to determine it, as mentioned in section 1.3.3 of

the complaint, therefore violating Article 13(2)(a) GDPR. Furthermore, Meta fails to inform the complainant of whether the personal data will be "shelved" and/or when a new LLM could be deployed.

Therefore, Meta acts in violation of multiple elements of Article 13 GDPR.

2.9. Violation of Articles 17(1)(c), 19 and 21(1) GDPR

As shown above at 1.5, Meta takes the view that any objection or other finding that personal data is processed without a legal basis (anymore) would not lead to the end of processing within an artificial intelligence system when data was already ingested.

This is contrary to the "right to be forgotten" and would instead limit the rights of data subjects under Articles 17 and 19 GDPR as well as under Article 21(1) GDPR to a mere "*right to not have even more data processed*".

This is nothing but an official proclamation to openly violate the GDPR.

2.10. Violation of Articles 25 GDPR

From the documentation that was provided by Meta, it seems obvious that Meta has not entertained any technical and organisational measures to:

- limit the processing of personal data or the impact on the fundamental rights of data subjects (such as an opt-in system or clear controls for data subjects),
- implement an approach of data minimisation in practice,
- limit the processing only to strictly "necessary" personal data,
- limit the processing to anonymised or pseudonymised personal data,

or indeed any other publicly available and enforceable measure. By failing to do so, Meta has also violated its duties under Article 25 GDPR ("data protection by design and default") when simply declaring the personal data of roughly 4 billion users worldwide[31] to be the "new oil" for any future AI machine.

[31] https://www.statista.com/statistics/947869/facebook-product-mau/

3. APPLICATIONS

Based on the above facts and law, and indeed any other facts or legal arguments that may arise during the procedure, we make the following applications:

3.1. Duty to act

The CJEU has repeatedly held that supervisory authorities have a positive duty to act if they are made aware of a GDPR violation. In C-311/18 *Schrems II* the CJEU held at paragraph 111:

> *"In order to handle complaints lodged, Article 58(1) of the GDPR confers extensive investigative powers on each supervisory authority. If a supervisory authority takes the view, following an investigation, that a data subject whose personal data have been transferred to a third country is not afforded an adequate level of protection in that country, it is required, under EU law, to take appropriate action in order to remedy any findings of inadequacy, irrespective of the reason for, or nature of, that inadequacy. To that effect, Article 58(2) of that regulation lists the various corrective powers which the supervisory authority may adopt."*

In the Joint Cases C-26/22 and C-64/22 *SCHUFA* the CJEU has further highlighted at paragraph 57:

> *"In order to handle complaints lodged, Article 58(1) of the GDPR confers extensive investigative powers on each supervisory authority. Where, following its investigation, such an authority finds an infringement of the provisions of that regulation, it is required to react appropriately in order to remedy the shortcoming found. To that end, Article 58(2) of that regulation lists the various corrective measures that the supervisory authority may adopt."*

In C-768/21 *Land Hessen*, the AG has further issued an opinion saying at paragraph 82:

> *"[...] that the supervisory authority has an obligation to act when it finds a personal data breach in the course of investigating a complaint. In particular, it is required to define the most appropriate corrective measure(s) to remedy the infringement and ensure that the data subject's rights are respected.[...]"*

An equal result can be derived from the general duty of public authorities to uphold fundamental rights - like the right to data protection in Article 8 of the Charter. There is consequently no question that any supervisory authority has a duty to act in this case.

3.2. Investigation under Article 58(1) GDPR

Given that some of the details of Meta's processing are unclear, we hereby apply for a full investigation using all powers under Article 58(1) GDPR, which should at least include the following steps:

- Clarification of the concrete "artificial intelligence technology" that will be used.
- Clarification of the personal data that will be ingested into such systems.

- Clarification on how Meta intends to separate EU/EEA personal data, data falling under Article 9 GDPR and data for which users have exercised choice (opt-in or opt-out) from data of data subjects that have taken the opposite decision.
- Clarification on the options to exercise the "right to be forgotten" under Article 17 GDPR, but also other GDPR rights (like the right to access or rectification) once personal data is ingested into such systems.
- Demanding any "Legitimate Interest" assessment that Meta may have conducted under Article 6(1)(f) GDPR.
- Demanding the record of processing activities under Article 30 GDPR (which previously only consisted of four (!) pages).[32]
- Demanding the documentation of any Data Protection Impact Assessment under Article 35 GDPR that Meta should have produced on these systems.

3.3. Preliminary stop of the processing activities under Article 58(2) GDPR and the Urgency Procedure under Article 66 GDPR

Given the exceptional circumstances of this case (see below), we apply to have a preliminary stop of any processing activities enforced via the "urgency procedure" in Article 66(1), (2) and (3) GDPR:

3.3.1. Urgency based on pending deadline and "no way back"

As outlined under 1.2, Meta seems determined to start using the complainant's personal data for some types of AI technology as of Wednesday 26.06.2024 - so in less than three weeks.

As further detailed under 1.5, Meta takes the view that data subjects cannot (effectively) object to the ingestion of their data into AI systems after 26.06.2024 as any such objections would only apply "*going forward*", which seems to mean that personal data once ingested into an AI system cannot be "forgotten" or "unlearned" - contrary to the GDPR's requirements in Articles 17(1)(c), 18(1) and 21(1). In other words, Meta says there will be no way back.

Furthermore, the fact that all personal data of more than 400 million affected people may be unlawfully processed is an additional factor that would constitute an "exceptional circumstance".

3.3.2. No imminent threat to Meta & limitation to three months

On the other hand, a preliminary halt of processing activities would merely amount to a "delay" of the processing operations - if the supervisory authorities may (opposite to any suggestion in the case law) later take a view that the approach by Meta was in fact legal.

[32] https://noyb.eu/geo/AR3/ROPA%20of%20Facebook_bk.pdf

According to Article 66(1) GDPR, any urgency action is also limited to three months, which would allow Meta to explain how this approach is legal.

3.3.3. Action by the Irish Supervisory Authority is unlikely

Given that:

- Meta has agreed with the Irish Supervisory Authority on this approach (see 1.1),
- The Irish Supervisory Authority has previously engaged in "confidential" backroom agreements with Meta,[33]
- The Irish Supervisory Authority and Meta are currently suing the EDPB over the application of Article 9 GDPR to personal data on Facebook (see 1.1),
- The previous need to issue Urgent Binding Decisions 01/2021 and Urgent Binding Decisions 01/2023 against the Irish Supervisory Authority on processing by Meta and
- The fact that Irish Supervisory Authority has by now a track record of 8 cases where the EDPB had to force it to follow its statutory duties,

we do not think it is realistic that the Irish Supervisory Authority will take appropriate steps to protect the personal data of roughly 400 million people.

While after six years of inaction by the Irish Supervisory Authority this may not be seen as an "exceptional circumstance" within the GDPR enforcement framework, we argue that the meaning of "exceptional" must be read in an objective way and may not be diluted by the extreme (in)actions of one supervisory authority.

3.4. Corrective powers under Article 58(2) GDPR

Even before any investigation may have come to a final conclusion, we urge the authority to take imminent, preliminary steps (or have the Lead Supervisory Authority take these steps via Articles 60 to 62 GDPR) to ensure that Meta does not pursue the processing operations any further, including but not limited to:

- Immediately issue a warning under Article 58(2)(a) GDPR, highlighting the unlawfulness of the intended processing.
- Order Meta to stop processing personal data of affected users for artificial intelligence purposes under Article 58(2)(d) and (f) GDPR.

3.5. Penalty

We assume that Meta's violations of Articles 5(1) and (2), 6(1), 9(1), 12(1) and (2), 13(1) and (2), 17(1)(c), 18(1)(d), 21(1) and 25 GDPR overall amount to a clear intentional breach of the law - especially in the light of the long list of previous CJEU, EDPB and SA decisions. We note that Article 83(1) GDPR require that Supervisory Authorities issue fines that are "*effective, proportionate and dissuasive*".

[33] https://noyb.eu/en/just-eu-55-million-whatsapp-dpc-finally-gives-finger-edpb