

Privacy policy for our collection of social media data for carrying out research of public interest

Analyse & Tal respects individuals' right to privacy and the right to correct and lawful.

This privacy policy is intended to support Analyse & Tal in complying with applicable laws at all times and to meet and comply with current data protection laws, including the EU's General Data Protection Regulation (GDPR) and the Danish Data Protection Act.

The purpose of this privacy policy is therefore to ensure transparency and legality in our processing of personal information for the individuals we analyze for carrying out research for public interest. Data is used in aggregated form for statistics and knowledge creation around a broad range of social media issues.

1. Contact information: Data controller and Data Protection Officer

Analyse & Tal acts as the data controller for this processing activity. Our contact information is the following:

Analyse & Tal F.M.B.A.
Lygten 39, 2400 København NV
Info@ogtal.dk
CVR. 36452595

Analyse & Tal have an internal standing 'committee for personal data' which is the company's compliance advisor and responsible for all Analyse & Tal's processing of personal data. The committee can be reached by the following:

Tobias Bornakke
Tlf.: +45 61 77 51 98
E-mail: Tobias@ogtal.dk

2. To which purpose do we process your personal information?

We process personal information collected from social media for multiple purposes, in particular public research studying:

- Online hate speech and minority rights
- Extremism and online radicalization
- Spread of mis- and disinformation
- Public debate, freedom of speech and democratic engagement
- Online volunteering
- Dissemination of illegal content
- Public health issues
- The protection of minors
- Data privacy
- AI generated content in the public debate

3. Legal basis of processing your data

The data processed in the project is primarily considered non-sensitive personal data. The data is thus collected and processed on the legal basis of the European General Data Protection Regulation (GDPR) article 6(1)(e), which permits for processing of general non-special category personal data with the goal of carrying out research of 'public interest'.

In some occasions, we carry out studies based upon special category data i.e. data linked to data subjects racial/ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sexual orientation, or the data subject's general health. In the event, we process special categories of personal data, which is prohibited by GDPR article 9(1), we base the legality of our temporary processing hereof on the exception in GDPR, art. 9(2)(e).

This specific legal basis of processing special category personal data is applicable to personal data, which are manifestly made public by the data subject itself and is exclusively used for processing personal data in these circumstances. We understand 'public' as communities either 1) defining themselves as public, e.g. being a 'public group' or presenting themselves as a public space, or 2) having at least 2000 members¹.

4. What data do we process?

We process content that sometime contains personal data (i.e. posts, images, tweets, comments, likes) from public social media pages and groups. We collect from a broad range of social media platforms, specifically but not exclusively:

- Facebook pages and public groups
- YouTube
- X (former twitter)
- Instagram
- Reddit
- TikTok
- Discord
- LinkedIn
- Flashback
- 4chan
- Threads
- Telegram
- Snapchat

For the majority of studies, we do not retain profile names or usernames. However, in some cases we chose to retain the first name of the profile to approximate demographic statistics.

Mitigating the risk of special category data

'Special category' data can emerge in our datasets both intentionally and unintentionally.

When studying sexual minorities, racial and ethnic groups, religious groups, trade unions movement, health groups and political groups we sometimes intentionally process special category data.

In these cases, we qualitatively screen all communities before data collection to establish to what extent the community should be considered 'public' and what risk our data collection poses for them. We will also often reach out to them, to make sure that we have a full understanding of how our data collection might pose a risk for them as a potential vulnerable group. Communities that do not qualify as 'public' or where the potential outcomes of the project outweigh the risk of the data subjects are then removed from the research project or fully anonymized.

¹ This specific limitation is based upon the official recommendation in the official guidelines for internet-based research developed by the national committee of research ethics in Norway 2019 available here: <https://www.forskningsetikk.no/retningslinjer/hum-sam/forskningsetisk-veileder-for-internettforskning/>.

Beside intentionally processing of special category data, a small risk exists that we unintentionally might process special category data.

Since full profile names and usernames are not collected, reidentifying the data subject based solely upon the dataset is in general impossible. However, a small risk exists that a user might mention or tag another user's name within a community that can reveal sensitive information about a data subject (e.g. a user tagging his friend with his full name within a community for homosexuals). If such data is encountered, we delete it immediately within our processing.

What data do we NOT process?

We do not process personal data pertaining to children under the age of 15 years without valid consent in accordance with the Danish Data Protection Act and GDPR. All communities are screened before collection of personal data in order to ensure that children under the age of 15 years and their personal data is not collected without valid consent or authorized by the holder of parental responsibility over the child.

Data storage and deletion

All data is stored in secured servers in data centers within the EU. Data is stored on encrypted hard drives and only transported through SSL-encrypted connections. All data collected is either fully anonymized or deleted 4 years after completion of each project. To respect the rights of data controllers to maintain control of their personal data, we will remove from every dataset any personal data pertaining to an individual who requests such deletion.

Analysis and presentation of data

We strive not to publish any personal data collected during research. An occasional exception to this policy is observed when the user is publicly known to the extent that they would not reasonably expect their social media posts to be private. It should be noted here that the GDPR only applies to natural persons, and not companies or organizations.

Personal data is also not shared with third parties external to Analyse & Tal without the explicit consent of the data subject. Any data published or shared with a third party is aggregated, anonymized, or altered to prevent identification of a natural person.

Where quotes from social media users are presented in our reporting, regardless of format, these quotes are bowdlerized/altered in a way which preserves meaning but prevents retroactive identification of the original post through e.g. an online search. This can consist in editing parts of the posts to make it impossible to identify, anonymizing text-bites or by removing the name of the page or group from where the post was collected.

National provisions

Since our organization is based in Denmark, where our headquarters are located, we follow the national provisions of Denmark and the guidelines put forward by the Danish Data Protection Authority (4 article, 16). Although, as the data is collected and processed on the legal basis of the European General Data Protection Regulation (GDPR) article 6(1)(e), which permits for processing of non-special category personal data with goal of carrying out research of 'public interest', this also applies to all Nordic countries.

5. Your rights as a data subject

Your rights in accordance with the EU's General Data Protection Regulation and the Danish Data Protection Act, you have several rights that you can invoke in connection with Analyse & Tal's processing of personal data. Beware that these rights can be limited due to this processing's nature of a research activity. The rights are as follows:

5.1 Right of access

You have the right to access the information we process about you and the right to receive a copy of any information we hold about you, including information about who has disclosed the information if it did not come from yourself.

5.2 Right to erasure and right to rectification

You have the right to have information about you erased or rectified. You have the right to have your information erased when it is no longer necessary. You can also contact us if you believe that we are processing your personal data unlawfully.

When you request to have your information erased or rectified, we assess whether the conditions are met. If the conditions are met, we rectify or erase your information as soon as possible, and if not, we will contact you with a reason why your information cannot be erased or rectified.

5.3 Right to restriction of processing

You have the right to have the processing of your personal data restricted in certain circumstances. This applies if 1) the accuracy of your personal data is contested by you and we as the data controller are unable to verify the accuracy of this personal data, 2) the processing of your personal data is unlawful and you request the restriction of their use instead of erasure, 3) we do not longer need your personal data but they are required by you for the establishment, exercise or defense of legal claims and 4) you have objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

5.4 Right to object

You have the right to object, on grounds relating to your particular situation, at any time to processing of your personal data which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. As the data controller, we shall no longer process the personal data unless we can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of you or for the establishment, exercise or defense of legal claims.

5.5 Right to complain to a Data Protection Authority

You have the right to complain to the Danish Data Protection Agency if you believe we are processing your information unlawfully, or if you believe we are not respecting your rights.

The contact information to the Danish Data Protection Agency is as follows:

Datatilsynet
Carl Jacobsens Vej 35.
2500 Valby
Telefon: 33 19 32 00
Mail: dt@datatilsynet.dk
www.datatilsynet.dk